

Administration Guide

This guide is targeted for administrators responsible for managing [user](#) and [group](#) rights and [register recorded phones](#) and more.

[Authentication and access control](#)

- [Authentication](#)
- [User roles](#)
- [User permissions](#)
- [Visibility of functions and conversations](#)
- [How to make Secondary recordings visible](#)

[Users](#)

- [Find and List Users](#)
- [User Configuration](#)
- [User-Group Association](#)
- [User Group Membership History](#)
- [User Default Call List Layout](#)
- [Custom User Fields](#)
- [Built-in user accounts](#)

[Groups](#)

- [Group List](#)
- [Group Details](#)
- [Group Membership History](#)
- [Group queries configuration](#)

[Recording rules](#)

- [Extension list](#)
- [Extension details](#)
- [Recording modes](#)
- [Conversation direction and modality support](#)
- [Modality and recorded platform support matrix](#)
- [Selective recording rule configuration](#)
- [Administration of recorded extensions for Cisco network-based recording](#)
- [Administration of recorded extensions for Passive Recorder](#)
- [Correcting user-extension assignments](#)
- [Microsoft Teams selective recording settings](#)
- [Relay-only configuration for Microsoft SfB - Lync](#)
- [Shared line recording configuration with Cisco recording](#)

[User and Group Management Tools](#)

- [Active Directory synchronization](#)
- [Bulk User and Extension Update](#)
- [Bulk user import](#)
- [Using the Group CSV Import](#)

[Data management](#)

- [Data management policies](#)
- [Data retention](#)
- [WORM](#)
- [Storage and export targets](#)
- [Data processors](#)
- [Import sources](#)

- [Resilient storage and archiving](#)
- [Best practices for large databases](#)
- [Data management policy monitoring](#)
- [Data management policy audit log](#)
- [Disposal audit log](#)

[Export](#)

[Server and service configuration](#)

- [Service control and activation](#)
- [Verba server administration](#)
- [Verba server configuration](#)
- [Verba server configuration profiles](#)
- [Shared servers](#)
- [Server Certificates](#)

[Log and Configuration Collector](#)

[Metadata templates](#)

- [Metadata template details](#)
- [Metadata template fields](#)

[Labels](#)

- [Managing Labels](#)
- [Automatic labeling](#)

[Audit logs](#)

- [Audit log for user related events](#)
- [Searching a call playback event](#)
- [Conversation audit log](#)

[Multitenancy](#)

- [Configuring Verba for Multitenancy](#)
- [Creating a new Environment](#)
- [Adding a user to an Environment](#)
- [Adding an extension to an Environment](#)
- [Environment login](#)
- [Searching calls in different Environments](#)
- [Managing Data Retention in Environments](#)
- [Multi-tenant License Allocation](#)

[Configuring metadata for contact center integrations](#)

[Migration from Verint](#)

- [Migration from Verint v11 and v15.1 Legacy systems](#)
- [Migration from Verint v15.2 systems](#)

[Sites](#)

[Hub](#)

Authentication and access control

Access to the Verba system and the recordings are controlled by the configuration of users, roles, groups and extensions.

Users

[Users](#) represent people who are able to login to the system. Users have the following fundamental parameters that define their access:

- [general user settings](#), such as validity period, visibility window, etc.
- [four eyes policy](#) settings
- [user roles](#) define what actions they can do in the system
- [associated extensions](#) define which records they can get access to based on the configured phone numbers / extensions / SIP URIs
- [group associations](#) define which groups a user belong to; if a user is promoted to be **group supervisor** of a group, the user will be able to see all calls of the users of that group

Groups

[Groups](#) represent a list of users who belong together for some organizational reason. The key aspect of groups is the possibility of promoting users to become **group supervisors** and see all calls of the members of the group. Each user can supervise and belong to multiple groups.

Extensions

[Extensions](#) represent phone numbers in the system. These Extensions can have different recording modes (always-on, on-demand, do not record), and can be **associated with a user**. A user can have multiple extensions, but an extension can belong to only one user.

Which calls can I see?

The [Visibility of functions and conversations](#) article summarizes the factors that decide who will see what in the system.

Further details

- [Authentication](#)
- [User roles](#)
- [User permissions](#)
- [Visibility of functions and conversations](#)
- [How to make Secondary recordings visible](#)

Authentication

Each time a user logs into the system, the user is authenticated. Authentication of a user's credentials means that the system identifies the user and gives her/him permission to access the system according to the configuration of the user. The system supports multiple methods of user authentication. Each method uses a specific authentication principle:

- Form-based: the user has to provide the username and password in a form each time they try to access the system
- Federated: user credentials are held with a third-party identity provider (IdP) and not within the system, and a token is provided to the system to validate. It is used to provide the single-sign-on capability for the system.

Authentication Type	Authentication Principle	Description
Database Credentials	Form-based	<p>Database Credentials authenticates the user with a user name and password that is maintained in the system database. The password hashes are managed securely in the database. When the Database Credentials authentication method is used, password and account locking policies are also managed within the system.</p> <p>For more information, see Password and user lockout policy</p>
Windows Active Directory (LDAP)	Form-based	<p>The Windows Active Directory (LDAP) uses a simple bind authentication process. The user is identified by the Active Directory and the proof of identity comes in the form of a password. When a more secure method is required, Secure LDAP (SLDAP) can be used.</p> <p>To configure this authentication mode, see Identity provider - Active Directory.</p>
Windows Active Directory Federation Service (ADFS)	Federated	<p>Windows Active Directory Federation Service (ADFS) authentication is an OpenID Connect (OIDC) based authentication method. OIDC is an authentication method where the user's credentials are held with a third-party identity provider (ADFS) and not within the system. The system verifies the user's identity based on a simple JSON- based identity token which is delivered on top of the OAuth protocol.</p> <p>To configure this authentication mode, see Identity provider - Active Directory Federation Services.</p>
Azure Active Directory (AAD)	Federated	<p>Azure Active Directory (AAD) authentication is an OpenID Connect (OIDC) based authentication method. OIDC is an authentication method where the user's credentials are held with a third-party identity provider (Azure Active Directory) and not within the system. The system verifies the user's identity based on a simple JSON- based identity token which is delivered on top of the OAuth protocol.</p> <p>To configure this authentication mode, see Identity provider - Azure Active Directory.</p>
Integrated Windows Authentication (IWA)	Federated	<p>Integrated Windows Authentication (IWA) allows users, once they have signed in to Windows, to automatically log in to the system. Password verification takes place during Windows sign in. Upon success, a Kerberos ticket is generated. When the user is authenticated by the system the Kerberos ticket is validated.</p> <p>To configure this authentication mode, see Identity provider - Integrated Windows Authentication.</p>
JSON Web Token (JWT)	Federated	<p>The system can be integrated with customer applications via JSON Web Token (JWT) based authentication to provide a seamless single sign on login experience. Authentication and password verification takes place during signing in to the client application. The system verifies the user's identity based on the information presented in the JWT.</p> <p>To configure this authentication mode, see Identity provider - JSON Web Token.</p>

Reverse Proxy	Federated	Reverse proxy based authentication allows users, once they have authenticated with an authentication server through the proxy, to automatically log in to the system. The system verifies the user's identity based on the information presented in the request from the proxy. To configure this authentication mode, see Identity provider - Reverse proxy .
OpenID Connect	Federated	OpenID Connect is an open standard identity layer on top of the OAuth 2.0 protocol, it allows third-party applications to verify the identity of the end-user and to obtain basic user profile information. The Verba system only utilizes the Login ID of the authenticated user. Verba supports the Authorization Code Flow . To configure this authentication mode, see Identity provider - OpenID Connect .

The authentication process is implemented in the Web Application component installed on the Media Repository / Application Server role.

The system allows configuring multiple identity providers in a single system (or in a tenant in case of multi-tenant deployment). For a user to log into the system, must have at least one of the identity providers enabled. Identity providers are configured through the roles /permissions for the users.

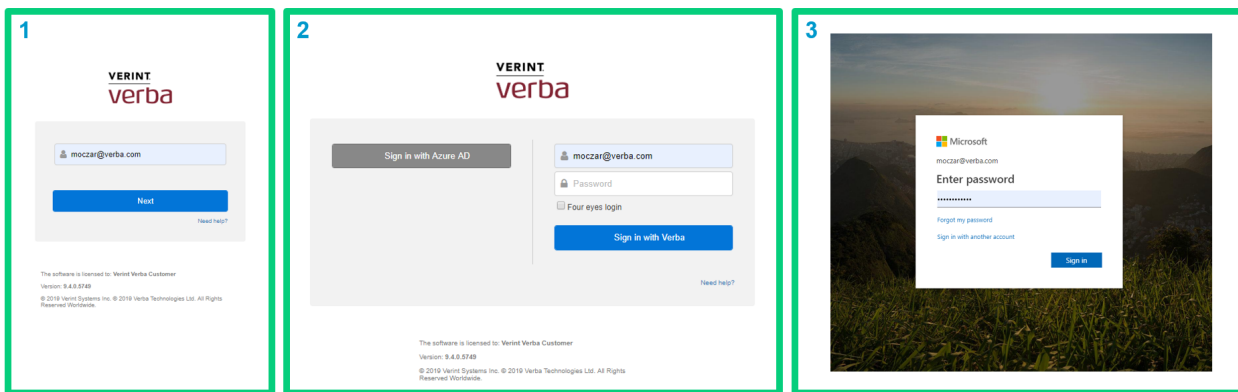
By default, all roles have the Database Credentials and Integrated Windows Authentication options are enabled. System administrators can add new identity providers and change the default settings by updating the role configuration.

Login process

Depending on the configured IdPs for the users, the login screens and the login process might be different for users.

When multiple IdPs are enabled in the system, the system provides a 2-step authentication process. In the first step, the system identifies the user. In the second step, the system offers all configured authentication options. If there is only one IdP enabled, the system automatically skips the first step.

The following image shows the 2-step authentication in case of Azure AD and Database Credentials IdPs are both enabled.



Configuring identity providers

See the following article to configure identity providers and assign them to users: [Identity providers](#).

Identity providers

The system allows configuring multiple identity providers in a single system (or in a tenant in case of multi-tenant deployment). For a user to log into the system, must have at least one of the identity providers enabled. Identity providers are configured through the roles /permissions for the users.

By default, all roles have the Database Credentials and Integrated Windows Authentication options are enabled. System administrators can add new identity providers and change the default settings by updating the role configuration.

Adding a new identity provider

To add a new identity provider, follow the steps below:

Step 1 - On the web interface go to **System / Security / Identity Providers** menu option.

Step 2 - Click on the **Add New Identity Provider** link on the top right.

Step 3 - Add a **Name** and select the **Type**.

Step 4 - Configure the parameters depending on the selected type.

[Integrated Windows Authentication configuration](#)

[Windows Active Directory \(LDAP\) configuration](#)

[Windows Active Directory Federation Services \(ADFS\) configuration](#)

[Azure Active Directory \(AAD\) configuration](#)

[JSON Web Token configuration](#)

[Reverse proxy configuration](#)

[OpenID Connect configuration](#)

Step 5 - Press **Save** to add the new identity provider. Once the identity provider is added, it is available under the role configuration.

Assigning identity providers to users

To assign one or more identity providers to users, follow the steps below:

Step 1 - On the web interface go to **Users / Administration / Roles** menu option.

Step 2 - Click on one of the existing roles in the list to create a new one by clicking on the **Add New Role** link on the top right.

Step 3 - Under **Regular User Permissions / Application Access**, select an item from the **Available Identity Providers** list box and click on the



button to add the item to the **Associated Identity Providers** list.

Step 4 - Press **Save** to change the configuration settings of the role. The new settings will be applied once the users with the configured role will try to login again.

Identity provider - Integrated Windows Authentication

Overview

The web application can authenticate users using Microsoft Windows domain authentication information. If a user is logged into the Windows Domain on a PC, the same user can access the web application without authenticating again.

When the domain user opens the web interface the system automatically authenticates the Windows user against the AD and logs in him /her to the recording system seamlessly. However this still requires a user created in the Verba Recording System due to the need for configuration settings not available in active directory.

Do not confuse this SSO functionality with the separate [Single Sign-On API](#), that allows Single Sign-on integration with any systems/portals using a simple web protocol.

✔ This SSO function helps you stop managing user passwords and user deletions in the Verba Recording System. You will still need to create the users in Verba, configure access rights and assign phone numbers to them.

Configuring Integrated Windows Authentication

Follow three steps to enable/configure SSO.

Step 1 - Make sure your Verba web app server in the same domain where your users are.

Step 2 - Configure the web app for SSO. With System Administrator rights you will find these under **Administration menu / Verba Servers / (select your server) / Change Configuration Settings / Web Application Configuration / Single sign on settings**. See the parameters in the [Web application settings](#) topic.

Configuration Parameter Name	Description
Strip Domain Information from Login ID	If enabled, the system will not use the Windows domain information during the single sign-on process. Practically it means, that the users - configured in the Verba system - do not contain the domain information in the login ID.
Domain User Account Format	If the Windows domain information is used during the single sign-on process (the Strip Domain Information from Login ID setting is disabled), then the users - configured in the Verba system - have to contain the domain information. This setting allows users to select the way the domain information is stored in the login ID in the Verba system.
Allow Single Sign-On for System Administrators	Enables or disables the single sign-on feature for system administrators. If disabled, the users with system administrator privileges are not allowed to authenticate using the single sign-on functionality.

Step 3 - Configure users with the login name in the Verba Recording System as in Active Directory

If you have problems with SSO verify the following:

- [Integrated Windows Authentication browser requirements](#)
- [Integrated Windows Authentication server requirements](#)

Accessing the web interface with IWA


In order to access the web interface using SSO, use the following URL:

```
http://ServerNameorIPAddress/verba/sso
```

When Verba is configured to use the secured SSL (HTTPS) protocol, to access the web interface, the following must be in the address bar:

```
https://ServerNameorIPAddress/verba/sso
```

If a user already logged in to the domain of the web application, they can just access the system. If they are not logged in, the browser will automatically asks for the Windows user credentials.

 You can use Active Directory / Windows Domain based authentication and standard Verba authentication at the same time on one system. Your users need to access the web interface using the above links to use SSO. Other web links do not provide this capability.

Forcing non-IWA login when IWA is enabled

It is possible to force a non SSO login by visiting the following URL:

```
https://ServerNameorIPAddress/verba/login.do
```

Changing the default login procedure to single sign-on

You can change the above behaviour, where SSO requires a separate link.

Step 1 - If you have not already done that, please follow the above steps to enable SSO

Step 2 - Access the Verba server using **Remote desktop**

Step 3 - Open the **<PROGRAM FILES>\Verba\tomcat\webapps\ROOT\index.html** file where **<PROGRAM FILES>** is e.g. "C:\Program Files (x86)"

Step 4 - Change the META line from

```
<META HTTP-EQUIV="Refresh" CONTENT="0; URL=/verba">  
to  
<META HTTP-EQUIV="Refresh" CONTENT="0; URL=/verba/sso">
```

Step 5 - This change goes live without any restart, point your browser to <http://ServerNameorIPAddress>

Integrated Windows Authentication browser requirements

If you have problems with IWA, verify the following:

- **For all types of browsers**

- **Use the hostname of the server instead of the IP address**
- **Use https, make sure the server's certificate is trusted by the browser**
- **Add the URL to Local intranet zone in IE even if you use Chrome or Firefox**

AD SSO might not work if Internet Explorer does not consider the server as a Local Intranet site. Make sure you add your service domain URL (e.g. verba.company.com) to the Local intranet zone in Internet Explorer.

Go to Tools > Internet Options > Security

Select the Local intranet icon and click Sites

Click Advanced and add the URL of the server (for example: <http://verbaserver.com>).

- **Internet Explorer**

- **Strange error pages with HTTP Status 401**

Internet Explorer users may occasionally receive strange error pages after logged in to Verba using Single Sign On. Unfortunately, the cause of the issue is an Internet Explorer feature and can be solved on the client computer only. Microsoft has confirmed that this is a problem with the Microsoft products.

The only workaround currently is to disable NTLM Pre-Authentication on the client computer:

Use Registry Editor (Regedt32.exe) to add a value to the following registry key: HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Internet Settings/

Add the following registry value:

Value Name: DisableNTLMPreAuth

Data Type: REG_DWORD

Value: 1

A description and the same workaround from Microsoft can be read here: <http://support.microsoft.com/kb/2749007>

- **Ensure that "Enable Integrated Windows Authentication" is checked (by default it is).**

Go to Tools > Internet Options > Advanced

Scroll down to the Security section

Find "Enable Integrated Windows Authentication" and ensure that it is checked.

- **Firefox**

- **If SSO does not work (ie. an unexpected login box appears, or HTTP 401 error comes up), probably the Verba server has to be added to the trusted SSO servers.**

At the address field, type <about:config>

In the Filter, type network.n

Double click on network.negotiate-auth.trusted-uris

This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser

Enter a comma-delimited list of trusted domains or URLs (for example: <http://verbaserver.com>).

- **Chrome**


- **Everything should work properly without any further configuration.**

Integrated Windows Authentication server requirements

- **Add the server to Windows Domain** - The server running the Verba web app (Media Repository component) has to be added to the Windows Domain where your users are. Currently, there is no simple SSO solution for organizations with multiple domains.
- **Tomcat has to be run as a service with Local System or Network Service account** to enable all types of authentication.

Or alternatively, use the following setspn commands in your AD:

```
setspn -S HTTP/Verbaserver-name.domain.com verba-service-user
setspn -S HTTP/Verbaserver-name verba-service-user
setspn -S HTTP/Verbaserver-name.domain.com domain\verba-service-user
setspn -S HTTP/Verbaserver-name domain\verba-service-user
```

 You should wait one day for the setspn commands to take effect!

- If you have done the client side requirements as well and you are still having issues with SSO then navigate to C:\Program Files\Verba\tomcat\webapps\verba\META-INF\context.xml and uncomment the following line:

```
<!-- By default, this parameter is not set -->
<!--
<Parameter name="onlyntlm" value="" override="false"/>
-->
```

- **To enable logging** add this to the end of C:\Program Files\Verba\tomcat\conf\logging.properties:

```
fr.doume.level = FINE
```

Identity provider - Active Directory

Step 1 - Provide a **Name**.

Step 2 - Provide the address of a domain controller at the **Host** setting.

Step 3 - If login without specifying the domain is required, complete steps 4-6

Step 4 - Provide an AD user at the **Login Name** setting. Provide its password in the **Password** field.

Step 5 - Provide the appropriate LDAP **User Search Base**

Step 6 - Provide the **Login ID Attribute** to be matched.

ID

Name * Identity provider - Active Directory

Type * Windows Active Directory (LDAP) ▼

Verba Login ID does not Contain Domain *

Host * dc.verbalabs.com

Port * 389

Use SSL *

If the following settings are configured, then the users can authenticate using their login name without the domain part. The system will find the AD user based on the Login ID Attribute.

Login Name verbalabs\administrator

Password *****

User Search Base OU=Users,DC=verbalabs,DC=com

Login ID Attribute sAMAccountName

Item	Description
Host	Fully Qualified Domain Name of the server hosting the active directory.
Port	389/3268 (global catalog query) or 636 /3269 (global catalog query) if SSL is used
Use SSL	Check to use Secure LDAP protocol to authenticate users
Login Name	The username of an AD user in Down-Level Logon or User principal name format
Password	The password for the user
User Search Base	The tree in the active directory that contains application users.
Login ID Attribute	The AD attribute that the Verba Login ID is matched against

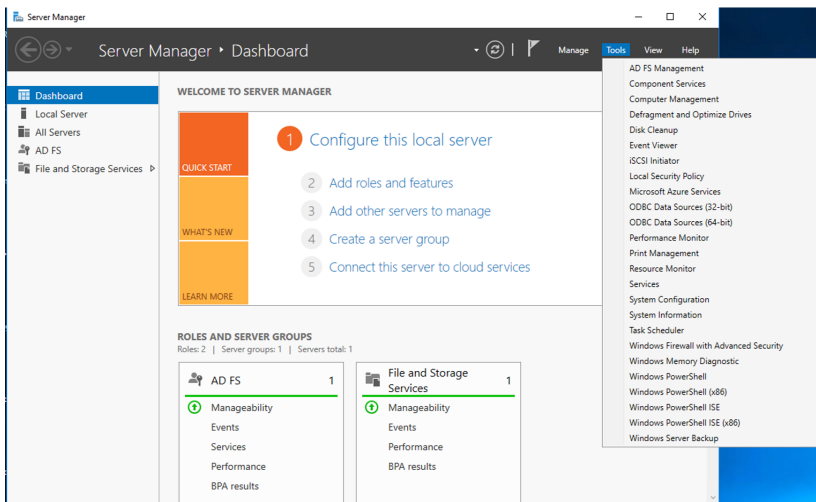
Identity provider - Active Directory Federation Services

Windows server configuration

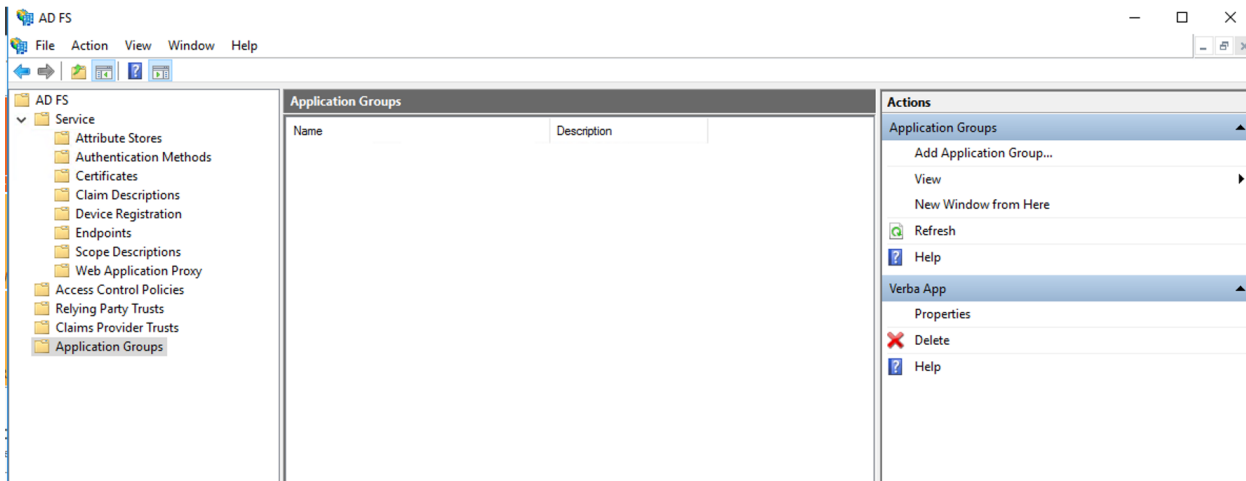
Open ID connect requires ADFS 4.0 - Windows Server 2016 or later.

The server needs the Active Directory Federation Services role installed and configured. For the official Microsoft guide, refer to [Install the AD FS Role Service](#)

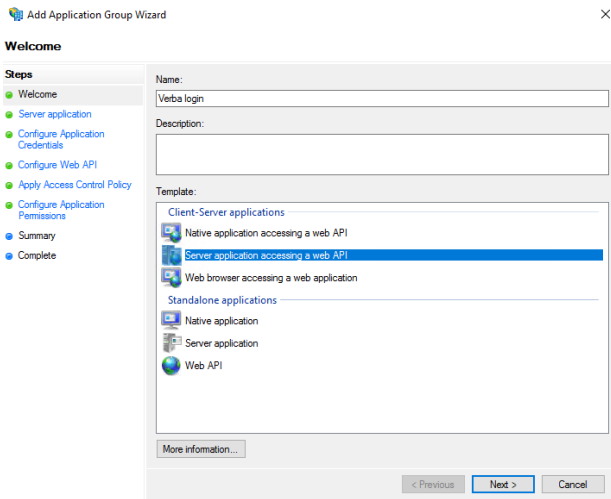
Step 1 - Connect to the server with AD FS role and open the AD FS Management



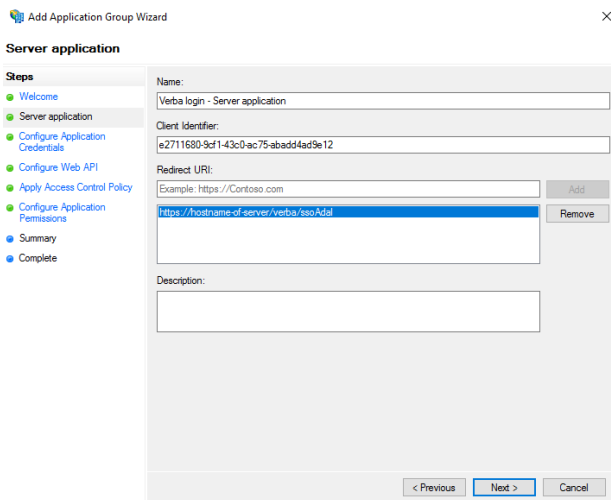
Step 2 - Navigate to Application Groups / Add application group



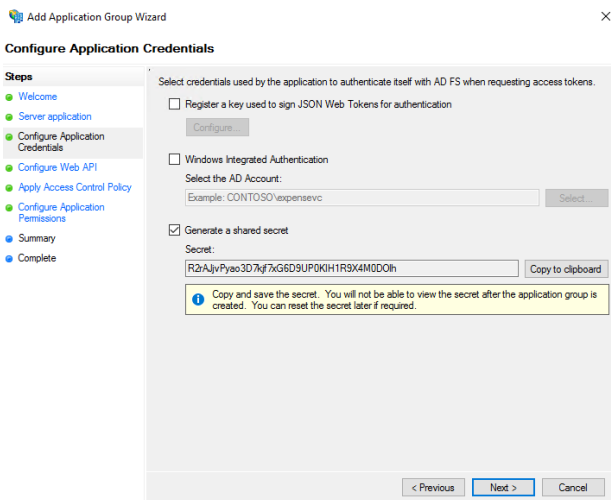
Step 3 - Select the Server application accessing a web API template and name the application group (optional)



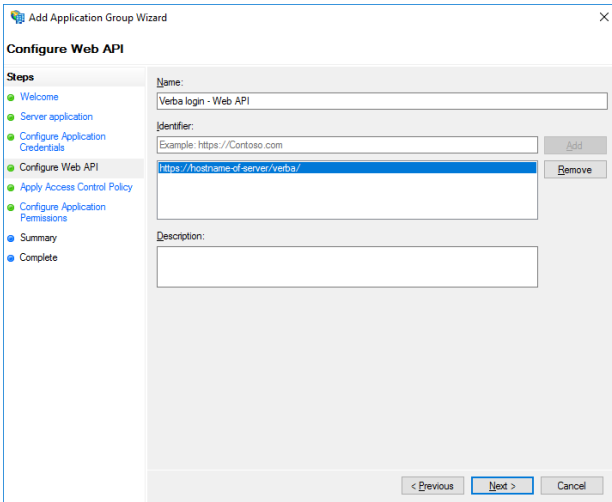
Step 4 - Click next, note the Client Identifier and add the redirect URI in the format: <https://hostname-of-server/verba/ssoAdal>



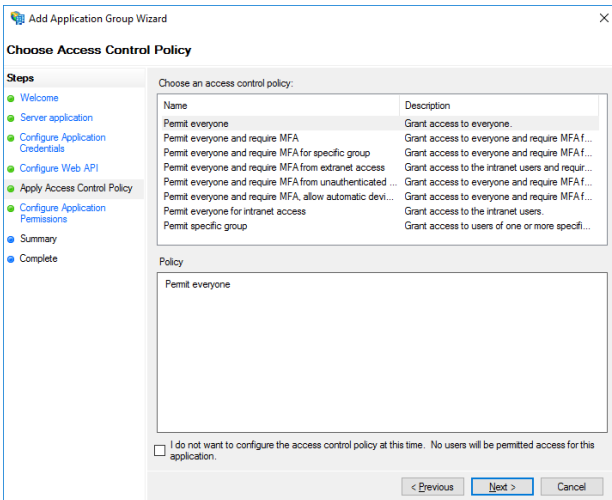
Step 5 - Select the Generate shared secret option, note the secret



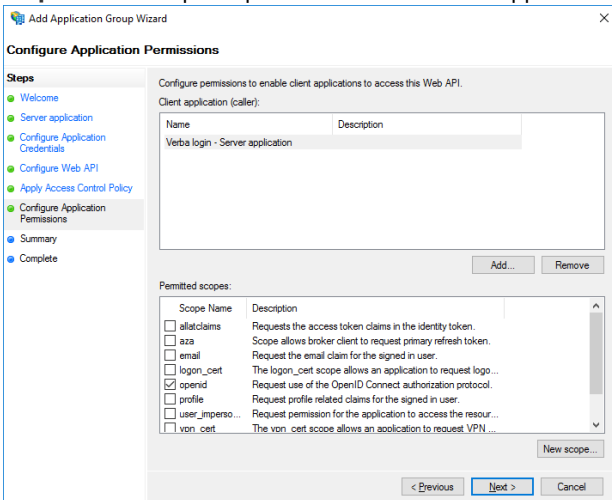
Step 6 - Add the redirect URI in the format: <https://hostname-of-server/verba/>



Step 7 - Configure the MFA if required. For the official Microsoft guide, refer to [Configure Additional Authentication Methods for AD FS](#)



Step 8 - Add the openid permission for the server application



Verba configuration

Fill the required fields based on the description

Name	Description
Client ID	The ADFS identifier noted in step 4
Client Secret	The ADFS secret noted in step 5
Authority	The server with the ADFS role in https://adfs-server/adfs format
Certificate	CA or server certificate in Base-64 encoded X509

Identity provider - Azure Active Directory

Azure configuration

Step 1 - Log in to <https://portal.azure.com>

Step 2 - Navigate to Azure Active Directory - App registrations - New registration

Register an application

* Name
The user-facing display name for this application (this can be changed later).
Verba login ✓

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Verba Technologies Ltd. only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web | <https://hostname-of-server/verba/ssoAdal> ✓

Step 3 - Define the display name of the application, and the supported account types

Step 4 - Add the redirect URI in the format: <https://hostname-of-server/verba/ssoAdal>

Step 5 - After the application is created, note down the client and tenant ID

Display name : Verba login

Application (client) ID : 98e84d21-ece4-4207-838f-291f8e9a625a

Directory (tenant) ID : aa6e6a76-90dd-4ca7-ad13-9c12600b9f18

Step 6 - Open certificates & secrets and add a New client secret

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE
Password uploaded on Mon Sep 09 2019	12/31/2299	MnUGmk1M68rmi:Ehs3Fnw/*+nwVu@zIR

Step 7 - Note the value of the new secret

Step 8 - Navigate to Azure Active Directory - App registrations - Created application - API permissions

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	STATUS
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

Step 8 - Add the app the User.Read permission

Step 9 - Grant administrator consent to the application (Optional)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

Grant admin consent for Verba Technologies Ltd.

Verba configuration

Name	Description
Tenant ID	The identifier noted in step 5 or the yoursitehere.onmicrosoft.com
Application ID	The identifier noted in step 5
Client Secret	The value noted in step 7
Authority	Default value is https://login.microsoftonline.com/

Identity provider - JSON Web Token

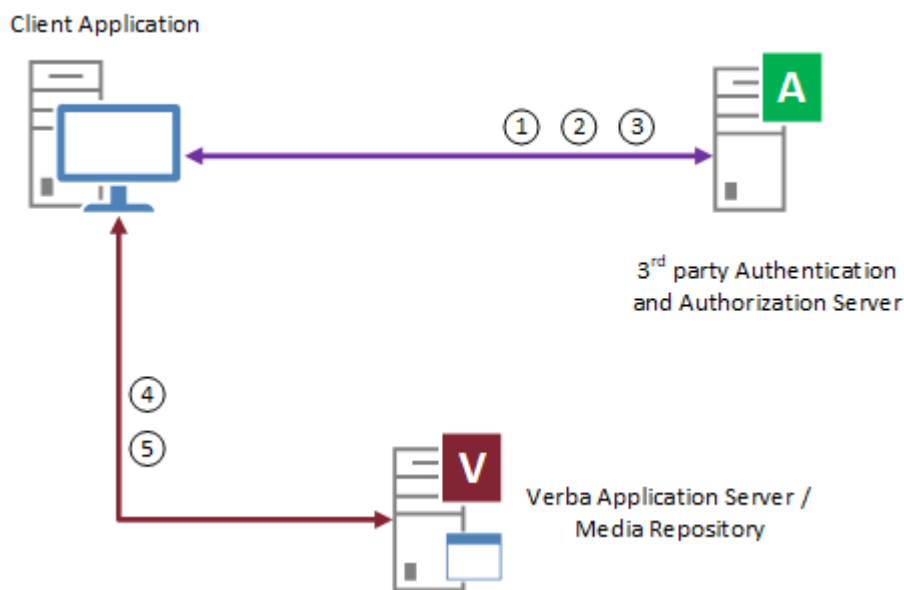
AVAILABLE IN 9.6.6 AND LATER

Overview

JSON Web Token (JWT) is an open standard ([RFC 7519](#)) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed. JWTs can be signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA. When tokens are signed using public/private key pairs, the signature also certifies that only the party holding the private key is the one that signed it. Authorization and single sign on are the most common scenario for using JWT. Once the user is logged in, each subsequent request will include the JWT, allowing the user to access routes, services, and resources that are permitted with that token.

The Verba system can be integrated with customer applications via JSON Web Token (JWT) based authentication to provide a seamless single sign on login experience. Authentication and password verification takes place during signing in to the client application. The system verifies the user's identity based on the information presented in the JWT.

A sample scenario is shown on the diagram below.



1. User authenticates in the Client Application (web, mobile, etc.) with the Authentication Server.
2. Client Application requests a JSON Web Token (JWT) from the Authorization Server to login to the Verba Web Application.
3. The Authorization Server verifies the request and signs the JWT with its private key and sends the JWT to the Client Application
4. The Client Application opens/redirects to the Verba Web Application with the JWT (which includes the user ID) in the HTTP header.
5. The Verba Web Application validates the JWT (verifies the signature, the user ID, etc). If all checks succeed, the user is logged into the application.

Configuration

Step 1 - Provide a **Name**.

Step 2 - Provide the user attribute for the matching in the **Verba User Attribute** setting.

Step 3 - If not exact matching of the attribute is required, change the **Verba User Attribute Matching**

Step 4 - Edit the **Request Header**, **Request Header prefix**, and **Request Parameter** if needed

Step 5 - Provide the **Expiration Timezone**

Step 6 - Check **Prevent Token Reuse Mandatory Token Fields**

Step 7 - Define the **Signature Algorithm** for the **Signature Key** (*RSA needs a Public Key, HMAC needs Secret Key*)

Step 8 - In case of multiple issuers, define a Regex unique to each issuer and repeat **Step 7** for each

Step 9 - Check if **HMAC Secret is Base64 Encoded**

Multiple timezones

If multiple Issuers (Authorization Servers) are used with different time zones, then separate Identity Providers are needed.

Item	Description
Verba User Attribute	The user attribute used for matching the user
Verba User Attribute Matching	Defines the matching for the user attribute
Request Header	The token can be sent either by a request header or an HTTP parameter This configuration specifies the HTTP request header that will contain the token The default value is "Authorization"
Request Header prefix	The authorization scheme This prefix will be cut by the Verba server from the request header value
Request parameter	The token can be sent either by a request header or an HTTP parameter This configuration specifies the HTTP request parameter that will contain the token
Audience Regex	Optional, if defined the system will disregard tokens that do not have the matching "aud" attribute
Expiration Timezone	The timezone for the token expiration
Prevent Token Reuse	Checking prevents reuse of the token
Mandatory Token Fields	Defines mandatory token fields Tokens that do not contain the fields marked as mandatory will be discarded
Signature Keys	
One Identity Provider can have multiple Signature Keys to support multiple Issuers (Authorization Servers).	
Issuer Regex	The system will use the Issuer Regex to choose which key to be used to validate a given token
Signature Algorithm	The algorithm used for the communication, either RSA or HMAC
Key	The key used for the communication RSA needs a Public Key, HMAC needs Secret Key
HMAC Secret is Base64 Encoded	The HMAC Secret is a list of bytes and so can contain special or even non-displayable characters In that case, the secret's Base64 encoded form should be used in the Key field, and this checkbox should be turned on.

Identity provider - Reverse proxy

AVAILABLE IN 9.6.6 AND LATER

Overview

This authentication option allows using a reverse proxy to handle the authentication of the users, meaning that once the user has logged into their proxy, they can seamlessly access the Verba Web Application.

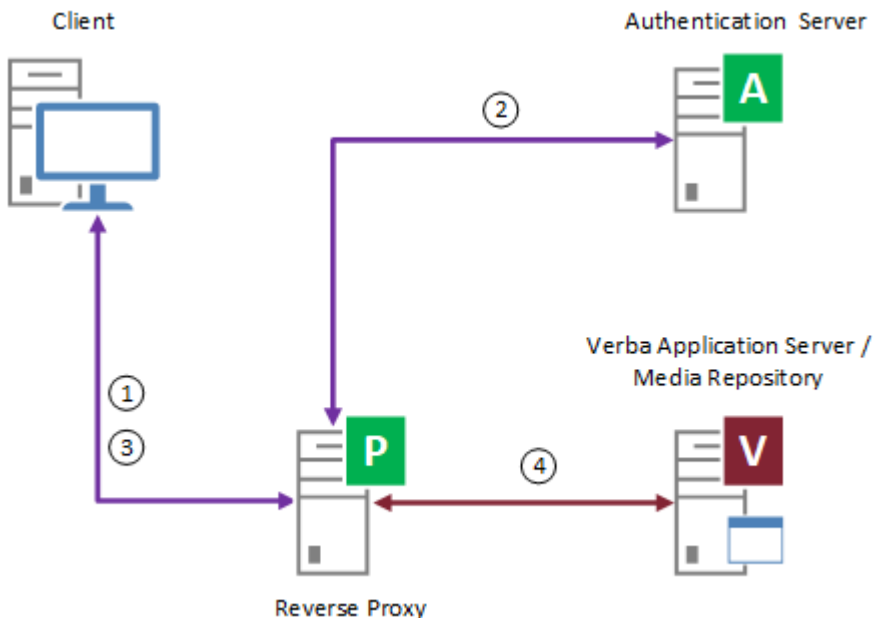
When the users attempt to access the Verba Web Application URL, the proxy server authenticates the incoming request against your authentication system. After successful authentication, the proxy sets a request header with the authenticated user identity and sends this information to Verba Web Application. The Verba Web Application accepts the incoming HTTP request from the proxy, and if it recognizes the user contained in the header, the user will be automatically logged in to the application. For successful single sign-on, all requests from the proxy to the Verba Web Application must include the authentication headers. If the header is not included in a request, then the user is returned to the login page. The Web Application uses the authenticated header for the duration of the browser session.

⚠ The header value is trusted without further checks or additional authentication, all incoming connections from the reverse proxy will log in all users based on the HTTP headers.

It is highly recommended to restrict the access to the Verba Web Application to the proxy server(s) by configuring either:

- Windows Firewall
- or Remote Address Filtering on Tomcat. For more information, see https://tomcat.apache.org/tomcat-9.0-doc/config/filter.html#Remote_Address_Filter.

A sample scenario is shown on the diagram below.



1. The user opens the Verba Web Application URL which is directed to the Reverse Proxy
2. The Reverse Proxy authenticates the user with the Authentication Server
3. After successful user authentication, the Reverse Proxy forwards the request to the Verba Web Application and provides the user identity in request headers

- The Verba Web Application validates the user identity and if the user is recognized the user is logged into the application automatically.

An example of reverse proxy-based authentication is based on Symantec SiteMinder (formerly CA SiteMinder). In this configuration, the Reverse Proxy is a Microsoft IIS web server that is integrated with the SiteMinder Agent.

Configuration

Step 1 - Provide a **Name**.

Step 2 - Provide the user attribute for the matching in **Verba User Attribute** setting.

Step 3 - If not exact matching of the attribute is required, change the **Verba User Attribute Matching**

Step 4 - Provide the **Request Header** sent by the reverse proxy

Step 5 - Provide a Regex that matches the header immediately before the User Attribute

Step 6 - Provide a Regex that matches immediately after the User Attribute

ID

Name * Identity provider - Reverse proxy

Type * Authentication with Reverse Proxy

Verba Login ID does not Contain Domain *

Verba User Attribute * Login ID

Verba User Attribute Matching * Exact

Request Header * X-AUTH

Prefix Regex (^[:;*\s]*)sAMAccountName=

Stop Regex ;

For example, if the header value is "userID=123; sAMAccountName=john.doe@verba.com; displayName=John Doe" and you would like to match the Verba user by "john.doe@verba.com", then set the Prefix Regex to "^([:;*\s]*)sAMAccountName=" and the Stop Regex to ";" (quotes are only for clarity).

Item	Description
Verba User Attribute	The user attribute used for matching the user
Verba User Attribute Matching	Defines the matching for the user attribute
Request Header	The header sent by the reverse proxy
Prefix Regex	Regex matching the prefix
Stop Regex	Regex for stopping after the User Attribute

Identity provider - OpenID Connect

AVAILABLE IN 9.7.6 AND LATER

Overview

OpenID Connect is an open standard identity layer on top of the OAuth 2.0 protocol, it allows third-party applications to verify the identity of the end-user and to obtain basic user profile information. The Verba system only utilizes the Login ID of the authenticated user.

Verba supports the [Authorization Code Flow](#):

1. The user opens the Verba web interface and types the Login ID
2. The Verba web interface offers the OpenID Connect authentication
3. The user chooses the OpenID Connect and the browser is redirected to the Authorization Server
4. The user authenticates itself and is redirected back to the Verba web interface with the Authorization Code
5. The Verba back-end requests an ID Token using the Authorization Code at the Token Endpoint
6. The Verba Web Application validates the ID Token and the user is logged into the application

Configuration

Item	Description
Client ID	The Verba web interface will use this Client ID to request the ID Token
Client Secret	The Verba web interface will use this Client Secret to request the ID Token
Authentication Request URL	The Authorization Server URL
Authentication Request - response_type parameter	Usually should be set to "code"
Authentication Request - scope parameter	Usually should be set to "openid"
Authentication Request - login hint parameter name	Login Hint parameter name that will be passed to the Authorization Server (optional)
Token Request URL	The Token Request URL
Token Request - grant_type parameter	Usually should be set to "authorization_code"
Token Request - Authentication	The authentication method of the Token Request (BASIC or POST body parameters)
ID Token Attribute	Which ID Token Attribute should be used to look up the Verba user (usually "sub")
Verify the state parameter	Should the "state" parameter be passed and verified in the response? All modern OpenID Connect providers should support the state parameter
Verify the nonce claim	Should the "nonce" parameter be passed and verified in the token? All modern OpenID Connect providers should support the state parameter
Authorization Endpoint HTTPS Certificate	Only set if the Authorization Endpoint's HTTPS Certificate is not trusted by Java running the Verba web application

Password and user lockout policy

Password policy

Various settings for rules applied to passwords.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
Minimum Password Length	Defines the minimum length of the password fields in the system. The setting applies for all users configured on the web interface.
Passwords Expire after (days)	Defines the number of days, after which the passwords expire in the system. This setting only applies for users where this feature is enabled. 0 means that the password never expires.
Passwords Must Include Capital Letter	Password phrases must include at least one capital letter or not. The setting applies for all users configured on the web interface.
Passwords Must Include Numeric Character	Password phrases must include at least one numeric character or not. The setting applies for all users configured on the web interface.
Passwords Must Include Special Character	Password phrases must include at least one special character or not. The setting applies for all users configured on the web interface.
Password History Count	Defines how many passwords will be stored for each user. Password history prevents users from changing their passwords to ones that they have used in the past. If the value equals to 0, it means that password history is disabled. The setting applies for all users configured on the web interface.

User lockout policy

When enabled the user lockout settings automatically locks users out after a certain number of incorrect login attempts.

The following table provides detailed instructions on each configuration setting:

Configuration Parameter Name	Description
User Lockout Attempts Threshold	The lockout threshold can be set to any value from 0 to 999 (attempts). If the lockout threshold is set to zero, users will not be locked out due to invalid logon attempts. Any other value sets a specific lockout threshold. The setting applies for all users configured on the web interface.
User Lockout Threshold Reset After (minutes)	This value represents how long a user will be locked out after unsuccessfully logging into the system. By default, the lockout threshold is maintained for 30 minutes, but any value can be set from 1 to 99,999 minutes. The setting applies for all users configured on the web interface.

User roles

The Verba Recording System provides a highly customizable role-based user access control system. Administrators can create user roles, each containing a specific set of rights that define which features of the web interface can users with that role access.

After creating them, each user can be assigned one or more roles. They will be granted all the permissions that at least one of their assigned roles contain.

This article is a guide on creating and managing user roles. It also describes how to assign roles to users.

Creating new user roles

To create a new user role, log into the web interface with the sufficient administrative rights and select **Administration > Roles** from the **Users** top menu. This will display a list of currently defined user roles. Verba ships with a collection of default roles pre-configured, but you are free to change, or remove these and create new ones.

Find and List Roles [Add New Role](#)

Name begins with

Name	Description	# of Assigned Users	# of Admin Rights	# of End User Rights	Enabled	Last Modification Date
Contact Center Supervisor		0	2	37	Yes	Sep 14, 2017 3:24:15 PM
Data Retention Administrator		0	4	2	Yes	Sep 14, 2017 3:24:15 PM
eDiscovery Manager		0	11	27	Yes	Sep 14, 2017 3:24:15 PM
eDiscovery User		0	11	26	Yes	Sep 14, 2017 3:24:15 PM
Multi-tenant Administrator		0	1	2	Yes	Sep 14, 2017 3:24:15 PM
Quality Management Administrator		0	1	2	Yes	Sep 14, 2017 3:24:15 PM
Quality Management Agent		0	0	4	Yes	Sep 14, 2017 3:24:15 PM
Quality Management Evaluator		0	0	5	Yes	Sep 14, 2017 3:24:15 PM
Read-only Administrator		0	24	2	Yes	Sep 14, 2017 3:24:15 PM
Server Administrator		0	7	2	Yes	Sep 14, 2017 3:24:15 PM
Shared-only User		0	0	8	Yes	Sep 14, 2017 3:24:15 PM
Speech Analytics Administrator	Can create speech indexing policies and manage speech phrases	0	1	2	Yes	Sep 14, 2017 3:24:15 PM

Click on the Add new Role button in the top right corner of the page. The next page lets you name your role, apply a description and define the set of rights specific for this role. For more information on the various permissions available refer to the [User Permissions page](#).

Role Configuration [Add New Role](#)
[Back to Previous Page](#)

Role

Name*

API Name*

Description

Enabled Yes

Regular User Permissions

Application Access

Available Identity Providers

Associated Identity Providers

Mobile web

Dial-in interface

Conversation Access

Scope

Filtering Criteria

Filtering Criteria Relationship Across Roles

Once you are done with setting up the role properties, click Save at the bottom of the page. The new role will appear in the role list and is now assignable to users.

Managing existing user roles

To edit the properties of an existing role, log into the web interface with the sufficient administrative rights and select **Administration > Roles** from the top menu. This will display a list of currently defined user roles. Click on the role you need to edit, then make your changes on the role properties page.

When you are done editing, click Save.

After this point, each user with the edited role assigned to it will have the new set of permissions according to the changes made to their role.

Assigning roles to users

There are two ways to associate roles and users. You can either associate multiple users at once with a specific role or you can grant a single user multiple roles at once. Please note that these two processes have equal effect behind the scenes, you are free to choose which one is more convenient for you.

To define a user's set of roles open the Verba web interface with the sufficient administrative privileges, then select **Administration > Users**. Select the user you want to manage from the list. This opens the user configuration page. To assign roles to the user, scroll down to the bottom of the page.

The Assigned Roles section contains a list of roles the user currently has. The Other roles section contains a list of roles that can be assigned to the user. Configure the user's roles using the checkboxes next to the roles.

The screenshot shows the 'User Data' and 'Authentication' sections of a user configuration page. The 'User Data' section includes fields for 'Display Name' (Thomas Powell), 'Login ID' (thomas), 'E-mail Address', 'Location', and 'Type' (Standard). The 'Authentication' section includes fields for 'Password' and 'Confirm Password', checkboxes for 'Password Expires' and 'User Must Change Password at Next Logon', date pickers for 'Valid From' (1970.01.01 01:00) and 'Valid Until' (2099.01.01 01:00), a 'Recorder Line PIN' field with 'Generate' and 'Clear' buttons, checkboxes for 'Locked' and 'API Access Only', and dropdown menus for 'Observer User (four eyes login)' and 'Observer Group (four eyes login)'.

By clicking on the gear icon next to one of the roles in the list, you can open a new window where you can quickly access the properties page of the selected role.

System Supervisor

To associate multiple users at once with a single role, go to **Administration > Roles**, then select the role you want to manage. Click on the Assign Users tab on the top of the page. On the next page you will see a list of users currently associated with the role you selected. You can add more users to the role using the Search field to find the users you need.

You can remove users from the role by clicking on the Trash icon next to the user in the list.

The screenshot shows the 'Role Configuration' page with the 'Assign Users' tab selected. It displays 'Found 2 users, listing all.' and a search field. Below the search field, a table lists 'Current Users having Role System Supervisor' with columns for 'User Name' and 'Action'. The table contains two entries: 'Verba Api User (verbaapi)' and 'Verba Desktop Api User (verbaDesktopapi)'. A 'Save' button is visible at the bottom. A 'Snipping Tool' window is overlaid on the bottom right of the page.

When you are ready with the configuration, click Save for the changes to take effect.

Legacy roles

To achieve backward compatibility with previous Verba releases, the system contains a pre-defined non-editable set of legacy roles which correspond with user rights present in pre-Verba 8 releases.

When upgrading Verba to version 8 or above, each user will be assigned one or more of the legacy roles according to their original rights.

Find and List Roles Add New Role						
<input type="radio"/> Standard Roles <input checked="" type="radio"/> Legacy Roles						
Name <input type="text"/> begins with <input type="text"/> <input type="button" value="Find"/>						
<small>No active query. Please enter your search criteria using the options above.</small>						
21 items found, displaying 1 to 20. Page(s): < < 1 2 > >						
Name	Description	# of Assigned Users	# of Admin Rights	# of End User Rights	Enabled	Last Modification Date
Access to Shared Calls (Legacy)		1	1	5	Yes	Nov 8, 2014 7:40:43 PM
Call Protection (Legacy)		1	1	7	Yes	Nov 8, 2014 7:40:43 PM
Comment (Legacy)		2	1	7	Yes	Nov 8, 2014 7:40:43 PM
Delete Call (Legacy)		1	1	7	Yes	Nov 8, 2014 7:40:43 PM
Download (Legacy)		2	1	7	Yes	Nov 8, 2014 7:40:43 PM
E-mail (Legacy)		2	1	7	Yes	Nov 8, 2014 7:40:43 PM
Play (Legacy)		12	1	7	Yes	Nov 8, 2014 7:40:43 PM
Private (Legacy)		1	1	7	Yes	Nov 8, 2014 7:40:43 PM
Quality Management Administrator (Legacy)		1	2	3	Yes	Nov 8, 2014 7:40:43 PM
Quality Management Agent (Legacy)		0	1	3	Yes	Nov 8, 2014 7:40:43 PM
Quality Management Supervisor (Legacy)		0	1	5	Yes	Nov 8, 2014 7:40:43 PM
Recycle Bin (Legacy)		1	1	6	Yes	Nov 8, 2014 7:40:43 PM
Reporting (Legacy)		2	1	3	Yes	Nov 8, 2014 7:40:43 PM
Share Calls (Legacy)		1	1	6	Yes	Nov 8, 2014 7:40:43 PM
Silent Monitor (Legacy)		2	1	6	Yes	Nov 8, 2014 7:40:43 PM
Speech - Indexed User (Legacy)		0	1	3	Yes	Nov 8, 2014 7:40:43 PM
Speech Administrator (Legacy)		1	2	2	Yes	Nov 8, 2014 7:40:43 PM
Speech Search (Legacy)		1	1	6	Yes	Nov 8, 2014 7:40:43 PM
System Administrator (Legacy)		2	22	2	Yes	Nov 8, 2014 7:40:42 PM
System Supervisor (Legacy)		2	1	27	Yes	Nov 8, 2014 7:40:43 PM

21 items found, displaying 1 to 20. Page(s): | < < 1 2 > > |

Export options: [Excel](#) | [RTF](#)

User permissions

- [Regular User Permissions](#)
 - [Application Access](#)
 - [Conversation Access](#)
 - [Group Supervisor Access Scope](#)
 - [Download / Export](#)
 - [Sharing](#)
 - [Annotation](#)
 - [Data Retention](#)
 - [Reporting](#)
 - [Quality Management](#)
 - [Speech Analytics](#)
 - [Communication Policies](#)
 - [Customization](#)
- [Administrative Permissions](#)
 - [User Administration](#)
 - [Security](#)
 - [Customizations](#)
 - [Data Management](#)
 - [Operation and Maintenance](#)
 - [Multi-tenant](#)
 - [Quality Management](#)
 - [Speech Analytics](#)
 - [Communication Policies](#)
 - [Authorization Request](#)
 - [Announcement](#)
- [Dashboard Widgets](#)

Regular User Permissions


This page contains a list of all the different user permissions that are available in the system. You can define a fully customizable set of these permissions for each user role.

Permission Name	Description
-----------------	-------------

Application Access

Available Identity Providers	The list of the available identity providers for login. For more information, see: Authentication
Associated Identity Providers	The identity providers associated with the role. This determines the login options of the user.
Mobile web	Grants access to the mobile web interface of Verba to the user.
Dial-in interface	Allows the user to use the Dial-In recorder services. Dial-In recording has to be configured as a prerequisite. For more information, see the following article: Configuring the Verba Dial-in Recorder Service

Conversation Access

Scope	<p>Determines the range of conversations the user has access to:</p> <ul style="list-style-type: none"> • No Access to Conversations • Access Shared Only: the user can only access conversations that have been previously shared with them by other users. • Standard (User and group-based): the user can access the conversations that belong to it and the conversations of the other users that are in the groups the user is a supervisor of • Access All: the user can access every conversation in the system
Filtering Criteria	<p>Additional filtering criteria can be added by the  icon. These filters will restrict the access to the recorded conversations further above the setting selected at the Scope setting.</p>
Filtering Criteria Relationship Across Roles	When multiple roles are assigned to the same user, and more than one role has filtering criteria, then this setting determines whether AND or OR logic will be used between the filters depending to separate roles.
Unable to Access Conversations Older than	Denies access to calls for the user that are older than the specified amount of time (hours). Zero value means that there is no denial of access based on the age of conversations.
List Ongoing Conversations	Grants the user permission to view ongoing calls that are currently being recorded.
Agent View Scope	<p>Grants the user permission to view the desktop screens of agents that have been configured for screen capturing:</p> <ul style="list-style-type: none"> • 'On the phone' Screens Only: grants the user permission to view the desktop screens of agents currently in a conversation • 'On the phone' & Idle Screens: grants the user permission to view the desktop screens of agents regardless if the agent is talking or not
Real-Time Silent Monitoring of Ongoing Conversations	Grants the user permission to listen in (silent monitor) to ongoing calls that are currently being recorded.
View Conversation Details	Grants the user permission to view the details of a conversation in the search interface.
Play Conversation	Grants the user permission to play/view conversations from the search interface.
Preview Conversation	Grants the user permission to play/view a small portion of the conversations (from the beginning) only from the search interface. The default setting for voice/video/screen share recordings is up to 15 seconds, and for instant messages is up to 5 messages.

Require Access (Playback/View /Download) Reason	Specifies if the user has to provide a reason (free from text) before playing back, downloading, or viewing a conversation.
Use Participant Set	Grants the user permission to use the Participant Set feature.
Participant Set	Grants access to creating or sharing participant sets: <ul style="list-style-type: none"> • No access: user is not allowed to create or share participant sets. • Define Users: with this permission can create Participant Sets, but can't share them with other users. • Define & Share: users with this permission can create and share Participant Sets.
Access Secondary Recordings	Grants the user permission to access secondary recordings which are recorded by recording servers designated as secondary servers in a duplicate (2N) recording configuration. For more information, see How to make Secondary recordings visible .
Access Media-Only Recordings	Grants the user permission to access Media-Only recordings which are representing the audio segments when the advanced voice data model is used, primarily for trader voice integrations. For more information, see Data models .
Ad-hoc Transcode	Grants the user permission to use the ad-hoc transcoding feature in the player application for video and screen share recordings.
Phone Number Masking in Search	Specifies if the phone numbers are masked on the search screen for the user. For more information, see Customer Identification Data Masking .
Adjust Media Length	Defines the maximum value of the media adjustment configurable in the player when stitching voice recordings stored using the advanced data model (e.g. trader voice). For more information, see Configuring media stitching adjustment .

Group Supervisor Access Scope

These permissions are only effective for Group Supervisors. The system records group membership history and the Group Supervisors can access conversations of the Group Members according to the history by default. This means that if a Member was added to the Group later than the Group Supervisor, then the Group Supervisor will be able to access their conversations only from the time the Member was added to the Group. The Group Supervisor Access Scope permissions can be used to change this behavior.

All of these permissions have three possible values:

- According to Server Configuration (default)
- Yes
- No

The default server configuration settings can be changed in the Server Configuration under Web Application / Conversation Access Scope.

Access All Conversations of Current Members	If set to Yes, then the Group Supervisors can access all conversations of the currently active members regardless of when they were added to the group. Default: No.
Access Previous Conversations of Removed Members	If set to No, then the Group Supervisors will not be able to access the previous conversations of the members that have been already removed from the group. Default: Yes.
Access Previous Conversations After Lost Supervisory Status	If set to No, then the former Group Supervisor will not be able to access the previous conversations of the Group Members after lost the Supervisory status. Default: Yes.

Download / Export

Download a Conversation	Grants the user permission to download conversations from the storage to their own computer.
Conversation Export	Grants access to export recorded conversations: <ul style="list-style-type: none"> • No access: user is not allowed to export recorded conversations. • Media Files Only: users can export only media files. • Metadata Files Only: users can export only metadata files. • Both Media and Metadata Files: users can export media and metadata files as well.
Recurring Conversation Export	Grants the user permission to create recurring conversation export.
Conversations List Export	Grants the user permission to perform conversation list exports.
Customize Conversation Export Target Folder	Grants the user permission to change the export target folder for advanced export.
Sharing	
E-mail	Grants the user permission to share conversations visible to them via emailing an URL pointing to the conversation.
Share Conversations	Grants the user permission to share conversations via the web interface sharing page.
Access View Shared Items menu	Grants the user permission to view shared conversations shared with them via the web interface sharing page.
Allow Granting Playback Right	Grants the user permission to grant the following rights: <ul style="list-style-type: none"> • Playback right when sharing conversation through a label • Playback right when sharing conversations through a case • Investigator right for a group member
Define Label Sharing Expiration	Grants the user permission to define the expiration for the sharing of a label.
Override "Unable to Access Conversations Older than" in Label Sharing	Grants the user permission to override the "Unable to Access Conversations Older than" permission when sharing recorded conversations through labels.
Annotation	
Comment	Grants the user permission to add custom metadata to conversations.
Mark as Private	Grants the user permission to mark conversations as private. When a conversation is marked as private, nobody else (not even group supervisors and users with 'Access All' rights) in the system can access it except for the user who marked it.
Manual Labeling	Grants the user permission to manually apply labels to conversations (the scope of the users access to certain labels and conversations can be limited by other permissions).
Automatic Labeling from Search	Grants the user permission to setup an automatic labeling rule from the search page.
Data Retention	
Delete a Conversation	Grants the user permission to delete conversations with the exception of conversations that have been placed under Legal Hold .
Mute Recording	Grants the user permission to mute/pause recording.

Protect a Conversation	Grants the user permission to mark conversations as protected. When there are data retention policies in place that are configured to ignore protected conversations, the button associated with this permission can be used to protect conversations from the execution of those policies.
Enable Legal Hold	Grants the user permission to enable Legal Hold for labels. For more info on Legal hold, see the corresponding article .
Initiate Release from Legal Hold	Grants the user permission to initiate release of a legal hold for labels. This request still has to be approved by a user with the 'Approve Release from Legal Hold' permission for the legal hold to be successfully lifted.
Approve Release from Legal Hold	Grants the user permission to approve the release of legal hold from a label. The release first has to be initiated by a user with the 'Initiate Release from Legal Hold' permission.
Reporting	
Reporting	Grants the user access to the reporting features of Verba. For more information on reporting see the Reporting guide .
Dashboard	Grants the user permission to dashboards: <ul style="list-style-type: none"> • No Access: user is not allowed to access dashboards • Configure: user is allowed to create, update and delete her/his own dashboards • Configure and Share: user create, update, delete and share her/his own dashboards
Global Dashboard Administration	Grants the user permission to manage all dashboards in the system. The level of permission depends on your choice from the list. <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Quality Management	
Quality Management Agent	Enables the user as a Quality Management Agent. The user's conversations can be selected by Quality Management projects to be evaluated by Quality Management Evaluators. For more information on the Quality Management module of Verba, see the Quality Management guide .
View Own Scorecard	Grants the user permission to view her/his own scorecards.
Quality Management Evaluator	Enables the user as a Quality Management Evaluator. The user can evaluate Quality Management Agent users' conversations that are selected by a Quality Management project. For more information on the Quality Management module of Verba, see the Quality Management guide .
Add Conversations to Evaluation Projects	Grants the user permission to manually add recorded conversations to an evaluation project.
Remove Conversations from Evaluation Projects	Grants the user permission to manually remove recorded conversations from an evaluation project.
Speech Analytics	
Phonetic Index Conversations	Allows speech indexing of conversations associated with the user.
Speech Search	Grants the user permission to the speech search features of the search interface.

Transcribe Conversations (Built-in)	Allows transcribing of conversations, associated with the user, with the Verint engine.
Transcribe Conversations (Advanced)	Allows transcribing of conversations, associated with the user, with the advanced Verint engine.
Transcribe Conversations (3rd Party)	Allows transcribing of conversations, associated with the user, with the 3rd party engines.
Communication Policies	
Ethical Wall User	Allows configuring communication policies for the user.
Customization	
Personalize Conversation List Layout	Grants the user permission to modify of Search Layout on the Search page.

Administrative Permissions

Permission Name	Description
User Administration	
Users	<p>Grants the user permission to manage user settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Groups	<p>Grants the user permission to manage group settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Group Membership Administration	Grants the user permission to manage group membership settings in the system.
Extensions	<p>Grants the user permission to manage extension settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete

Recording Rules	<p>Grants the user permission to manage recording rules in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Managed Users/Groups /Extensions	<p>Grants group administrator users permission to manage the settings of users in the groups they are administrators in. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Roles	<p>Grants the user permission to manage user role settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
AD Profiles	<p>Grants the user permission to manage Active Directory Synchronization profile settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Identity Providers	<p>Grants the user permission to manage identity provider settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Bulk User Extension Update	Grants the user permission to use the bulk user and extension update feature.
Bulk User Import	Grants the user permission to use the bulk user import feature.
Group CSV Import	Grants the user permission to use the CSV file based group import feature.
VoH/ViQ Incoming Call Rules	<p>Grants the user permission to manage video on hold and video in queue incoming call rule settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete

VoH/ViQ Media Files	<p>Grants the user permission to manage video on hold and video in queue media file settings in the system. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
---------------------	---

Security

Search Audit Log	Grants the user permission to view and search the system audit log.
------------------	---

Alert Management	<p>Grants the user access to the Alert Management page. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update
------------------	---

Audit Log Alerts	<p>Grants the user access to the Audit Log Alerts page. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
------------------	---

Certificates	<p>Grants the user access to the certificate management page. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Create
--------------	---

API Keys	<p>Grants the user access to the API key management page. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
----------	---

Session Monitor	Grants the user access to the session monitor feature to review current web interface access sessions.
-----------------	--

Customizations

Metadata Templates	<p>Grants the user permission to manage metadata templates. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
--------------------	---

Automatic Labeling Rules	Grants the user permission to create and manage automatic labeling rules.
--------------------------	---

Default Conversation List Layout	<p>Grants the user permission to manage the default conversation list layout of the search interface. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update
Data Management	
Storage Targets	<p>Grants the user permission to manage storage targets. For more information, see Storage and export targets. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Data Processor	<p>Grants the user permission to manage data processors. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Import Source	<p>Grants the user permission to manage import sources. For more information, see Import sources. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Retention Policies	<p>Grants the user permission to manage data retention policies. For more information, see Data management policies. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Conversation Import	Grants the user permission to import conversations to the system.
Conversation Export	<p>Grants the user permission to export conversations from the system:</p> <ul style="list-style-type: none"> • Media Files Only: the user is only allowed to export media files • Metadata Files Only: the user is only allowed to export metadata • Both Media and Metadata Files: the user is only allowed to export both media files and metadata <p>For more information, see Export.</p>
Recurring Conversation Export	Grants the user permission to create recurring conversation export.
List User Exports	Grants the user permission to list other user's exports.
Operation and Maintenance	

Server Configuration	<p>Grants the user permission to server configuration. This includes the configuration of all Verba Nodes. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update
Site Configuration	<p>Grants the user permission to manage sites. For more information, see Sites. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
License	<p>Grants the user permission to manage Verba Licenses. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update
Database Monitoring	Grants the user access to the database monitoring features of the web interface accessible from the System menu.
Background Task Monitoring	Grants the user access to the background task monitoring features accessible from the System menu.
Collect Configuration and Logs	Grants the user access to the configuration and log collection feature accessible from the System menu.
Request Server Certificate	Grants the user access to the server certificate request feature accessible from the System menu.
Multi-tenant	
Multi-Tenant Administrator	Grants the user access to the multi-tenant deployment-specific configuration settings of Verba. This is only available in multi-tenant deployments.
Quality Management	
Quality Management Administrator	Grants the user permission to manage quality management module including creating and maintaining quality management projects and forms.
Speech Analytics	
Speech Analytics Administrator	Grants the user permission to administer speech indexing of conversations to allow users with the 'Speech Search' permission to search for phrases in audio conversations.
Communication Policies	
Communication Policies	<p>Grants the user permission to communication policies. For more information, see Communication Policies. The level of permission depends on your choice from the list.</p> <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete

Policy Validator	Grants the user access to the communication policy validator feature.
Audit Log	Grants the user access to the communication policy audit log feature.
Authorization Request	
Workflow Configuration	Grants the user permission to authorization requests. For more information, see Approval Workflows . The level of permission depends on your choice from the list. <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete
Announcement	
Announcement Audit Log	Grants the user access to the announcement audit log feature.
Announcement Whitelist	Grants the user permission to announcement whitelists. For more information, see Announcement whitelist . The level of permission depends on your choice from the list. <ul style="list-style-type: none"> • Read Only • Read, Update • Read, Update, Delete • Read, Update, Create • Read, Update, Create, Delete

Dashboard Widgets

Grants the user permission to the selected widget types in the system. By selecting **All**, all types of widgets will be accessible for the user.

- [Regular User Permissions](#)
 - [Application Access](#)
 - [Conversation Access](#)
 - [Group Supervisor Access Scope](#)
 - [Download / Export](#)
 - [Sharing](#)
 - [Annotation](#)
 - [Data Retention](#)
 - [Reporting](#)
 - [Quality Management](#)
 - [Speech Analytics](#)
 - [Communication Policies](#)
 - [Customization](#)
- [Administrative Permissions](#)
 - [User Administration](#)
 - [Security](#)
 - [Customizations](#)
 - [Data Management](#)
 - [Operation and Maintenance](#)
 - [Multi-tenant](#)
 - [Quality Management](#)
 - [Speech Analytics](#)
 - [Communication Policies](#)

- [Authorization Request](#)
- [Announcement](#)
- [Dashboard Widgets](#)

Visibility of functions and conversations

Based on the configured user roles, groups and extensions the system calculates what functions and conversations a user can see in the system when they login to the web interface.

Functions available for a user

Each user will see a different set of functions on the web interface based on their [user roles](#) configuration.


These rights include Playback, Download, Delete rights [and more](#).

Conversations visible for a user

The system calculates a restricted set of conversations on every search based on User, Group and Extension configurations.

These are the factors that define call visibility of a user:

Visibility factor	Description
User validity period	Only calls within the Users Valid From and Valid To time period will be visible for the User
User visibility window	The visibility of a user can be restricted to calls only in the last X hours using the "Unable to access calls older than" field on the User Configuration page
Extension assignments	The user will see calls for a phone Extension during the time period set under the Extension assigned to the User . Users can have multiple extensions.
Group supervisor rights	The user will see all calls of Group members of every group where the user is promoted to Group Supervisor . The historical scope of the calls can be configured with the Group Supervisor Access Scope permissions.
Group membership history	A Group Supervisor will see only calls recorded for the duration the supervisor rights are set for a supervisor. Moreover only those member calls will be seen, that came in during the membership period of the user. These periods can be manually modified on the Group Membership History page.
Access All rights	Users whose User Permission Scope is Access All can see all conversations in the system
Access extension with Labels	Labels can be configured in a way that they extend the visibility of calls to other users
Access extension with Cases	Cases can be configured in a way that they extend the visibility of calls to other users
Approval workflows	Users can request and be granted access to conversations through Approval Workflows

 The system keeps an [audit log](#) of every action of every user for security purposes. This audit log is available to users with System Administrator rights.

How to make Secondary recordings visible

AVAILABLE IN VERBA 8.5 AND LATER

It's possible to configure two recorders in Verba to make two exactly same copies from the recordable media at two different locations for redundancy and security purposes.

However, when users see two records for each call/conversation it is confusing. For this, we created the term 'secondary recorded media' which refers to the secondary copy of the media files.

By default, only the Verba Administrator user can see the secondary recordings.

How to enable the Secondary Recordings feature:

Step 1 - Go to '**Configuration/Verba Servers**' and select your Media Repository server.

Step 2 - Select '**Change Configuration Settings**' and navigate to '**Web Application / Secondary Recording Servers**'

Step 3 - Change the value of '**Enable Secondary Recording Servers:**' to **Yes**.


- ▶ Network
- ▶ Password Policy
- ▶ User Lockout Policy
- ▲ Authentication
 - ▶ Available Authentication Modes
 - ▶ Single Sign-On
- ▶ Reporting
- ▶ Active Directory Synchronization
- ▶ Media Utility Service
- ▶ Lync Recording Announcement
- ▶ HTTP Business API
- ▶ Conference Invitation
- ▶ Provisioning API
- ▲ Secondary Recording Servers
 - Enable Secondary Recording Servers: Yes
 - Recording Service IDs to be Linked:
 - Maximum Difference in Start Time (sec): 3600

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute Selected Tasks** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Step 6 - Log in to the server and restart the **Verba Web Application service**.

How to set Recording Servers as secondary

Step 1 - Go to '**Administration/Verba Servers**' and select your Recording Server.

Step 2 - Select '**Change Configuration Settings**' tab.


Step 3 - Set the **Passive Recorder->Basics->Secondary Recording Server** setting to **Yes**.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute Selected Tasks** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please **click here** .

How to enable users to see Secondary Recordings:

Step 1 - Go to '**Administration/Roles**'.

Step 2 - Create a new role or edit your previously created role for the user/group you would like to enable this feature.

Step 3 - On the '**Role Configuration**' page find '**Conversation Access**' -> '**Access Secondary Recordings**' and check the checkbox then save your changes at the bottom of the page.

Access Secondary Recordings

How to watch and play back Secondary Recordings on the Search page:

You need to complete the previous two sections to be able to see and playback your Secondary Recording on the Search page.

You will see a new scope called **Secondary Records** on the left side of the search view inside the **Advanced Search Options**.



Search



<saved query name>



Basic Search Options



Interval



2018.12.11 00:00

2019.02.11 23:59

Phone Number (From or To Party)



Enter number or URI...



User



Enter user name...



Search conference participants

Label



Enter label name...

Advanced Search Options (*)



Display results according to timezone

GMT+00:00 - GMT - Greenwich Mean Time



Scope

Archived Conversations

Secondary Records



Media-Only Records

Users

- [Find and List Users](#)
- [User Configuration](#)
- [User-Group Association](#)
- [User Group Membership History](#)
- [User Default Call List Layout](#)
- [Custom User Fields](#)
- [Built-in user accounts](#)

Find and List Users

Users represent people who can log in to the recording system. Users can belong to Groups and have associated Extensions. The web interface hides the features the logged in user does not have the right to access.

Only system administrators and group administrators have access to user management. The User List is available by clicking on the **Administration / Users** submenu.


Find and list users

System administrators have full control. Group administrators can only manage users that are part of their group.

This page displays a list which contains all users with their most important data.

Find and List Users

[Add New User](#)
[Manage Custom Fields](#)
[Show Expired Users](#)

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

Display Name begins with [Find](#)

Display Name	Login ID	Extensions	Groups	Roles	Authorization Workflow	Valid From	Type
Carrie Reid	carrie	carrie@verba.com	Default Customer Services Group US Legal - PiedPiper Team	Standard User Approval Workflow Managers		Jan 1, 1970	Standard
Chad Gray	chad	chad@verba.com	Default Tech Group US Legal - Hooli Team	Standard User		Jan 1, 1970	Standard
Corey Mendoza	corey	corey@verba.com	Default Administration Group US Legal - PiedPiper Team	Standard User		Jan 1, 1970	Standard
Jerry Jones	jerry	1026 1514 jerry@verba.com	Default Customer Services Group	Standard User		Jan 1, 1970	Standard
Kenneth Franklin	kenneth	1945 kenneth@verba.com	Default Tech Group US Legal - Hooli Team	Standard User	External Investigator access	Jan 1, 1970	Standard
Michael Cohen	michael	1914 michael@verba.com	Default Administration Group Global Compliance Office ...	Standard User Quality Management Agent		Jan 1, 1970	Standard
Sharon Harrington	sharon	1949 sharon@verba.com	Default Administration Group US Billing	Standard User Quality Management Agent		Jan 1, 1970	Standard
Sue Mathis	sue	1010 1932 sue@verba.com	Default Tech Group US Legal - Hooli Team	Standard User Quality Management Agent		Jan 1, 1970	Standard

- [Add New User](#)
- [Manage Custom Fields](#)
- [Show / Hide Expired Users](#)

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 realm 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 alphanumeric 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.	<p>Required field.</p> <p>Minimum length: 5*</p> <p>Maximum length: 32</p> <p>Password phrase must include at least one numeric character!**</p> <p>Password phrase must include at least one special character!**</p> <p>Password phrase must include at least one uppercase letter!**</p> <p>The field is case sensitive.</p> <p>*The minimum number of required password length can be configured.</p> <p>**These settings are optional and can be configured globally.</p> <p>For more information refer to Configuration settings for Verba Web Application.</p>
	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	Indicates whether the user is locked or not. If a user is locked, she/he is unable to use the Verba Web Application. 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 .	-
	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 Upload 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 Export 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. The audio file can be selected from the dropdown. ***	-
	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.***	-
	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

*** To add custom notification prompts, refer to the [Installing and configuring Microsoft Teams custom announcement](#) article 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 - Pied Piper 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

User-Group Association

Every user has to be associated with at least one group, because data, like comment templates, are configured through groups. When inserting a new user, the user is automatically associated with the Default group. After creating a new user, administrators are able to change group associations for the user. This page is also used for granting group administrator and/or group supervisor privileges to the user. Group assignment for users can be found on the 'Group Assignment' tab of the user configuration page.

Show direct groups only Show indirect groups too

Selected Groups

<input type="checkbox"/>	Group Name	Member	Supervisor	Investigator	Administrator	Manager	Primary Group
<input type="checkbox"/>	Customer Services Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
<input type="checkbox"/>	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="radio"/>
<input type="checkbox"/>	US Legal - PledPiper Team	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>

Adding a user to a group

In order to add a user to a group, select the desired group by ticking the checkbox on the left side of the row in the lower pane (where the available, not selected groups are listed), then press the **'Add Selected'** button.

Removing a user from a group

In order to remove a user from a group, you have to put the desired group to the Available Groups list (lower panel) from the Selected Groups list (upper pane). Select the desired group by ticking the checkbox on the left side of the row in the upper pane (where the selected groups are listed), then press the - button. If only one group is selected for a user, it cannot be removed.

Granting Group Administrator right

To grant group administrator right to a user in a selected group, simply check in the **Group Administrator Right** checkbox in the desired row. For further information on group administrator right, refer to [Group Administrator](#) level on page 1.

Granting Group Supervisor right

To grant group supervisor right to a user in a selected group, simply check in the **Group Supervisor Right** checkbox in the desired row. For further information on group supervisor right, refer to [Group Supervisor](#) level on page 1.

Granting group membership

To grant group member right to a user in a selected group, simply check in the **Group Member Right** checkbox in the desired row. By granting group membership, the group supervisors are allowed to view the calls of the member. If you do not grant the group membership to a user, than group supervisor will not able to view the calls of that user. Group administrators and supervisors do not have to be group members.

Selecting the primary group

Every user has to be assigned to a primary group. The primary group determines:

- Verba XML Service for Cisco IP phones uses the comment template of the primary group (to avoid complexity) for each user.

In order to select the primary group, select the desired radio button in the **Selected Groups** list.

If all modifications are done, press the **Save** button.

The user-group linking is timeframe based, which determines for a group supervisor the available calls of the group members. The validation from field on user configuration pane determines the starting date of the group administrator privilege, which enables to grant group administrator privileges for a new user too by setting the validation from field to an appropriate value. You can modify the validation dates of a user group assignment, for more information, check the next topic.

User Group Membership History

Group supervisors are allowed to access calls linked to group members, but the validation date of the group supervisor controls this feature. Group supervisors are only able to see calls in their groups that were recorded after their group membership started ('Valid From' field).

This feature is also available from the **Group Configuration** page, for more information see [Group membership history](#).

In order to change the user group validation dates, system and group administrators are able to access **Group Membership History**. This page is available from the top right corner the user configuration page.

Group Membership History User Configuration (Carrie Reid (carrie))
User: Carrie Reid (carrie)

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

Group Name	User	Valid From	Valid Until	Member	Supervisor	Investigator	Administrator	Manager	Primary
Customer Services Group	Carrie Reid (carrie)	Jun 1, 2014 2:00:00 AM	Jan 1, 2099 1:00:00 AM	Yes	Yes	No	No	Yes	No
Default	Carrie Reid (carrie)	Jan 1, 1970 1:00:00 AM		Yes	No	No	No	No	Yes
US Legal - PiedPiper Team	Carrie Reid (carrie)	Jun 1, 2014 2:00:00 AM		Yes **	No	No	No	No	No

3 items found, displaying all items.
Export options: [Excel](#) | [RTF](#) | [PDF](#)

* Expired Group Membership
** Indirect Relationship

Changing existing user group assignment

In order to change an existing user group assignment, select the desired user group assignment row. The **Group Membership Configuration** page opens, where system and group administrators can modify the configuration settings.

If all modifications are done, press the **Save** button.

Group Membership Configuration Back to Previous Group Membership List

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

Group Membership Data

Group Name:

User:

Valid From:

Valid Until:

Primary:

Effective: Direct:

Member: Supervisor: Investigator: Administrator: Manager:

The Direct and Effective switches should be set the same except if the membership is inherited through a group-group membership.

[Save](#)

Creating new user group assignment

This feature is almost equivalent with the standard user group assignment functionality on the **Group Assignment** page. The only difference is that system and group administrators are able to set validation dates directly. In order to add a new user group assignment entry, click on the **Add New Group Membership** link on the top right corner of the **Group Membership Configuration** page.

If all fields are filled in, press the **Save** button.

Deleting a user group assignment

This feature is equivalent with the standard user group assignment functionality on the **Group Assignment** page. In order to delete a user group assignment entry, select the desired user group assignment for the given user and on the **Group Membership Configuration** page, press the **Delete** button.


User Default Call List Layout


Administrators can define the content of the default call list layout, which is automatically assigned to a new user.





The layout setting is available under the **Configuration / Conversation List Layout** menu.

The right pane contains the configured/selected fields and their order. The left pane contains the available, not selected fields.

Default Conversation List Layout Configuration

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



Selectable Columns		Position	Added Columns
<input type="checkbox"/> Location		<input type="checkbox"/> 1.	Labels
<input type="checkbox"/> End Cause		<input type="checkbox"/> 2.	Start Date
<input type="checkbox"/> Audio Codec		<input type="checkbox"/> 3.	Start Time
<input type="checkbox"/> Start DateTime		<input type="checkbox"/> 4.	Duration
<input type="checkbox"/> Start DateTime (GMT)		<input type="checkbox"/> 5.	From
<input type="checkbox"/> End DateTime		<input type="checkbox"/> 6.	From Info
<input type="checkbox"/> End DateTime (GMT)		<input type="checkbox"/> 7.	To
<input type="checkbox"/> Archive Status		<input type="checkbox"/> 8.	To Info
<input type="checkbox"/> From (Verba)		<input type="checkbox"/> 9.	Direction
<input type="checkbox"/> To (Verba)			
<input type="checkbox"/> End Date			
<input type="checkbox"/> End Time			
<input type="checkbox"/> File Format			

Adding a field to the default call list layout

In order to add a field, select the desired field by enabling the checkbox on the left side of the row in the left pane, then press the **>>** button.

Removing a field from the default call list layout

In order to remove a field, select the desired field by enabling the checkbox on the left side of the row in the right pane then press the **<<** button.

Changing field order

In order to change the order of the selected fields, select the desired field by enabling the checkbox on the left side of the row in the right pane, then click the **Up** button to move a field further up in the list or select the **Down** button to move it further down.

Applying your changes to existing users

In order to apply your changes to all existing users press the **Apply for All Users** button.

Custom User Fields

This feature allows configuring up to 10 custom user fields. Custom user fields are available for conversation search. Active Directory synchronization is able to automatically populate these fields. Custom user fields are also available at various part of the system including data retention, exporting, etc.

Configuring Custom User Fields

Step 1 - To access the custom user fields interface, navigate to **Administration -> Users**.

Step 2 - Select **manage Custom Fields** on the top right edge of the screen.

Step 3 - Check the **Enabled** checkbox and enter the field name.

Enabled	Field Name
<input checked="" type="checkbox"/>	<input type="text" value="objectGUID"/>
<input checked="" type="checkbox"/>	<input type="text" value="objectSid"/>
<input checked="" type="checkbox"/>	<input type="text" value="distinguishedName"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>

Step 4 - You can manually set/edit these values or automatically populate them using AD sync.

Manually set/edit the Custom User Fields

Step 1 - To manually set/edit the custom user fields navigate to **Administration / Users** and select the user you would like to edit.

Step 2 - The previously created custom user fields are stored under **Customizations**. The values can be set and modified here.

Automatic population of the Custom User Fields

Step 1 - To automatically populate the custom user fields using AD sync navigate to **Management Tools / Active Directory Synchronization**.

Step 2 - Select **Add New Active Directory Profile** on the top right edge of the screen. See [Active Directory synchronization](#) page for more information.

Step 3 - The previously created custom user fields are stored under **Synchronized LDAP Attributes Mapping**. The (case sensitive) values can be set and modified here. The entered value must match an AD user property attribute otherwise nothing will be imported.

Synchronized LDAP Attributes Mapping

Verba User Field LDAP Attribute

Display Name*

Login ID*

User Matching ID

If empty, the Login ID field will be used to match AD and Verba users.

E-mail Address

Location Attribute

Location

Will be used when the Location Attribute is not set up or the attribute is not filled in for a user in the AD.

Step 4 - After filling the form, press the **Test Connection** button to see what user attributes are going to be synchronized.

Step 5 - Once you are done, press the **Save** button to store the new profile under the **Administration -> Active Directory Synchronization** menu item. Select **Run Each Active Directory Profile Now** to run the synchronization.

Built-in user accounts

The system installs with built-in user accounts. Some of these accounts can be invalidated or restricted. The following table summarizes the information about these accounts.

Built-in User Account Name	Description	Roles	Can it be invalidated?	Can it be deleted?
Verba Administrator	This user account is created during install and required to set up the system and the first user(s)	Superuser	Yes	No
Verba System	This user account is created during install without any active role, it is used by the system to reference audit log entries related to system activities, etc. This user account cannot be managed through the UI.	-	No	No
Verba API User	This user account is created during install and required for the system to operate, certain components use this account to connect to the APIs, external applications can also use this account.	System Supervisor, System Administrator	No	No

Groups

- [Group List](#)
- [Group Details](#)
- [Group Membership History](#)
- [Group queries configuration](#)


Group List


Groups are essentially lists of Users. You can define Group supervisors who can see calls of Group members. Verba user group administration is available only for the administrator and the system administrators and the group administrators by selecting **Administration / Groups** submenu. The administrator and the system administrators have full control. The group administrators can only access those groups, which are linked to them and they have group administration privilege in those groups. The group administrators are only allowed to modify group data, they cannot add new groups or delete existing ones.

Find and list groups

You can use the search form below the title, to filter groups: just select your filter and click find.

Find and List Groups [Add New Group](#)

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

 Extension configuration should be applied on recording servers.
If you would like to apply the configuration now, please [click here](#).

Manual Groups Active Directory Synced Groups Authorization Groups ?

Group Name ▾ begins with ▾ Find

Group Name ⇅	Metadata Template ⇅	Authorization Workflow ⇅
Default	Default	

1 item found.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

To ensure consistency the system contains a group named Default, which cannot be deleted.

Group Details

- [Creating a group](#)
- [Assigning users](#)
 - [Adding a user to a group](#)
 - [Removing a user from a group](#)
 - [Granting group administrator right](#)
 - [Granting group supervisor right](#)
 - [Granting group manager right](#)
 - [Granting group membership](#)
 - [Selecting the primary group](#)
 - [Display indirect members](#)
- [Assigning Member Groups](#)
 - [Adding a member group to a group](#)
 - [Removing a member group from a group](#)
 - [Granting group administrator right](#)
 - [Granting group supervisor right](#)
 - [Granting group manager right](#)
 - [Granting group membership](#)
- [Assigning Parent Groups](#)
 - [Adding a parent group to a group](#)
 - [Removing a parent group from a group](#)
 - [Granting group administrator right](#)
 - [Granting group supervisor right](#)
 - [Granting group manager right](#)
 - [Granting group membership](#)
- [Privilege levels](#)
 - [Group administrator](#)
 - [Group supervisor](#)
 - [Group manager](#)
 - [Group investigator](#)
- [Modifying and deleting groups](#)

Groups are essentially lists of Users. You can define Group supervisors who can see calls of Group members.

Verba user group administration is available only for the administrator and the system administrators and the group administrators by selecting **Administration / Groups** submenu. The administrator and the system administrators have full control. The group administrators can only access those groups, which are linked to them and they have group administration privilege in those groups. The group administrators are only allowed to modify group data, they cannot add new groups or delete existing ones.

Creating a group

You can create new Verba group by clicking on the **Add New Group** link on the **Administration / Groups** page. After selecting the link, the following page is opened.

Group Configuration

[Add New Group](#)
[Back to Previous Group List](#)

Group Data
Assign Users
Member Groups
Parent Groups

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

⚠ Extension and Communication Policy configuration should be applied on recording servers. If you would like to apply the configuration now, please [click here](#).

?

Group Data

Enable Active Directory Synchronization

Group Name*

Metadata Template* Default ▼

Authorization Workflow --Choose-- ▼

Metadata Template Association

Cisco UCCX Template

Cloud9 Template

Default

Lync (Anywhere365) Template

Lync (Geomant CE) Template

Lync (Luware) Template

>>

<<

Playback Reasons

Save Delete

The following table describes the available fields:

Field Name	Description	Requirements
Group Name	Name of the group.	Required field. Minimum length: 3 Maximum length: 64 Must be unique in the system. Only alphanumeric characters are allowed in this field. Reserved name: Default
Metadata Template	The metadata template for the group. It contains the available metadata fields (including custom comment fields), that show up in web interface search results for each conversation.	-
Logo	Optional logo image can be attached to a group. The logo image will be displayed in the header of Verba Web Application for every user in the group. The logo will be also displayed in report headers generated by group members. If the user is a member of more than one group, the primary group settings will be applied. In order to select a logo image, press the Choose Logo button. In the window that opens, you can see the uploaded logo images. Simply click on the name of the file in the first column to select an image.	-

Fill in the form and press the **Save** button to save group data into the database.

Assigning users

On the **Group Configuration** page, administrators can assign or remove users to/from a given group. Simply click on the **Assign Users** tab to display the configuration page.

In the list, click on the magnifier icon to go to **User Configuration** and check the group membership of a given user.

Group Configuration Add New Group
Group Queries
Group Membership History
Back to Previous Group List

Tech Group

Group Data **Assign Users** Member Groups Parent Groups

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

⚠ Extension and Communication Policy configuration should be applied on recording servers. If you would like to apply the configuration now, please [click here](#).

Show direct members only Show indirect members too

Found 3 members, listing all.

Search and Add Users

Current Members of Tech Group

User Name	Member	Supervisor	Investigator	Administrator	Manager	Primary Group	
Chad Gray (chad)	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Kenneth Franklin (kenneth)	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sue Mathis (sue)	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

[Save](#)

Adding a user to a group

In order to add a user to a group, use the Search field on the top of the list to find the user and click on it in the list that pops up.

Removing a user from a group

In order to remove a user from a group, click on the trash icon next to the user's name in the list.

Granting group administrator right

To grant the group administration right to a user in the group, simply check the **Group Administrator Right** checkbox in the desired row. For further information on group administrator right, refer to [privilege levels](#).

Granting group supervisor right

To grant the group supervisor right to a user in the group, simply check the **Group Supervisor Right** checkbox in the desired row. For further information on group supervisor right, refer to [privilege levels](#).

Granting group manager right

To grant the group supervisor right to a user in the group, simply check the **Group Manager Right** checkbox in the desired row. For further information on group supervisor right, refer to [privilege levels](#).

Granting group membership

To grant group member right to a user in a selected group, simply check the **Group Member Right** checkbox in the desired row. By granting group membership, the group supervisors are allowed to view the calls of the member. If you do not grant the group membership to a user, then group supervisors will not be able to view the calls of that user. Group administrators and supervisors do not have to be group members.

Selecting the primary group

Every user has to have a primary group. The primary group determines: Verba XML Service for Cisco IP phones uses the comment template of the primary group (to avoid complexity) for each user.

In order to select the primary group, select the desired radio button in the list.

When all modifications are done, press the **Save** button.

Display indirect members

To show the indirect members of the group just simply select the **Show indirect members too** radio button. The list will show every related user which is a member of a member group.

Assigning Member Groups

On the **Group Configuration** page, administrators are able to assign or remove child groups to/from a given group. Simply click on the **Member Groups** tab to display the configuration page.

The screenshot shows the 'Group Configuration' page for 'Tech Group'. It features a navigation bar with tabs for 'Group Data', 'Assign Users', 'Member Groups' (which is active), and 'Parent Groups'. On the right side, there are links for 'Add New Group', 'Group Queries', 'Group Membership History', and 'Back to Previous Group List'. Below the navigation, there are two yellow warning boxes: one about email alert settings and another about Extension and Communication Policy configuration. There are two radio buttons for 'Show direct members only' (selected) and 'Show indirect members too'. Below this, it says 'Found 0 members, listing all.' and there is a search field labeled 'Search and Add Groups' with the placeholder 'Enter group name...'. At the bottom, there is a table titled 'Current Members of Tech Group' with columns for 'Group Name', 'Member', 'Supervisor', 'Investigator', 'Administrator', and 'Manager'. A 'Save' button is located below the table.

Adding a member group to a group

In order to add a user to a group, use the Search field on the top of the list to find the user and click on it in the list that pops up.

Removing a member group from a group

In order to remove a user from a group, click on the trash icon next to the user's name in the list.

Granting group administrator right

To grant the group administration right to a group, simply check the **Group Administrator Right** checkbox in the desired row. For further information on group administrator rights, refer to [privilege levels](#).

Every member of the child group will get group administrator permission.

Granting group supervisor right

To grant the group supervisor right to a group, simply check the **Group Supervisor Right** checkbox in the desired row. For further information on group supervisor rights, refer to [privilege levels](#).

Every member of the child group will get group supervisor permission.

Granting group manager right

To grant the group manager right to a group, simply check the **Group Manager Right** checkbox in the desired row. For further information on group manager rights, refer to [privilege levels](#).

Every member of the child group will get group manager permission.

Granting group membership

To grant group member right to a group, simply check the **Group Member Right** checkbox in the desired row. By granting group membership, the group supervisors are allowed to view the calls of the member. If you do not grant the group membership to a user, then group supervisors will not be able to view the calls of that user. Group administrators and supervisors do not have to be group members. Every member of the child group will become the group member of the group.

Assigning Parent Groups

On the **Group Configuration** page, administrators are able to assign or remove parent groups to/from a given group. Simply click on the **Parent Groups** tab to display the configuration page.

Group Configuration [Add New Group](#)
[Group Queries](#)
[Group Membership History](#)
[Back to Previous Group List](#)

Tech Group

[Group Data](#) [Assign Users](#) [Member Groups](#) [Parent Groups](#)

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

⚠ Extension and Communication Policy configuration should be applied on recording servers.
If you would like to apply the configuration now, please [click here](#).

Show direct parents only Show indirect parents too

Found 0 parents, listing all.

Search and Add Groups

Current Parents of Tech Group

Group Name	Member	Supervisor	Investigator	Administrator	Manager
------------	--------	------------	--------------	---------------	---------

[Save](#)

Adding a parent group to a group

In order to add a user to a group, use the Search field on the top of the list to find the user and click on it in the list that pops up.

Removing a parent group from a group

In order to remove a user from a group, click on the trash icon next to the user's name in the list.

Granting group administrator right

To grant the group administration right to a group, simply check the **Group Administrator Right** checkbox in the desired row. For further information on group administrator right, refer to [privilege levels](#).

Every member of the group will get group administrator permission on the added parent group.

Granting group supervisor right

To grant the group supervisor right to a group, simply check the **Group Supervisor Right** checkbox in the desired row. For further information on group supervisor right, refer to [privilege levels](#).

Every member of the group will get group supervisor permission on the added parent group.

Granting group manager right

To grant the group manager right to a group, simply check the **Group Manager Right** checkbox in the desired row. For further information on group manager right, refer to [privilege levels](#).

Every member of the group will get group manager permission on the added parent group.

Granting group membership

To grant group member right to a group, simply check the **Group Member Right** checkbox in the desired row. By granting group membership, the group supervisors are allowed to view the calls of the member. If you do not grant the group membership to a user, then group supervisors will not be able to view the calls of that user. Group administrators and supervisors do not have to be group members.

Every member of the child group will become the group member of the parent group.

Privilege levels

Group administrator

The group administrator has administrative privileges to the group and to the group members.

Group supervisor

The group supervisor has access to the conversations of all group members.

Group manager

The group manager is for the compliance workflows. The group manager is the first approver when a group member creates a workflow.

Group investigator

The group investigator gives playback rights to the conversations of all group members.

Modifying and deleting groups

To edit group data, you have to click on the desired row of the table showing configured Verba groups. After clicking on the row, a new page opens automatically.

To have changes take effect, push the **Save** button. All conditions, which are described in the previous articles, have to be met.

You can delete the group by pressing the **Delete** button. Deletion of a group is only enabled if no users are associated with the group.

Group Membership History

Group supervisors are allowed to access calls associated with group members, but the validation date of the group supervisor limits this feature. This feature is also available from the User Configuration page.

In order to change the user group validation dates, system and group administrators can access Group Membership History. This page is available from the top right corner the group configuration page.

Group Membership History Group Configuration (Test)

Group: Test

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

Group Name	User	Valid From	Valid Until	Member	Supervisor	Investigator	Administrator	Manager	Primary
Test	Verba Administrator (Administrator)	Oct 16, 2017 12:06:34 PM		Yes	No	No	No	No	No
Test	Verba Api User (verbaapi)	Oct 16, 2017 12:06:34 PM		Yes	No	No	No	No	No

2 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

* Expired Group Membership
** Indirect Relationship

Changing existing user group assignment

In order to change an existing user group assignment, select the desired user group assignment row. The **Group Membership Configuration** page opens, where the system and group administrators can modify the configuration settings.

Once all modifications are done, press the **Save** button.

Group Configuration Add New Group
Group Queries
Group Membership History
Back to Previous Group List

Test

[Group Data](#) | [Assign Users](#) | [Member Groups](#) | [Parent Groups](#)

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

⚠ Extension configuration should be applied on recording servers.
If you would like to apply the configuration now, please [click here](#).

Show direct members only Show indirect members too

Found 2 members, listing all.

Search and Add Users

Current Members of Test							
User Name	Member	Supervisor	Investigator	Administrator	Manager	Primary Group	
<input type="checkbox"/> Verba Administrator (Administrator)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Verba Api User (verbaapi)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Save](#)

Creating new user group assignment

This feature is almost the same as the standard user group assignment functionality on the User Assignment page. The only difference is that, system and group administrators are able to set validation dates directly. In order to add a new user group assignment entry, click on the **Add New Group Membership** link on the top right corner of the **Group Membership Configuration** page.

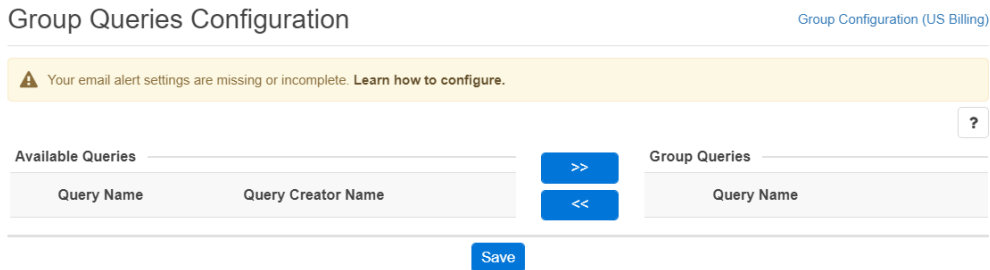
Once all fields are filled in, press the **Save** button.


Deleting a user group assignment


This feature is the same as the standard user group assignment functionality on the **Group Assignment** page. In order to delete a user group assignment entry, select the desired user group assignment for the given group and on the **Group Membership Configuration** page, press the **Delete** button.

Group queries configuration

This feature enables the sharing of saved queries to the members of a given group. Administrators can choose from all saved queries, independently from the creator of the query. The group query configuration page is available from the group configuration page by selecting **Group Queries** link on the top left corner.

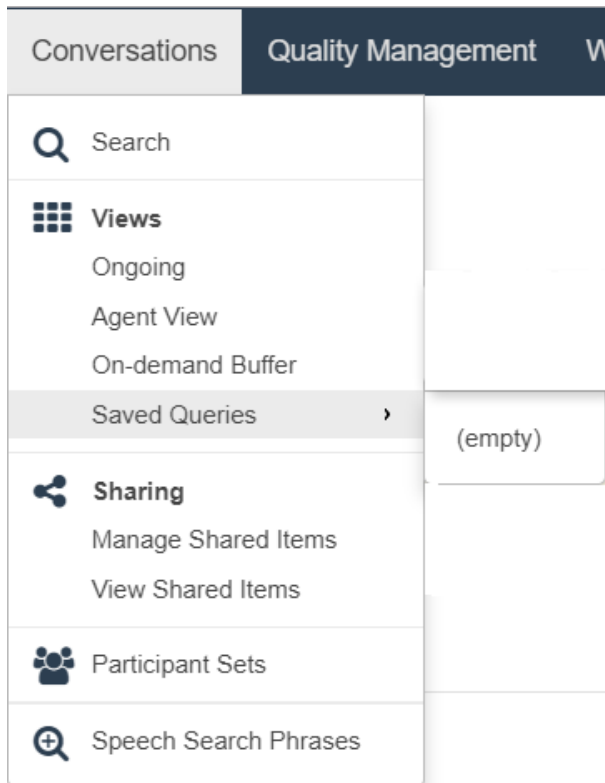


You can add a query to the group by selecting the appropriate item on the left and pressing the  button.

You can remove a query from the group by selecting the appropriate item on the right and selecting the  button. The query will be not deleted, it will only be unlinked from the group.

In order to save the configuration changes, simply press the **Save** button.

The changes only take effect after the members of the given group log out and log in again to the system. The queries configured for the group are listed under **Calls / Saved Queries** menu item, just like other personal queries. You can differentiate group based queries because these items are separated from personal queries by a line.



Recording rules

- [Extension list](#) — Extensions are phone numbers or addresses configured with recording modes and user association (the basis of access control).
- [Extension details](#)
- [Recording modes](#)
- [Conversation direction and modality support](#)
- [Modality and recorded platform support matrix](#)
- [Selective recording rule configuration](#)
- [Administration of recorded extensions for Cisco network-based recording](#)
- [Administration of recorded extensions for Passive Recorder](#)
- [Correcting user-extension assignments](#)
- [Microsoft Teams selective recording settings](#)
- [Relay-only configuration for Microsoft SfB - Lync](#)
- [Shared line recording configuration with Cisco recording](#)

Extension list


Extensions are phone numbers or addresses configured with recording modes and user association (the basis of access control).

Find and list extensions

Navigate to **User / Extensions**. You can use the search form on the top of the page to filter extensions: just select your filter and click Find.

[Add New Extension](#)
[View Last Conversations by Extensions](#)
[Apply Extension Configuration](#)
[Apply Communication Policy Configuration](#)
[Show Expired Extensions](#)

Find and List Extensions

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

Filter by Modality

Extension begins with

Extension	User name (login)	Description	Type	Recording Mode	Modalities
1010	Sue Mathis (sue)		Number/Address	On-demand	Voice
1026	Jerry Jones (jerry)		Number/Address	Full	Voice
1222	Thomas Powell (thomas)		Number/Address	Full	
1514	Jerry Jones (jerry)		Number/Address	Full	
1848	Sharon Harrington (sharon)		Number/Address	Full	
1914	Michael Cohen (michael)		Number/Address	Full	
1918	Wesley Mack (wesley)		Number/Address	Full	
1939	Sue Mathis (sue)		Number/Address	Full	
1945	Kenneth Franklin (kenneth)		Number/Address	Full	
chad@verba.com	Chad Gray (chad)		Number/Address	Full	
corey@verba.com	Corey Mendoza (corey)		Number/Address	Full	
jerry@verba.com	Jerry Jones (jerry)		Number/Address	Full	
kenneth@verba.com	Kenneth Franklin (kenneth)		Number/Address	Full	
michael@verba.com	Michael Cohen (michael)		Number/Address	Full	
sharon@verba.com	Sharon Harrington (sharon)		Number/Address	Full	
sue@verba.com	Sue Mathis (sue)		Number/Address	Full	
thomas@verba.com	Thomas Powell (thomas)		Number/Address	Full	
wesley@verba.com	Wesley Mack (wesley)		Number/Address	Full	

18 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Export Options

The system allows users to export the list of configured extensions.

The RTF and PDF export options will export the list of configured extensions, please note that these options will only display the visible column headers, as seen on the Find and list extensions screen.

AVAILABLE IN VERSION 9.6.13 OR LATER

The Excel export option will export all configured Extension values, including all configured values within the Extension Configuration screen,

Extension details

Extension configuration provides the following functions:

Defining what to record and how	<p>If the recording system has to be configured to record selected extensions / phone numbers / SIP URIs only, administrators have to define the extension numbers. By default, the system records only configured extensions on a given Verba Recording Server. For more information on understanding the various recording modes, refer to the Verba Deployment Guide.</p> <p>Only the users with system administrator rights have access to extension configuration. The page is available by clicking on the Users / Extensions submenu. The group administrators can only access those phone numbers, which are linked to users from those groups which they administer.</p>
Extension Assignment to Users	<p>Extension Assignment enables administrators to link phone numbers / extensions / SIP URIs to Verba users. Using this feature, Verba can link Verba users to calls and users can search for recorded calls using these parameters / names. This feature is useful when the communication system does not provide name fields for the recorder.</p> <p>In order to use Verba special features like making calls private, XML-based services, on-demand recording, etc. system administrators have to map Verba users to phone numbers / extensions / SIP URIs. Through user-extension assignment, Verba can apply linking information for the above-mentioned services.</p>

Adding an extension

The extensions can be line numbers, SIP URIs or User IDs in the case of turret recording. In the case of high number extensions, instead of adding all of them manually, the [Active Directory synchronization](#) can be used.

Step 1 - Go to the **Users \ Extensions** menu.

Step 2 - Click on the **Add New Extension** link in the upper right corner.

Step 3 - Provide the line number or the SIP URI (without the "sip:") in the **Extension** field. This has to be exactly the same as what configured on the PBX side.

- In the case of **turret recording**, the User/Agent ID has to be provided.
- In the case of **Microsoft Teams**, the User Object ID has to be provided.


Step 4 - Provide a Verba user in the **User** field. Recorded conversations will be assigned to Verba users based on this setting. The Communication Policies also identify the Verba users in the communication sessions based on this setting. For more information, see [Adding a New User](#).

Step 5 (Turret and MS Teams only) - Set the **Type** setting to **User/Agent ID**.

Step 6 - Set the recording settings according to the requirements under the **Recording Settings** section.

Step 7 - Click **Save**.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Extension configuration details

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

⚠ Extension configuration should be applied on recording servers.
If you would like to apply the configuration now, please [click here](#).

⚠ Synchronization is enabled so the synchronized fields are not editable.



Extension Data

Synchronized by Active Directory: BASICAD

Extension* 000-111-2-10164
Phone number (*1234*) or address (*user@company.com*)

User testuser_1016 (testuser_1016)

If a user is missing from the list, please verify the Valid Until and Valid From fields of that user.

Type* Number/Address

Update user information on existing conversations
Apply on: new conversations unassigned conversations all conversations
 Update conversations within the user's validity period only

Description

Recording Settings

Recording Mode* Full

Voice

Instant Messaging

Video

Desktop Screen

Screen & Application Share

Whiteboard

Poll / Q&A

File Share

Support of modalities depends on the recorded platform, more information [here](#).

Recorded Directions All
 Internal PSTN In PSTN Out External Federated In Federated Out Conference

Record Calls Answered by 3rd Party
 All Forwarded Transferred Team Call Delegated

Only available for SfB/Lync recording

Data Sources

Record Every Platform

Recorded Platforms
ACME SIPREC
Analogue
Avaya DMCC/MR
Bosch Telex
BroadSoft SIPREC
Cisco CUBE
...
[>>] [<<]

Import from Every Source

Import Sources
[>>] [<<]

Selective Recording Settings

Sampling Rate %

Record only on the selected Verba Servers

Verba Server
LOADTESTSQL.VERBATEST.LOCAL
[>>] [<<]

Valid From

Valid Until

- ▶ Avaya Recorder Specific Settings _____
- ▶ Dial-in Recorder Specific Settings _____
- ▶ Cisco Unified Communications Manager Express Specific Settings _____

Creation Date: Oct 11, 2017 1:33:35 PM
 Created By: Verba Administrator (Administrator)
 Last Modification Date:
 Last Modified By:
[View Change History](#)

This shows the basic configuration options for the conversation modality and direction definition. To enable the advanced ruleset, in the menu navigate to **System / Verba Servers / Select the Media Repository server / Web Application / Miscellaneous / Enable Modality Based Direction Rules / Enable Contact Center Direction Rules**

With this advanced rule set, it is possible to define which direction should be recorded for each modality.

Synchronized by Active Directory

Extension*

Phone number (1234) or address (user@company.com)

User

If a user is missing from the list, please verify the Valid Until and Valid From fields of that user:

Type*

Apply on: new conversations unassigned conversations all conversations

Update conversations within the user's validity period only

Update user information on existing conversations

User information cannot be updated if there is no associated User to the Extension.

Description

Recording Mode*

Recording Rule

For Cisco J56P based selective recording integrations only

	All	Internal	PSTN In	PSTN Out	External	Federated In	Federated Out	Contact Center In	Contact Center Out	Conference
Voice	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Instant Messaging	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Desktop Screen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Screen & Application Share	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Whiteboard	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poll / Q&A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File Share	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Support of modalities depends on the recorded platform, more information [here](#)

All
 Forwarded Transferred Team Call Delegated
Record Calls Answered by 3rd Party
Only available for SIP/Lync recording

The following table describes the available fields:

Field Name	Description	Requirements
Environment	For Multi-tenant systems, each extension is assigned to one of the environments. This is only configurable by users that have multi-tenant administrator rights.	-
Extension	Phone number/ SIP URI. The defined extension has to match exactly the extension number configured in the recorded UC system. Also, you have to configure each appearance of the given number in the system in order to be sure that all calls for the given extension will be recorded.	Required field. Minimum length: 1 Maximum length: 32 Must be unique in the system. Only numeric characters are allowed in this field.
User	This field enables administrators to link an extension to a Verba user. You can select a registered Verba user from the list box. You are able to link more than one extension to the same user. If you are adding an extension pattern, then this field is not available.	-

Type	<ul style="list-style-type: none"> • Number/Address - This field is used if the endpoints are identified by their extensions. This is the default option. The other options should only be selected if they specifically match the defined use-cases. • User/Agent ID - Select this when turret user IDs are used, or conversations are to be assigned based on contact center agent IDs (or the Cisco Owner User ID field) • Persistent Chat Room - Select this when adding the address of a persistent chat room. 	-
Update user information on existing conversations	<p>Enables extension mapping for historical calls. For more information, see How to correct a forgotten user-extension assignment afterwards?</p> <p>This option is only available if a user is selected for the extension.</p>	-
Description	Description of the extension. This is an optional field for adding comments to an extension.	Maximum length: 64
Recording Mode	<p>Recording modes to control how conversations are recorded, captured or imported, whether it requires user interaction or not. The following valid values apply:</p> <ul style="list-style-type: none"> • Full • On-demand • Controlled • Controlled, Auto-start • Do not record • Never Record • Relay Only • Announcement Only <p>For more information, see Recording modes</p>	-
Recording Rule	You can set up the Extension to be recorded selectively based on a pre-defined selective recording rule.	

Recorded Modalities	<p>It is possible to define which modalities should be recorded for each extension.</p> <ul style="list-style-type: none"> • Voice - Records voice calls for this extension. To define which directions should be recorded, refer to the Recorded Directions section below. • Instant Messaging - Records IM when using Cisco Jabber or SfB/Lync. • Video - Records the video streams for this extension. To define which directions should be recorded, refer to the Recorded Directions section below. • Desktop Screen - This option enables the screen capture function for the given extension - user association. Computers with installed Verba Desktop Recorder application are enabled to record desktop screen activity into video files in conjunction with the voice recording. The system allows screen capturing for users logging into Windows with the same user ID as configured in the Verba system. After the user logs into Windows, the Verba Screen Capturing Service queries the central database with the Windows user ID and determines if there is any extension for the Verba user matching the same login ID, where screen capturing is enabled. This option is only available if a user is selected for the extension. On-demand recording mode is not supported for extensions, where screen capturing is enabled. • Screen & Application Share (Lync/SfB) - This is a Lync/SfB only feature. The option enables Screen and Application Share recording for the extension. Only External sessions can be recorded (sessions that are traversing the Edge servers). Screen Sharing can be recorded for Cisco deployments, for that the video modality needs to be turned on. • Whiteboard(Lync/SfB) - This is a Lync/SfB only feature. The native Lync Archive needs to be turned on for this feature to work. • Poll / Q&A(Lync/SfB) - This is a Lync/SfB only feature. The native Lync Archive needs to be turned on for this feature to work. • File Share(Lync/SfB) - This is a Lync/SfB and Cisco Jabber only feature. In the case of Lync /SfB conferences, the native Lync/SfB Archive needs to be turned on for this feature to work. In case of Cisco, the Managed File Transfer has to be enabled. • SMS - Records SMS messages. An SMPP connection has to be set up. <p>To see exactly which modality can be recorded and for which platform, refer to the Modality and recorded platform support matrix article.</p>	-
Recorded Directions	<p>You can define, which conversation direction should be recorded for the given extension. For more information please refer to the Conversation direction and modality support article.</p>	-
Record Calls Answered by 3rd Party	<p>The Record Calls Answered by 3rd Party configuration option makes it possible to record calls that were answered by a 3rd party for a certain extension. So for example, even if the recorded extension transferred the call to an external number and neither of the participants is a recorded user in the new session, the conversation will still be recorded.</p> <ul style="list-style-type: none"> • Forwarded - Record calls that have been forwarded from this extension. • Transferred - Record calls that have been transferred from this extension. • Team Call - Record calls that came in via a team call to this extension's team, but someone else answered. • Delegated - Record calls that have been delegated to someone else from this extension. <p>These calls will be assigned to the user that this extension belongs to so that the user can access them.</p> <p>This setting is only available for Skype for Business (Lync) deployments.</p>	
Record Every Platform	<p>If this setting is enabled, then Verba will record conversations for this extension on all available platforms. If disabled, the <i>Recorded Platforms</i> selection box becomes active.</p>	
Recorded Platforms	<p>Conversations for this extension will only be recorded if they originate from the selected platform(s). To select a platform, move it to the right-hand side box.</p>	
Import from Every Source	<p>If this setting is enabled, then Verba will import conversations for this extension from all available Import Sources. If disabled, the <i>Import Sources</i> selection box becomes active.</p>	

Import Sources	Conversations for this extension will only be imported from the selected sources. To select a source, move it to the right-hand side box.	
Sampling Rate	This percentage of all calls for this extension will be recorded.	-
Record only on the selected Verba Servers	If you would like to differentiate among recording servers in terms of which extension will be recorded, you can define it by selecting this option and choosing the desired recording server from the list below.	-
Valid From	Using this field you can control the validation interval for the given extension. If the validation of a given extension is changed, the configuration changes will not be propagated automatically to the Recording Servers. The change has to be initiated manually.	-
Valid To	Using this field you can control the validation interval for the extension. If the validation of a given extension is changed, the configuration changes will not be propagated automatically to the Recording Servers. The change has to be manually initiated.	-
Avaya Password	Password field set in the Avaya Communication Manager for the recorded device.	-
Confirm Avaya Password	Confirmation of the Avaya Password field.	It has to match exactly the Avaya Password field above.
Do not request PIN on Recorder Line	This configured extension, used for a Dial-in Recorder port, will not request PIN code for authorization before starting the recording if this option is checked in.	-
MAC Address	MAC address of the phone. This optional field is used by Verba XML Service when the identification of the user cannot be achieved by providing the login name of the user as a parameter in the service URL (e.g. in CUCM Express). For more information, see Configuring the Cisco IP Phone Service .	Maximum length: 32

After filling out the form, press the **Save** button to save extension data in the database. After saving the data, you have to initiate a server configuration refresh in order to apply the changes to all affected Verba Recording Servers. This type of configuration refresh does not require service restart, so the changes will take effect immediately.

Modifying, invalidating and deleting extensions

To edit an extension entry, click on the desired line of the list showing the registered Verba extensions. After clicking on the line, a new page opens automatically.

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

You can invalidate the extension by clicking on the **Invalidate** button. You can make an extension valid by clicking on the **Make Valid** button.

You can delete the extensions by clicking on the **Delete** button. Only those extensions can be deleted, which do not belong to a recorded call, which has already been associated with a user.

Recording modes

The system supports multiple recording modes to control how conversations are recorded, captured or imported, whether it requires user interaction or not. Different recording modes might have different licensing requirements. Some recording modes are only available for specific integrations and modalities. The table below summarizes the available recording modes.

Recording Mode	Description	Supported Modalities	Supported Integrations
Full	All conversations are automatically recorded and stored for the configured extension.	All modalities	All integrations
On-demand	All conversations are automatically recorded, but they are first put into a buffer. If the recorded user (or his/her group supervisor) marks the conversation to be kept then the conversation is placed into the permanent store. If it is left unmarked then it is automatically deleted after a period of time that is defined in the configuration (up to 48 hours).	Voice, Video, Screen and Application Share, File Share, Instant Messaging, SMS	All integrations except trader voice, radio, imports
Controlled	<p>The users need to start recording manually, conversations are not recorded automatically. Users can trigger recording:</p> <ul style="list-style-type: none"> • from the Web Application under Ongoing Conversations, • using the Skype for Business Window Extension (available on Windows-based desktop clients only), • from a Cisco phone, • or from a custom application using the related APIs. <p>The recording is started only when the user triggers recording, the conversation will not contain the entire conversation. The recording can be stopped using the same controls. Users can restart recording as well, in this case, a new recording is created in the system.</p>	Voice	All integrations except trader voice, radio, imports
Controlled, Auto-start	All conversations are automatically recorded and the users have the ability to stop recording at any time using the same controls available for controlled recording (see above). Users can restart recording as well, in this case, a new recording is created in the system.	Voice	All integrations except trader voice, radio, imports
Do not record	The configured extension will not trigger recording.	All modalities	All integrations except Avaya, radio, BT ITS, Teams IM
Never Record	A conversation will never be recorded if the configured extension is a participant, even if other participants are configured for recording.	All modalities	All integrations except Avaya, radio, BT ITS, Teams IM
Relay Only	The extension will not be recorded, but the calls will be relayed through a Verba proxy.	Voice, Video, Screen and Application Sharing	Skype for Business
Announcement Only	The extension will not be recorded, but an announcement will be played by the system.	N/A	Skype for Business


Conversation direction and modality support

- [Conversation direction detection using internal domain and number patterns](#)
 - [Internal Domain, Numbers Pattern Configuration](#)
 - [Example Patterns](#)
- [Direction based recording](#)
 - [Support matrix](#)

The Verba system detects the direction of each conversation and stores this information in the conversation detail records.

Conversation direction can be one of the following:

Conversation direction	Description
Internal	Conversations between two endpoints inside the organization
Conference	Conversations where the user is part of a conference
External	Conversations between two endpoints outside the organization
PSTN In	Conversations initiated in the PSTN network and coming into the organization
Federated In	Conversations initiated in a federated network and coming into the organization
Contact Center In	Conversations initiated in an external network and coming into the organization through a contact center application
PSTN Out	Conversations initiated inside and going out from the organization to the PSTN network
Federated Out	Conversations initiated inside and going out from the organization to a federated network
Contact Center Out	Conversations initiated inside and going out from the organization through a contact center application

 The **Contact Center In** direction works only when using the following Contact Center applications:

- Luware LUCS
- Workstreampeople Anywhere 365
- Mitel MiContact Center for Microsoft Lync (PrairieFyre)
- Altigen MaxUC Contact Center
- ComputerTalk ICE Contact Center
- Competella

The **Contact Center Out** direction works only when using the following Contact Center applications:

- Workstreampeople Anywhere 365
- ComputerTalk ICE Contact Center

Conversation direction detection using internal domain and number patterns

This feature allows proper call direction detection for recordings. It is essential when call direction is used in recording rules. By using a simple pattern (regular expression), the system is able to distinguish internal and external participants and set the call direction properly.

The call direction is defined based on the following rules:

Call Direction	Description
Internal	Both participants are a match for the defined pattern
External	Neither of the participants is a match for the defined pattern
PSTN In, Federated In	Only the receiving party is a match for the defined pattern
PSTN Out, Federated Out	Only the initiating party is a match for the defined pattern

Internal Domain, Numbers Pattern Configuration

Step 0 - The configuration is available for the following service configurations:

- Media Collector & Proxy -> *General*
- Lync Filter -> *General*
- Lync IM Filter -> *General*
- SfB/Lync IM Recorder -> *General*
- Passive Recorder -> *Basics*
- Unified Call Recorder -> *Recording Providers -> General*
- Avaya Recorder -> *Avaya DMCC*
- Cisco Compliance -> *IM Recording*

Step 1 - In the Verba web interface click on **Configuration > Servers** and select your server, or select the appropriate Configuration Profile at **Configuration > Configuration Profiles**.

Step 2 - Click on the **Change Configuration Settings** tab.

Step 3 - Expand the service fields that are shown in **Step 0**.

Step 4 - Configure the **Internal Domain, Numbers Pattern** field. Standard regular expressions are used.

Step 5 - Click the **Save** icon to save your settings.

Step 6 - A warning appears: " There are tasks to be executed...", click on the **click here** link.

Step 7 - Inspect the list of tasks that wait for execution and click on **Execute Selected Tasks**.

All settings for the services that are used should contain the same pattern. Otherwise, it can lead to missing recorded conversations when "Recorded Directions" condition is set to something different than "all".

The new settings take effect **only on new calls** since the call direction decision is made during the recording of the call.

Example Patterns

For regular expression language please refer to [https://msdn.microsoft.com/en-us/library/az24scfc\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx).

To check and validate your regular expressions, you can use <http://www.regexr.com/>.

Example domains, numbers:

- 1{DID}@128.144.122.12
- 12143221234@128.144.122.12
- some_extension_name@128.144.122.12:5080
- other_extension_name@voip.example.com

- extension_name@123456_subaccount
- {DID}@123456_subaccount

Example Description	Example Pattern
Match your domain	.*@yourdomain\.com
Match SIP URI that starts with "verba" plus one or more characters and ends with "@yourdomain.com"	verba(\w+)@yourdomain\.com
Match extension name that starts with "ext" plus one or more characters and ends with "@128.144.122.12:5080"	ext(\w+)@128\.144\.122\.12:5080
Match one digit numbers	[0-9]
Match four digit numbers	[0-9]{4}
Match numbers that start with 1213 and has one or more numbers at the end	1213[0-9]+
Match numbers that start with +1213 and has one or more numbers at the end	\+1213[0-9]+
Match numbers that start with 1213 and has 3 additional numbers at the end	1213[0-9]{3}
Match optional + sign at the beginning of a number	\+*1213
Multiple conditions, match numbers that start with +12 or +13 plus one or more numbers at the end	\+(12 13)[0-9]+
Multiple conditions, SIP URI / numbers	.*@yourdomain\.com 1213[0-9]+
Multiple conditions, multiple numbers	1213 1214 1215

Direction based recording

Extensions can be configured so that only certain directions are recorded. For example, some extensions should be recorded internally, but for others only PSTN incoming calls.

Support matrix

The following table shows the supported direction based recording rules for a modality and recorded platform.

Modality	Service	All	Internal	PSTN In	PSTN Out	External	Federated In	Federated Out	Contact Center In	Contact Center Out	Conference
Voice	Avaya DMCC /JTAPI	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes
	Passive Recorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Unified Call Recorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
	Cisco network-based recording does not support call direction rules defined in the extension configuration! You can find more information below the table.										

	Analogue and Radio Recorder	No ACL support									
	Centile Connector	No ACL support									
	Verba Import (Symphony)	Yes	Yes	No	No	Yes	No	No	No	No	No
	Verba Import (Cloud9)	Yes	Yes	No	No	No	No	No	No	No	No
	Verba Import (RingCentral)	Yes	Yes	No	No	Yes	No	No	No	No	No
	Verba Import (O2)	Yes	Yes	No	No	Yes	No	No	No	No	No
	Verba Import (Vodafone)	Yes	Yes	No	No	Yes	No	No	No	No	No
Video	Passive Recorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Unified Call Recorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
	Verba Import (Symphony)	Yes	Yes	No	No	Yes	No	No	No	No	No
Instant Messaging	SfB/Lync IM Recorder	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes
	Cisco Compliance	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes
	Verba Import (Symphony)	Yes	Yes	No	No	Yes	No	No	No	No	No
Desktop Screen	Screen Capture Multiplexer	No ACL support									
Screen and Application Share	Passive Recorder	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Verba Import (Symphony)	Yes	Yes	No	No	Yes	No	No	No	No	No
Whiteboard	Verba Import	Yes	Yes	No	No	No	No	No	No	No	Yes
Poll / Q&A	Verba Import	Yes	Yes	No	No	No	No	No	No	No	Yes
File Share	Verba Import	Yes	Yes	No	No	No	No	No	No	No	Yes
SMS	Verba SMS Recorder	Yes	Yes	Yes	Yes	No	No	No	No	No	No

Although the Unified Call Recorder service is used, direction differentiation is not possible this way when using Cisco network-based recording. To see what options exist to enforce direction support with Cisco network-based recording refer to the [Advanced Call Recording Rules](#) article.

To see which modalities can be recorded for which platform, refer to the [Modality and recorded platform support matrix](#) article.

✔ To see how to configure which modality and direction should be recorded, refer to the [Extension details](#) article.

Modality and recorded platform support matrix

The following table shows the support for modalities on the recorded platforms.

Recorded Platform	Recording Technology	Recording Service	Voice	Video	IM	SMS	Desktop Screen	Screen & Application Share	Whiteboard	Poll / Q&A	File Share /Transfer
Cisco	Network-based	Unified Call Recorder Cisco JTAPI	Yes	-	-	-	Yes	-	-	-	-
Cisco UBE (CUBE)	SIPREC	Unified Call Recorder	Yes	Yes	-	-	Yes	-	-	-	-
Cisco Voice Gateway	XCC	Unified Call Recorder	Yes	-	-	-	Yes	-	-	-	-
Cisco IM&P	IM&P Compliance API	Cisco Compliance	-	-	Yes	-	-	-	-	-	Yes
Cisco	Proxy-based	Passive Recorder Media Collector and Proxy	Yes	Yes	-	-	Yes	- 1	-	-	-
Cisco MediaSense	Import	Cisco MediaSense Connector	Yes	-	-	-	-	-	-	-	-
Cisco Webex Teams	Import	Verba Import	-	-	Yes	-	-	-	-	-	Yes
Microsoft SfB /Lync	-	Passive Recorder Media Collector and Proxy	Yes	Yes	-	-	Yes	Yes	-	-	Yes (P2P)
	-	SfB/Lync IM Recorder	-	-	Yes	-	-	-	-	-	-
	-	Verba Import	-	-	-	-	-	-	Yes	Yes	Yes (Meetings)
Microsoft Teams	Bot	Unified Call Recorder	Yes	Yes	-	-	Yes	Yes	-	-	-
	Webhook / Export API	Unified IM Recorder	-	-	Yes	-	-	-	-	-	Yes
Avaya	DMCC multiple registrations	Unified Call Recorder Avaya DMCC /JTAPI	Yes	-	-	-	Yes	-	-	-	-
Avaya SBCE	SIPREC	Unified Call Recorder	Yes	Yes	-	-	Yes	- 1	-	-	-
BroadSoft BroadWorks	SIPREC	Unified Call Recorder	Yes	Yes	-	-	Yes	- 1	-	-	-
Oracle/ACME Packet SBC	SIPREC	Unified Call Recorder	Yes	Yes	-	-	Yes	- 1	-	-	-
MetaSwitch Perimeta SBC	SIPREC	Unified Call Recorder	Yes	-	-	-	Yes	- 1	-	-	-


SIP/SCCP compatible	Network port mirroring	Passive Recorder	Yes	Yes	-	-	Yes	_1	-	-	-
BT ITS	IPSI, ITSLink	Unified Call Recorder	Yes	-	-	-	-	-	-	-	-
BT IP Trade	Recorder API	Unified Call Recorder	Yes	-	-	-	-	-	-	-	-
IPC Unigy	SIP, CTI	Unified Call Recorder	Yes	-	-	-	-	-	-	-	-
Speakerbus	RTP, iCDS	Unified Call Recorder	Yes	-	-	-	-	-	-	-	-
Truphone	SIP-based forking	Unified Call Recorder SMS Recorder	Yes	-	-	Yes	Yes	-	-	-	-
Huawei	SIP-based forking	Unified Call Recorder	Yes	-	-	-	Yes	-	-	-	-
Tango Networks	SIP-based forking	Unified Call Recorder	Yes	-	-	-	Yes	-	-	-	-
Analogue ²	Synology TAP card	Analogue and Radio Recorder	Yes	-	-	-	-	-	-	-	-
Bosch Telex ²	RTP streaming	Analogue and Radio Recorder	Yes	-	-	-	-	-	-	-	-
Generic RTP streaming ²	-	Analogue and Radio Recorder	Yes	-	-	-	-	-	-	-	-
Centile	Import	Centile Connector	Yes	-	-	-	-	-	-	-	-
SIP compatible	Dial-in and dial-out recorder	Unified Call Recorder	Yes	Yes	-	-	Yes	_1	-	-	-
Genesys	SIP-based forking	Unified Call Recorder	Yes	-	-	-	Yes	-	-	-	-
Symphony	SIPREC	Unified Call Recorder	Yes	Yes	-	-	Yes	Yes	-	-	-
	Import	Verba Import	-	-	Yes	-	-	-	-	-	Yes
Bloomberg Chat	Import	Verba Import	-	-	Yes	-	-	-	-	-	-
Cloud9	Import	Verba Import	Yes	-	-	-	-	-	-	-	-
RingCentral	Import	Verba Import	Yes	-	-	-	-	-	-	-	-
SMS	SMPP	SMS Recorder	-	-	-	Yes	-	-	-	-	-
O2	Import	Verba Import	Yes	-	-	-	-	-	-	-	-
Vodafone	Import	Verba Import	Yes	-	-	-	-	-	-	-	-

¹ SIP/BFCP based screen and application share recording is supported, mixed into video call recording, not available as a separate recording

² Recording rules are not supported, requires manual channel configuration

Selective recording rule configuration

Selective recording rules can be used to define when an extension should be recorded in a more complex way based on various CDR fields.

 Currently, this feature is supported only in Cisco JTAPI based selective recording integrations including Cisco UCCX, Cisco UCCE, and Genesys.

Prerequisites for rule based selective recording

CUCM configuration for selective recording

The [Verba JTAPI](#) user must have the Standard CTI Allow Recording group membership.

The extension configuration is detailed in the [Adding a new extension for recording in Cisco UCM](#).

The Recording Option at the Directory Number has to be set to Selective (**Step 4b**), and the Phone Device has to be added to the Verba JTAPI user as Controlled Device. (**Step 8**)

Verba configuration for selective recording

The [Recording Mode](#) of the [Extension](#) has to be set to full.

Recording rule configuration

You can add / modify / delete recording rules under the **Users / Recording Rules** menu.

Recording Rule Configuration

[Add New Recording Rule](#)
[Back to Previous Page](#)

▼ Recording Rule

ID 1

Name *

Description

▼ Rule Sections

[Move Up](#) [Move Down](#) [Remove Section](#)

ID 12

Name

Action

CTI Triggered Recording

Filters

[Add New Filter](#)

[Move Up](#) [Move Down](#) [Remove Section](#)

ID 11

Name

Action

CTI Triggered Recording

Filters

[Add New Filter](#)



[Save](#) [Delete](#)

Creation Date: Jan 11, 2018 4:17:58 PM
 Created By: Verba Administrator (Administrator)
 Last Modification Date: Jan 27, 2018 12:41:34 PM
 Last Modified By: Verba Administrator (Administrator)
[View Change History](#)

* Indicates required item.

The following table describes the available fields in the basic recording rule configuration:

Field Name	Description
------------	-------------

ID	Auto-generated identifier
Name	Name of the recording rule
Description	Longer description of the recording rule
Rule Sections	The rule logic

Rule section

A recording rule consists of several rule sections. The sections are evaluated in sequence one after the other. The recorder engine will perform the first matching section's action, and the rest will not be evaluated.

Each section defines the desired action and various filters that will be evaluated in order to determine if the section matches a conversation or not. The logical relation between the filters is AND so that all of the filters should match the conversation (within a section).

If a section has no filters, then it will always be evaluated as matching. Such section can be used to define a default behavior, practically as the last section of a rule. If no section matches a conversation, then no action will be performed, that is the conversation will not be recorded.

The following table describes the available fields within a recording rule section:

Field Name	Description
ID	Auto-generated identifier.
Name	Name of the section.
Action	<p>What should the system do when this section matches a conversation.</p> <p>Possible actions:</p> <ul style="list-style-type: none"> • Do not record • Record
CTI Triggered Recording	<p>If the recording is not triggered automatically by the PBX, but the recorder has to initiate the recording, then this option has to be turned on.</p> <p>Example: when a Cisco extension's recording mode is Selective.</p>

Filters

Defines when this section should be performed.

The following CDR fields can be used in the filters:

- Caller Party
- Called Party
- Any Party
- Partition (Cisco JTAPI)
- Genesys Field
 - Any Genesys field can be specified by typing the name of the field
 - Custom user data fields should be prefixed with "UserData.", for example: UserData.ShouldRecord
- Cisco UCCE Field
 - Any UCCE field can be specified by typing the name of the field
- Cisco UCCX Field
 - Any UCCX field can be specified by typing the name of the field

Matching patterns (the listbox next to the field):

- DOS: DOS-style wildcard characters can be used
 - asterisk (*) matches any sequence of characters
 - question mark (?) matches any single character
- Regular Expression
- Simple

Administration of recorded extensions for Cisco network-based recording

The Cisco network-based recording allows you to record the Cisco phones using the integrated recording technology available since CUCM 6.0. In order to set up extensions/directory numbers, the Cisco Unified Communications Manager has to be configured properly and extensions have to be added optionally in the Verba system.

This topic only focuses on phone administration, there are other mandatory tasks for the complete configuration of the CUCM and the Verba server. For further information, see [Configuring Verba for Cisco network-based recording](#).

The table below summarizes the necessary steps to add a recorded extension using Cisco network-based recording:

		Description
1	Configure recorded extension in CUCM	Set up a new recorded extension in CUCM. For a more detailed description, see Adding a new extension for recording in Cisco UCM
2	Update associated devices for the JTAPI application user	The JTAPI application user, utilized by the Verba system to provide additional metadata for the calls, has to be associated with each recorded device. Update the association configuration, see Creating an application user for the JTAPI connection
3	Configure recorded extension in Verba Recording System	You only have to take this step if you want to assign the newly configured extension to a Verba user for search and replay or on-demand recording. For more information, see Creating an extension .
4	Make test call	Test the configuration, by making a call from the phone and play it back in the Verba web interface.

Administration of recorded extensions for Passive Recorder

The Verba Passive Recorder service allows you to record SCCP and SIP phones or SIP trunks using packet capturing technology through monitor ports. In order to setup extensions/directory numbers for recording, the monitor port of the switch(es) has to be configured properly and the extension has to be added optionally in the Verba system.

This topic only focuses on the phone administration, there are other mandatory tasks for the complete configuration of the Verba server. For more information, see [Passive recorder configuration](#).

The table below summarizes the necessary steps to add a recorded extension using Passive Recorder:

		Description
1	Configure monitor port	Modify the configuration of the monitor port to include the traffic of the new device. For more information, see Configuring monitor port .
2	Configure recorded extension in Verba Recording System	You only have to take this step if the Recording Server is configured to record non-configured extensions and /or you want to assign the newly configured extension to a Verba user for search and replay or on-demand recording. For more information, see Creating a Verba Server and see Creating an extension .
3	Make test call	Test the configuration, by making a call from the phone and play it back in the Verba web interface.

Correcting user-extension assignments

Recorded conversations on an extension are associated to users **only after the time** when the extensions is already associated with the user.

When the conversation starts, Verba determines the associated user to a call record, based on the current phone number assignments. If the phone numbers were not assigned to the user before the start of the recording, the conversations will not be associated with any user. However, if you have already started recording on an extension without associated user, you can still **link the call records to a user retroactively**.

In order to associate previously recorded conversations to a given user, in cases when the numbers had not been associated to the user at the time of the call, follow the steps below:

Step 1 - Select the **Administration / Users** menu item and select the desired user. The user configuration page will be loaded.

Step 2 - Set the **Valid From** value to that date, which equals to or is earlier than the start date of the recorded calls. Press the **Save** button.

Step 3 - Go to the **Administration / Extensions** page and map the forgotten phone number to the given user and check the Update user information on existing calls checkbox. After pressing the **Save** button on the **Extension Configuration** page, the system automatically associates the previously recorded calls to the current user. The automatic association will only effect those calls,

- of which caller party phone number or called party phone number equals to the currently added phone number
- the start date of the call is equal to or later then the starting validation date of the given user
- the call has not been already associated to a user


Microsoft Teams selective recording settings

AVAILABLE IN 9.6.9 AND LATER


The selective recording settings provide additional controls on how the system should record Microsoft Teams voice, video and screen share calls:

- Record only if an external user is participating
- Record video only for external users
- Record only scheduled meetings

These settings are only supported for Microsoft Teams recording.

 External participant means that the Microsoft Tenant ID of the participant is different from the Microsoft Tenant ID of the recorded user. The Tenant ID is different:

- if the participant is part of another Teams tenant,
- or the participant is represented by a PSTN number,
- or it is empty.

Setting	Description
Record Only if External User is Participating	If the setting is enabled, the meeting, which the recorded user participating in, will be recorded only when at least one external participant is on the meeting. The recording starts when the first external participant enters the meeting, ends when the last external participant leaves the meeting.
Record Video Only for External Users	If the setting is enabled, the video modality will be only recorded for external participants at a meeting. The Verba Microsoft Teams Bot service won't subscribe to an internal user's video stream at all.
Record Only Scheduled Meetings	<p>Organizers</p> <p>The Verba Microsoft Teams Bot receives the meeting invite if a regulated user joins a meeting. The invite contains the Microsoft Azure Object ID of the meeting organizer.</p> <p>The organizer field is a line-separated multi-string type field, add the Microsoft Azure Object ID of the desired users, service accounts. If the Verba Microsoft Teams Bot identifies the meeting organized by the configured users, it will initiate recording after the recorded user joined the meeting.</p> <p>Subject</p> <p>The Verba Microsoft Teams Bot service uses the following Graph API endpoint: https://docs.microsoft.com/en-us/graph/api/calendar-get?view=graph-rest-1.0&tabs=http New Graph API permission is required: Calendars.Read</p> <p>The Verba Microsoft Teams Bot expects a regular expression as a setting if subject-based filtering is required.</p> <div data-bbox="309 1827 1485 1944"><p> Limitation: The subject-based filtering only works with scheduled meetings. It doesn't support 'Meet Now' meetings, those are not accessible through the Calendar API.</p></div>

Relay-only configuration for Microsoft SfB - Lync

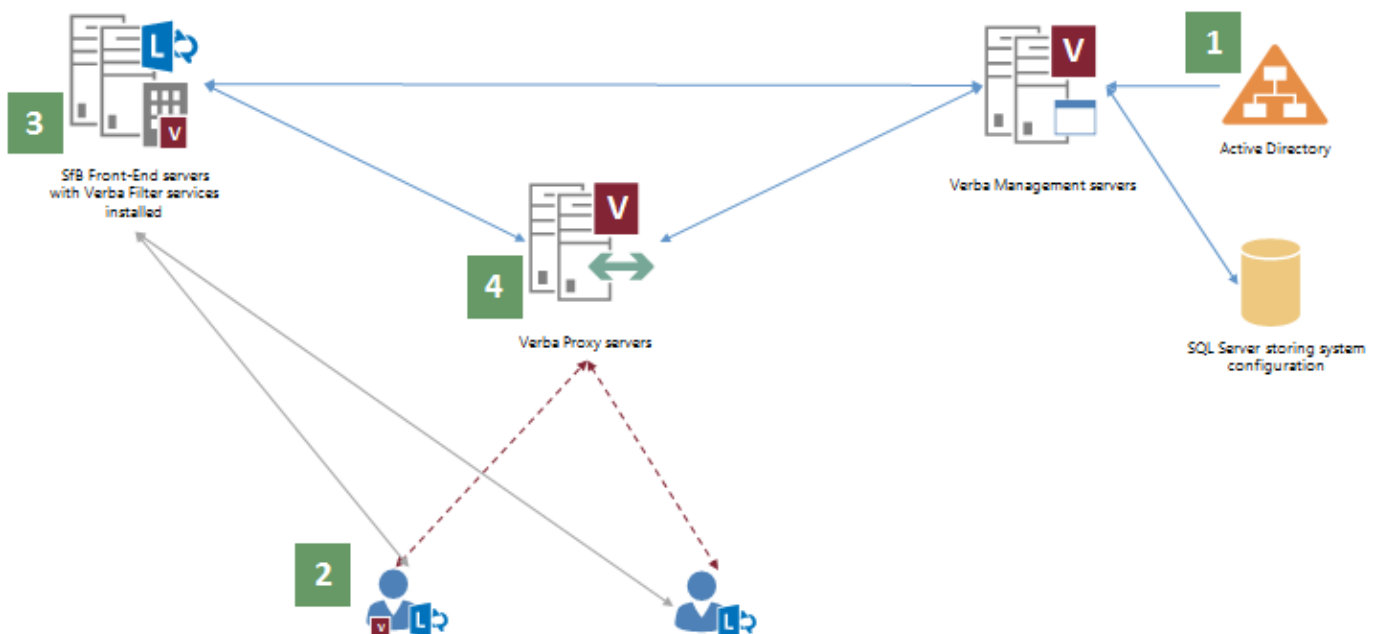
Available in version 8.4 and later

- [Overview](#)
- [Network requirements](#)
- [QoS and Firewall requirements](#)
- [Configuring relay-only extensions](#)

Overview

There are some specific use cases where customers would like to prevent P2P traffic between SfB/Lync endpoints to avoid any-to-any relations, primarily due to security and firewall issues. The following list summarizes the key features:

- Built on top of the Verba system. It can be deployed as a relay-only solution or as a mixed environment with recorded and relay-only users.
- Standard AD sync profiles can be configured for specific users, where relay-only "recording mode" can be configured for the associated extensions/addresses.
- When the Verba Filter Service recognizes a voice/video call for a configured user, it will update the SDP and relay the call through a Verba Proxy Server. Verba Proxy Servers can be deployed in a resilient fashion providing load balancing and failover functions. The same proxy server can be used for recording as well.
- The system does not store any information about relay-only calls besides the standard log entries related to the filter and relay services.
- The Verba Proxy Server currently has the following limitations:
 - It can only relay UDP streams, TCP is not supported
 - It cannot support endpoints behind NAT (this will be resolved soon)



1. Using AD sync, Verba stores the configuration of the users and their associated SIP URIs / phone numbers in an SQL Server. The configuration is automatically pushed down to all Verba servers, including the SfB FE filter applications. SfB FE filter applications store a local, cached copy of the configuration.
2. A configured SfB user starts a voice/video call.
3. The Verba Filter service detects the call for the configured user based on SIP URI/phone number. It forwards call setup messages to a Verba Proxy Server based on the load balancing and failover configuration.

- The Verba Proxy Server allocates relay ports and rewrites ICE candidates, then sends back the updated SDP to the filter application. Endpoints will connect via the relay port, internal routing logic will forward received RTP/RTCP packets to the other endpoint.

Network requirements

- Direct IP connectivity between the relay service and the call participants
- NAT traversing is currently not supported. If at least one endpoint is behind NAT, the call is expected to flow via the Edge Server.
- Network bandwidth: (codec rate + ~22.4 kbps packetization overhead) x 2x number of concurrent calls in both RX/TX direction
- Low delay, low jitter network link to SfB endpoints

QoS and Firewall requirements

- A dedicated port range for voice and for video calls can be specified
- DSCP/Diffserv TOS marking can be achieved by Windows QoS management: <https://technet.microsoft.com/en-us/library/cc771283.aspx>
- The firewall should allow inbound traffic from SfB endpoints (phones, mediation, AVMCU, ...) to relay port range and outbound traffic from relay ports to these endpoints
- One stream (voice or video) allocates 4 ports on the relay server (caller RTP+RTCP, callee RTP+RTCP).
- Skype for Business is now able to multiplex RTP and RTCP on the same port, even so, due to backward compatibility, we follow the “RTP on even, the RTCP on the next odd port number” rule
- By default the service listens on:
 - UDP 16384-65535 – relay port range
 - TLS 10201 – SfB filter connections
- More information: [Port range and QoS settings for proxy based recording](#)

Configuring relay-only extensions

Follow the steps below to configure a relay-only user:

Step 1 - In the Verba web interface click on **Users / Extensions**.

Step 2 - Select the extension you would like to be a relay-only extension.

Step 3 - Under **Recording Settings** change the **Recording Mode** drop-down value to **Relay Only**.

Step 4 - Scroll down to the bottom of the page and click the **Save** button.

Step 5 - Follow the instruction in the yellow stripe above the extensions list to apply changes to Verba services

Recording Settings

Recording Mode*

Voice

Instant Messaging

Video

Desktop Screen

Screen & Application Share

Whiteboard

Poll / Q&A

File Share

Support of modalities depends on the recorded platform, more information [here](#).

Recorded Directions All Internal PSTN In PSTN Out External Federated In Federated Out Conference

Record Calls Answered by 3rd Party All Forwarded Transferred Team Call Delegated

Only available for SBI/Lync recording

Shared line recording configuration with Cisco recording

The guide explains the recommended configuration for shared lines in the system if the [Cisco network-based recording](#) is utilized. The goal of this configuration is to accurately store who answered the shared line.

If desktop recording, speech analytics, announcement are user based, this may cause unexpected behavior

Configuring owner User IDs in CUCM

Step 1 - Login to CUCM web interface

Step 2 - Assign the phones sharing the line to users in Cisco UCM. Navigate to **Device / Phone**, and for each phone, set the **Owner** to **User**, and note the **Owner User ID**

Built In Bridge*	On
Privacy*	Default
Device Mobility Mode*	Default
Owner	<input checked="" type="radio"/> User <input type="radio"/> Anonymous (Public/Shared Space)
Owner User ID*	testuser1

Enabling Owner User ID support in Verba

Step 3 - In the Verba Web Interface navigate to **System / Servers** and select the server where the Cisco JTAPI Service is enabled (Recording Server/ Media Repository and Recording Server). Or navigate to **System / Configuration Profiles** and select the server profile which is used to run the Cisco JTAPI Service.

Step 4 - Click on the **Change Configuration Settings** tab.

Step 5 - Under the **Cisco JTAPI Configuration** node, select **Advanced** and set **Fill Agent ID with Owner User ID** to **Yes**.


- Cisco JTAPI Configuration
 - Basics
 - Cisco UCCX Integration
 - Cisco UCCE Integration
 - Genesys Integration
 - Advanced
| | |
| --- | --- |
| Service Port: | 11200 |
| Work Folder: | C:\Program Files\Verba\work\nativerec |
| Advanced Recording Rules Enabled: | No |
| Fill Agent ID with Owner User ID: | Yes |

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 8 - If you configured an individual server, instead of a configuration profile, repeat the steps above on all servers where the Cisco JTAPI Service is enabled.

Adding Owner User IDs and shared lines as extensions

Step 9 - Navigate to **Users / Extensions**. and add the Owner User IDs as **User/Agent ID** type extensions.

Step 10 - Also add the shared line extension as a **Number/Address** type recorded extension, and type "**Shared Line**" to the description to indicate that this is a shared line

Step 11 - Do not assign the shared line extension to any user.

Step 12 - Assign the Owner User ID extensions to the Verba Users.

Step 13 - Apply the changes.

Call assignment logic:

1. If **User ID** is available, the system looks for an extension where Type = User/Agent ID
2. If the User could not be determined by the User ID, then the call is assigned according to the recorded party, based on the source \ destination extension where the extension type is not User/Agent ID

User and Group Management Tools

- [Active Directory synchronization](#)
- [Bulk User and Extension Update](#)
- [Bulk user import](#)
- [Using the Group CSV Import](#)

Active Directory synchronization

- [Synchronization Interval and Run Now Feature](#)
- [Synchronization from Azure Active Directory](#)
- [Differential synchronization](#)
- [Adding a new Active Directory Profile](#)
- [Modifying AD Synchronized Users](#)
- [Export Options - Active Directory Synchronization Profiles](#)

Overview

Users stored in the company's Active Directory (or any other LDAP server) can be synchronized by the Verba database. It can be administered on the web interface under the **Administration / Active Directory Synchronization** menu item.

If you delete a user from your Active Directory Verba won't delete the user from its database. Instead of that the system will invalidate that user. This way 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.

Synchronization Interval and Run Now Feature

A full synchronization process might take long time (especially if there are many synchronized users) so it is scheduled to run once a day at 1 AM. (in pre Verba 9.1 versions)

For testing purposes and urgent cases, the synchronization can be started on the web interface. After creating and saving your profile (see below) you can start the synchronization under **Administration / Active Directory Synchronization / Run Each Active Directory Profile Now**.

It is also possible to run the configured synchronization profiles individually. In order to do that navigate to the **Administration / Active Directory Synchronization** menu, select the synchronization profile you want to run, then click on the **Run this Active Directory Profile Now** link. This method also runs the profile if the **Automatic Rollback Threshold on Invalidated Users** setting is reached.

Synchronization from Azure Active Directory

AVAILABLE IN 9.3 AND LATER

Verba can be configured to synchronize users and extensions from Azure Active Directory instead. The prerequisite for this is [registering Verba as a Connector App](#) on the Azure side.

The Azure AD Synchronization has some limitations:

- Organizational Units are not available
- Users can only be searched by a graph filter query parameter
- Manager / Direct Reports are not available
- Security Group Hierarchy synchronization is not available, the direct group membership is synchronized instead
- Connection test is not available
- Group names are not calculated from OU, instead, a property will be the name.

Differential synchronization

AVAILABLE IN 9.1 AND LATER

After the first full synchronization, Active Directory synchronization does differential user synchronization.

A typical full synchronization for 100K users synchronization time is ~10 hours.

With differential synchronization this time shortens significantly:

- 100K users differential synchronization time when there is no change: ~1 minute
- 100K users differential synchronization time when 1,000 users changed: ~2 minutes

In case of a change in the AD Synchronization profile, full synchronization is required. This can be done by setting the **Highest USN** setting to 0, then invoking a synchronization by clicking on the "Run this Active Directory Profile now" link.

Adding a new Active Directory Profile

Multiple Active Directory Profiles can be set up in Verba so multiple AD servers or users with different privileges can be synchronized. The profiles will always be executed in a configurable order, and each user will be processed by only one Active Directory Profile, so the Profile with the smaller sequence will process users read from multiple profiles.

Navigate to **Administration / Active Directory Synchronization** and select the **Add new Active Directory Profile** option on the top right corner of the page.

For the configuration guides, see:

- [Configuring Active Directory Synchronization - Basic \(LDAP\)](#)
- [Configuring Active Directory Synchronization - Basic \(Azure\)](#)
- [Configuring Active Directory Synchronization - Advanced](#)
- [New Users' Properties Rules](#)

For the full configuration reference, see: [Active Directory Synchronization Configuration Reference](#)

Modifying AD Synchronized Users

Modifications to the "New Users Properties" tab of the AD synchronized profiles won't affect the already synchronized users. The new settings will be applied only to the newly synchronized users. However, there are some ways to modify the already synchronized users in a bulk way:

- Using the [Bulk User and Extension Update](#).
- Creating a new AD synchronization profile with the new attributes, and adding it to the base profile at the **Profiles to be Merged** setting. With this approach, only the addition to the attributes is possible.
- Creating an additional [New Users' Properties Rule](#), and adding it to the base profile at the **Assign New Users' Properties Rules** setting.

Export Options - Active Directory Synchronization Profiles

The system allows users to export the list of configured Active Directory Profiles.

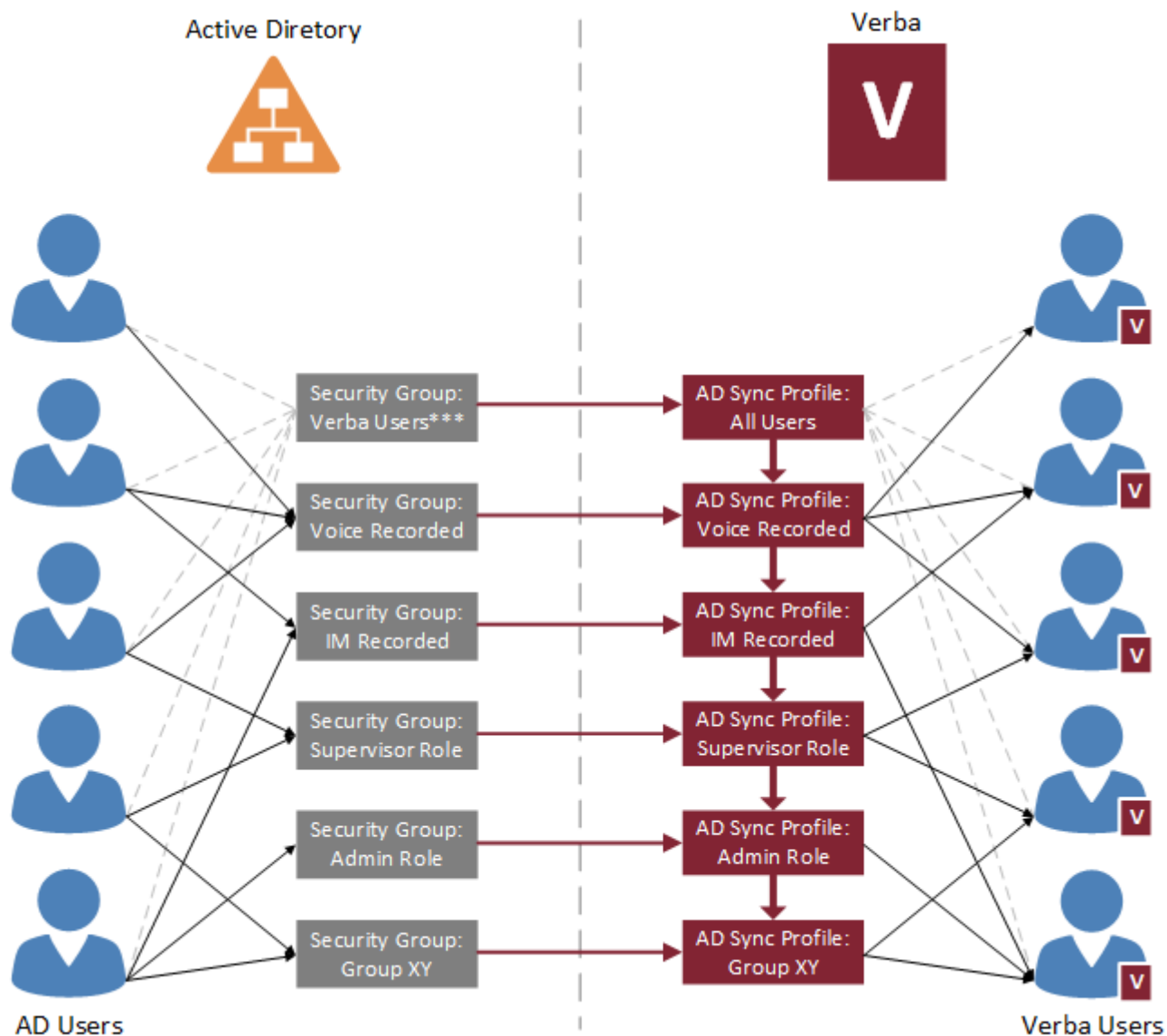
The RTF and PDF export options will export the list of configured Active Directory Profiles, please note that these options will only display the visible column headers, as seen on the Find and List Active Directory Profiles screen.

AVAILABLE IN VERSION 9.6.13 OR LATER

The Excel export option will export all configured Active Directory profile values, including all configured values within the Active Directory Profile Configuration Screen.

Configuring Active Directory Synchronization - Advanced

In large Verba deployments, where many different kinds of users would use Verba (with different recording settings, roles, and other settings, and the combination of these), the basic setup of the Active Directory Synchronization would need a very high number of security groups on the Active Directory side. It would require a separate group for each setting, and a separate group for each combination of these, which is hardly manageable. In order to avoid this, Verba offers a feature, called Merged Profiles.



***Creating an AD security group for all Verba users is not mandatory. See configuration stage 1.

With the Merged Profiles, once a user gets synchronized, the subsequent profiles can modify the user and add several additional settings. This way, the recording setting, the user role, and the group membership setting synchronization can be combined. If a more detailed fine-tuning is required, see [New Users' Properties Rules](#).

Stage 1: Configuring the base Active Directory Synchronization Profile

For the base profile configuration, complete the **steps 1-7** from the [Configuring Active Directory Synchronization - Basic \(LDAP\)](#) or the [Configuring Active Directory Synchronization - Basic \(Azure\)](#) article (Configuring AD Synchronization for Recorded Users section). At **step 7**, there are two options for the **LDAP Search Filter** setting:

- Creating a separate security group on the AD side for all Verba users, and using that one in the LDAP Search Filter.
E.g.: (&(objectcategory=person)(objectclass=user)(memberOf=CN=All Verba Users,OU=London,DC=CONTOSO,DC=COM))
- Skipping the creation of a security group for all Verba users, and using the other security groups with OR operation between them. This is recommended only in the case of a low number of groups.
E.g.: (&(objectcategory=person)(objectclass=user)((memberOf=CN=Voice Recorded,OU=London,DC=CONTOSO,DC=COM)(memberOf=CN=IM Recorded,OU=London,DC=CONTOSO,DC=COM)(memberOf=CN=Verba Supervisor,OU=London,DC=CONTOSO,DC=COM).....))

Stage 2: Configuring the Active Directory Synchronization Profiles based on recording modes, roles, and groups

Create multiple AD Synchronization Profiles using the [Configuring Active Directory Synchronization - Basic \(LDAP\)](#) or the [Configuring Active Directory Synchronization - Basic \(Azure\)](#) article. Use the different AD security groups at **step 7**. Configure each profile according to its purpose (Phone number and/or SIP URI mappings and recording settings, role settings, group settings).

Stage 3: Configuring the Active Directory Synchronization Profile Merging

Step 1 - Open the **base** Active Directory Synchronization Profile

Step 2 - At the **Profiles to be Merged** setting, add the other AD Synchronization Profiles by clicking on the >> icon.

Step 3 - Tick the settings to be merged (Extensions, Groups, Roles).

Profiles to be Merged

>>

<<

Voice Recorded Users
 IM Recorded Users
 Supervisors
 Administrators
 Group XY members

Merge Extensions

Merge Groups

Merge Roles

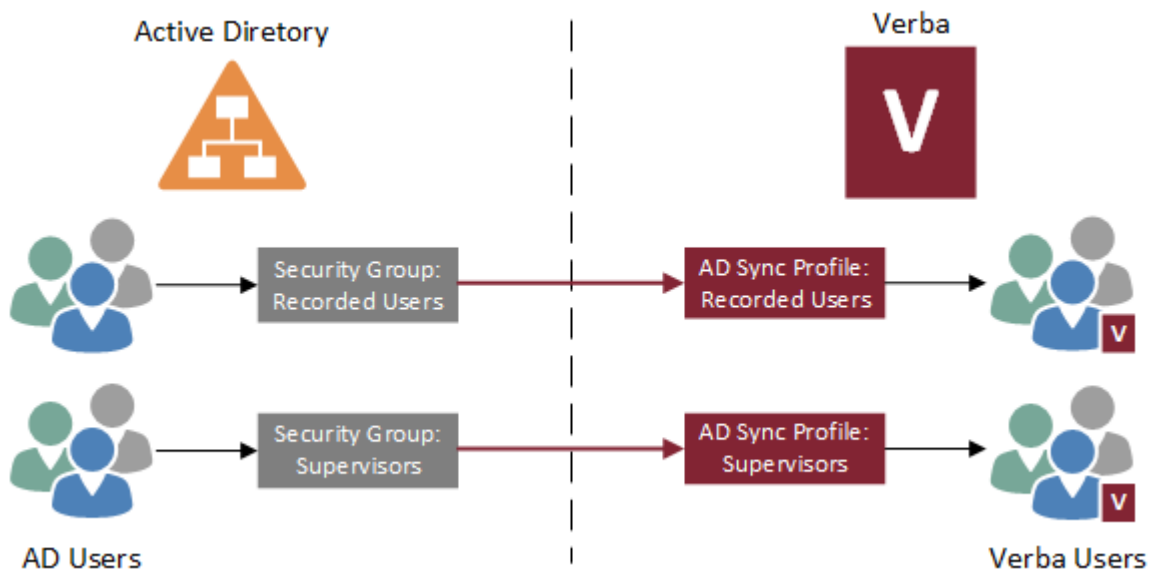
Step 4 - Click **Save**.

Configuring Active Directory Synchronization - Basic (LDAP)

In small or medium-sized Verba deployments, usually only a few Active Directory Synchronization Profiles are configured. When the only requirement is synchronizing the recorded users, even one profile is enough.

In the case of these basic setups, AD users separated by security groups based on the purpose of the users in Verba. These users then synchronized into Verba by Active Directory Synchronization Profiles tied to these groups.

The disadvantage of this kind of setup is, that in case of many different user setting combinations in the Verba side, lot of security groups would be required because of the combination of the settings (E.g: Voice recorded, IM recorded, Voice and IM Recorded, etc.). In cases like this, see [Configuring Active Directory Synchronization - Advanced](#).



Synchronization Profile Sequence

The Sequence setting of the AD Synchronization Profiles determines the execution order of the profiles. It starts from the smallest one. In case of using a basic setup of AD Synchronization Profiles, this setting is important when a user is member of multiple synchronized AD security groups. Once a user gets synchronized by the first profile based on the sequence, it won't be modified any more by the subsequent profiles.

Configuring AD Synchronization for Recorded Users

Step 1 - Go to the **Users \ Active Directory Synchronization** menu.

Step 2 - Click on the **Add New Active Directory Profile** link in the upper right corner.

Step 3 - Provide a **Description**.

Step 4 - Provide the address of a domain controller at the **LDAP Host** setting.

Step 5 - Provide an AD user at the **LDAP User Distinguished Name or Domain User Name** setting. Provide its password in the **LDAP Password** field.

Description* Recorded Users

Enabled* Yes ▾

Sequence* 100
Unless Merged Profiles are set, only one Active Directory Profile will be effective for individual users. Profiles with the smaller sequence numbers run first.

LDAP Host* dc.contoso.com

LDAP Port* 389
Default port is 389 (636 if SSL is used), default Active Directory Global Catalog Forest-Wide port is 3268 (3269 if SSL is used).

Use SSL

Character Encoding ISO-8859-1

LDAP User Distinguished Name or Domain User Name contoso\verba

LDAP Password

Step 6 - Click on the **Fetch** button next to the **LDAP User Search Base** in order to check the connection. If the connection is working, it will offer some options for the LDAP User Search Base setting.

Select (or provide) the appropriate LDAP User Search Base. This should be the base domain (E.g.: DC=CONTOSO,DC=COM), or in case of large domains with ten thousands of users, in order to avoid searching through the whole AD, provide the path to an OU which contains the users to be synchronized (E.g.: OU=Call Center,OU=London,DC=CONTOSO,DC=COM).

Step 7 - Configure the **LDAP Search Filter** setting for the users to be synchronized. The recommended way is copying the example configuration that can be found right beneath the setting, then replacing the example part (CN=Verba_Group,DC=yourdomain,DC=com) with the distinguished name of the security group to be synchronized. Make sure there are no spaces before or after the LDAP filter in the text box!

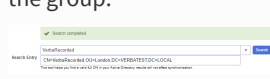
LDAP User Search Base* DC=CONTOSO,DC=COM ▾ **Fetch**

E.g. OU=Recorded Users,DC=yourdomain,DC=com
where 'Recorded Users' is an organization unit that should already exist.

LDAP Search Filter (&(objectcategory=person)(objectclass=user)(memberOf=CN=Verba Recorded,OU=London,DC=CON
E.g. (&(objectcategory=person)(objectclass=user)(memberOf=CN=Verba_Group,DC=yourdomain,DC=com))

Finding the distinguished name of a security group

The Active Directory Synchronization Profile configuration page offers a tool for searching for objects in the AD. Type in the name of the group at the Search Entry setting, click Search, then it will provide the full distinguished name of the group.



In the Active Directory, the distinguished name of a security group can be found by opening its properties, then navigating to the Attribute Editor tab. The Attribute Editor tab will be shown only, if the Advanced Features setting is turned on in the View menu.

Disabled users in Active Directory

There are cases when it is required for disabled users to be removed from Verba, it can be achieved by using the Syntax Filter (!userAccountControl:1.2.840.113556.1.4.803:=2))

The synchronization can be tested by the **Test Connection** button on the bottom. If the test fails, or users listed are not correct, then check the **LDAP Search Filter** setting.

Step 8a (non-SfB) - Configure the phone number and/or SIP URI mapping(s) under the **Phone Numbers** section.

Step 1 - Click on the



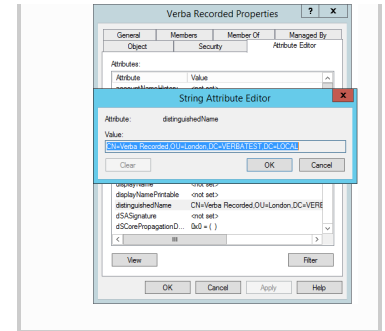
icon in order to add a new mapping.

Step 2 - Provide the LDAP attribute of the AD users to be synchronized into Verba as recorded extension (phone number or SIP URI).

Step 3 - If the whole phone number or SIP URI has to be synchronized, then provide the "(.*)" regex value in the Pattern to Match text box.

Step 4 - If no number or SIP URI transformation needed, then provide "\$1" in the Conversion Rule text box.

Step 5 - Repeat the steps if multiple phone numbers and/or SIP URIs have to be synchronized.



Phone Numbers

Synchronize Phone Numbers

Mapping Presets Custom

LDAP Attribute	ipPhone	Pattern to Match	(.*)	Conversion Rule	\$1
Type	Number/Address	Test:			

i Number and SIP URI conversion

There are cases when only a portion of the phone number or SIP URI is needed, or it has to be built from multiple elements.

If a portion of the phone number has to be cut down, modify the **Pattern to Match** value, so the part within brackets will match only the required part of the number. For example, let's say all the numbers in the AD start with 001, but it's not required for the recording. In this case, the "001(.*)" pattern can be used.

In other cases, the value found in the AD LDAP attribute is not enough, so we have to extend it. Let's say the SIP URIs are not stored in the AD, but the sAMAccountName is the same as the first part of the SIP URI. In this case, extend the **Conversion Rule** setting with the SIP domain part: \$1@contoso.com

Step 8b (Sfb/Lync) - Load the predefined mapping preset for Sfb/lync under the **Phone Numbers** section. Select **Lync** at the **Mapping Preset** setting, then click **Load**. The mapping settings will load automatically.

Phone Numbers

Synchronize Phone Numbers

Mapping Presets Lync

LDAP Attribute	msRTCSIP-PrimaryUserAddress	Pattern to Match	^[sS][0-9]{10}[pP];(.*)\$	Conversion Rule	\$1
Type	Number/Address	Test:			
LDAP Attribute	msRTCSIP-Line	Pattern to Match	^[tT][eE][lL];(.*)\$	Conversion Rule	\$1
Type	Number/Address	Test:			

i Removing the ext= part, and synchronizing the short extension

In some cases, the short extension number is stored within the msRTCSIP-Line LDAP attribute, right after the long number. In order to avoid synchronizing the short number together with the long number, change the **Pattern to Match** value at the second mapping to "^[tT][eE][lL];(. *);ext=.*\$".

If the short extension also required, then add a new mapping preset by clicking on the



set the **LDAP Attribute** to msRTCSIP-Line, set the **Pattern to Match** to "^[tT][eE][lL];.*;ext=(.*)\$" and the **Conversion Rule** to "\$1".

- ✔ The phone number and/or SIP URI synchronization can be tested also by the **Test Connection** button on the bottom. If the numbers and/or SIP URIs are not showing up, or they are in a wrong format, then check the mappings.

Step 9 - Click on the **New Users' Properties** tab on the top.

Step 10 - Set the recording setting of the synchronized users under the **Recording Settings** section.

Recording Settings

Recording Mode* Full ▼

Recording Rule --Choose-- ▼

For Cisco JTAPI based selective recording integrations only

Voice

Instant Messaging

Video

Desktop Screen

Screen & Application Share

Whiteboard

Poll / Q&A

File Share

SMS

Support of modalities depends on the recorded platform, more information [here](#).

Recorded Directions All
 Internal PSTN In PSTN Out External Federated In Federated Out Conference

All

Record Calls Answered by 3rd Party Forwarded Transferred Team Call Delegated

Only available for SFB/Lync recording

Step 11 - Click **Save**.

Configuring AD Synchronization for Supervisors or other users

Step 1 - Complete the **steps 1-7** from the **Configuring AD Synchronization for Recorded Users** section in order to set the basic settings of the AD Synchronization profile.

Step 2 - Click on the **New Users' Properties** tab on the top.

Step 3 - Tick the role(s) that is required for the synchronized users under the **Available Roles** section.

▼ Available Roles

- Standard User
- Superuser
- Contact Center Supervisor
- Data Retention Administrator
- eDiscovery Manager
- eDiscovery User
- Multi-tenant Administrator
- Quality Management Administrator
- Quality Management Agent
- Quality Management Evaluator
- Read-only Administrator
- Server Administrator
- Shared-only User
- Speech Analytics Administrator
- Speech Analytics User
- System Administrator
- System Supervisor
- User Administrator

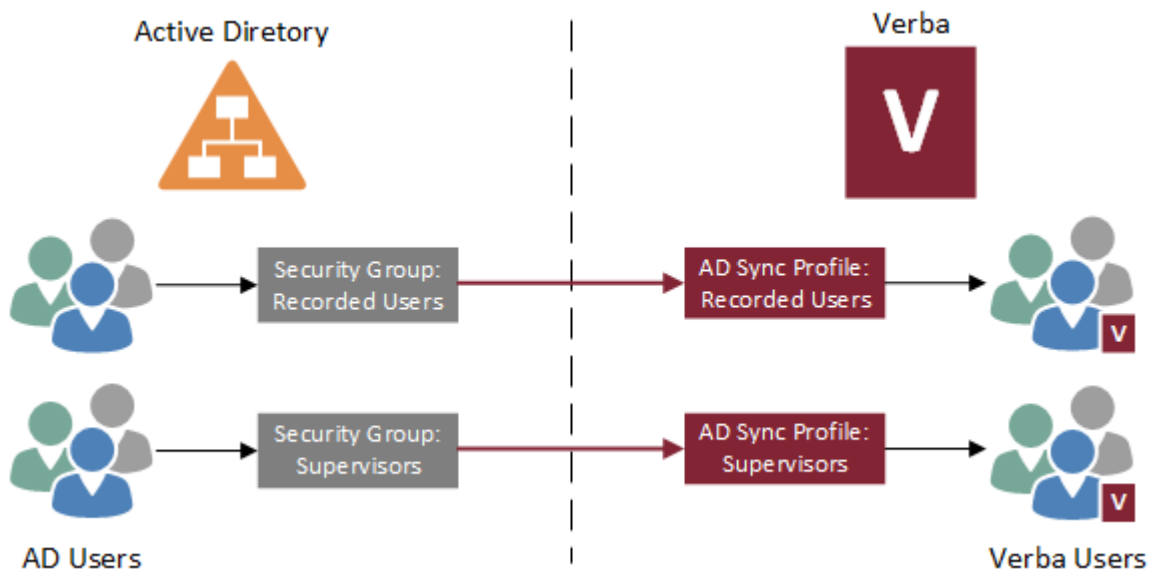
Step 4 - Click **Save**.

Configuring Active Directory Synchronization - Basic (Azure)

In small or medium-sized Verba deployments, usually only a few Active Directory Synchronization Profiles are configured. When the only requirement is synchronizing the recorded users, even one profile is enough.

In the case of these basic setups, AD users separated by security groups based on the purpose of the users in Verba. These users then synchronized into Verba by Active Directory Synchronization Profiles tied to these groups.

The disadvantage of this kind of setup is, that in case of many different user setting combinations in the Verba side, lot of security groups would be required because of the combination of the settings (E.g: Voice recorded, IM recorded, Voice and IM Recorded, etc.). In cases like this, see [Configuring Active Directory Synchronization - Advanced](#).



Synchronization Profile Sequence

The Sequence setting of the AD Synchronization Profiles determines the execution order of the profiles. It starts from the smallest one. In case of using a basic setup of AD Synchronization Profiles, this setting is important when a user is member of multiple synchronized AD security groups. Once a user gets synchronized by the first profile based on the sequence, it won't be modified any more by the subsequent profiles.

Prerequisites

Before creating the Verba Active Directory Synchronization Profile, a Connector App has to be registered in the Azure portal: [Registering a Connector App for Azure AD](#)

Configuring Azure AD Synchronization for Recorded Users

Step 1 - Go to the **Users \ Active Directory Synchronization** menu.

Step 2 - Click on the **Add New Active Directory Profile** link in the upper right corner.

Step 3 - Provide a **Description**.

Step 4 - Set the **Active Directory Type** to **Azure AD**.

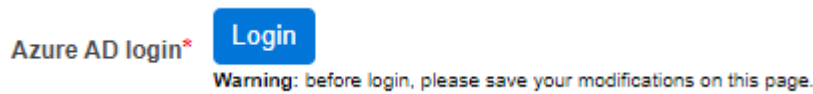
Step 5 - Provide the **Tenant ID** and the **Application ID**. These IDs can be found in the **Azure portal** by going to the **Azure Active Directory \ App registrations (Preview)** menu, and selecting the App:

Display name : Verba
Application (client) ID : 5a1e5acb-9bb4-4e36-9759-a7b18ae4990e
Directory (tenant) ID : df530937-2dd6-44ed-8ae9-77a9db3f82d7
Object ID : 2dee5dfa-3623-4f0e-97cf-efcc5f760aaf

Step 6 - Provide the **Application Secret Pass**. It can be gathered when registering the Connector App.

Step 7 - Scroll down to the bottom of the page, then click on the **Save** button.

Step 8 - Under the Azure AD Information section, a **Login** button appears. Click on that button.



Step 9 - The page will redirect to the Azure login screen. Log in with your Azure credentials, then accept the permissions requested by the application. The page will redirect back to the Verba Web Application.

Step 10 (Optional) - If you want to synchronize users based on user filter, for example, based on department, then set the **Azure Search Base Entry** setting to **User**. In the case of user filter based synchronization, **skip the Steps 11-14**, and see the **side note** for instructions.

Step 11 - Provide a group search filter at the **Azure AD Entry Search Filter** setting. For example, for searching for groups with name starting with "ad", provide "startswith(displayName,'ad')".

A screenshot of the application configuration page. It shows several input fields: 'Tenant ID' (df530937-2dd6-44ed-8ae9-77a9db3f82d7), 'Application ID' (e5b2d8ed-d416-450f-b53e-b7e446d996f9), 'Application Secret Pass' (masked with dots), 'Azure AD login' (with a 'Login again' button and a warning message), 'Azure Search Base Entry' (set to 'Group'), and 'Azure AD Entity Search Filter' (set to 'startswith(displayName,'ad')'). There is also a 'Select Groups' button and a checkbox for 'Decode "userPrincipalName" attribute'.

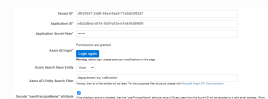
Step 12 - Click **Select Groups**.

Step 13 - The results will appear based on the filter provided in a new window. Select the groups that you want to use for synchronizing the users.

Using User filter instead of Group filter

(the part after [https://graph.microsoft.com/v1.0/users?\\$filter="](https://graph.microsoft.com/v1.0/users?$filter=)).

For example: "department eq 'callcenter'".



For the filter parameters and the user properties, see:

<https://docs.microsoft.com/en-us/graph/query-parameters#filter-parameter>
<https://docs.microsoft.com/en-us/graph/api/resources/user?view=graph-rest-1.0>

✓ Groups successfully read from Active Directory.

Group DN	Converted Name
<input checked="" type="checkbox"/> 90b75f43-4304-4c32-8464-43dd07c6e3d6	AD Group 3
<input type="checkbox"/> ba96ea93-d2ed-4957-82f1-267b6e423922	AD Group 1
<input checked="" type="checkbox"/> f7c258ce-ed58-4991-a14d-309ca2a3f1b5	AD Group 2

Update Active Directory Profile Configuration

Close

Step 14 - Click on the **Update Active Directory Profile Configuration** button. The selected groups will appear in the Synchronization Profile configuration.

Step 15 - Configure the phone number and/or SIP URI mapping(s) under the **Phone Numbers** section.

Step 1 - Click on the



icon in order to add a new mapping.

Step 2 - Provide the [user property](#) of the Azure AD users to be synchronized into Verba as recorded extension (phone number or SIP URI).

Step 3 - If the whole phone number or SIP URI has to be synchronized, then provide the "(.*)" regex value in the Pattern to Match text box.

Step 4 - If no number or SIP URI transformation needed, then provide "\$1" in the Conversion Rule text box.

Step 5 - Repeat the steps if multiple phone numbers and/or SIP URIs have to be synchronized.

Phone Numbers

Synchronize Phone Numbers

Mapping Presets: Custom

AD Attribute	ipPhone	Avaya Password	Avaya Password Attribute
Type	Number/Address	Pattern to Match	Conversion Rule
		(*)	\$1
		Test	

Number and SIP URI conversion

There are cases when only a portion of the phone number or SIP URI is needed, or it has to be built from multiple elements.

If a portion of the phone number has to be cut down, modify the **Pattern to Match** value, so the part within brackets will match only the required part of the number. For example, let's say all the numbers in the AD start with 001, but it's not required for the recording. In this case, the "001(.*)" pattern can be used.

In other cases, the value found in the AD LDAP attribute is not enough, so we have to extend it. Let's say the SIP URIs are not stored in the AD, but the sAMAccountName is the same as the first part of the SIP URI. In this case, extend the **Conversion Rule** setting with the SIP domain part: \$1@[contoso.com](#)

Step 16 - Click on the **New Users' Properties** tab on the top.

Step 17 - Set the recording setting of the synchronized users under the **Recording Settings** section.

Recording Settings

Recording Mode*

Recording Rule

For Cisco JTAPI based selective recording integrations only

Voice

Instant Messaging

Video

Desktop Screen

Screen & Application Share

Whiteboard

Poll / Q&A

File Share

SMS

Support of modalities depends on the recorded platform, more information [here](#).

Recorded Directions All
 Internal PSTN In PSTN Out External Federated In Federated Out Conference

All

Record Calls Answered by 3rd Party Forwarded Transferred Team Call Delegated

Only available for SIB/Lync recording

Step 18 - Click **Save**.

Configuring AD Synchronization for Supervisors or other users

Step 1 - Complete the **steps 1-14** from the **Configuring Azure AD Synchronization for Recorded Users** section in order to set the basic settings of the Azure AD Synchronization profile.

Step 2 - Click on the **New Users' Properties** tab on the top.

Step 3 - Tick the role(s) that is required for the synchronized users under the **Available Roles** section.

▼ Available Roles

- Standard User
- Superuser
- Contact Center Supervisor
- Data Retention Administrator
- eDiscovery Manager
- eDiscovery User
- Multi-tenant Administrator
- Quality Management Administrator
- Quality Management Agent
- Quality Management Evaluator
- Read-only Administrator
- Server Administrator
- Shared-only User
- Speech Analytics Administrator
- Speech Analytics User
- System Administrator
- System Supervisor
- User Administrator

Step 4 - Click **Save**.

Troubleshooting

The most common problems and their solutions are listed in the [Troubleshooting Azure Active Directory Synchronization](#) article.

Troubleshooting Azure Active Directory Synchronization

In this article, the most common problems are listed for troubleshooting purposes.

Error symptoms	Solution
<p>The synchronization doesn't run and the following error message can be found in the web application log:</p> <pre>java.lang.Exception: Missing admin consent for Graph API</pre>	<p>Although the Active Directory Synchronization profile is set in the web application and the connector application is registered in the Azure Active Directory, administrator consent must be added to the connector application from the web application.</p> <p>Visit the Active Directory Synchronization profile configuration page and proceed with the step 8 and step 9 of the article Configuring Active Directory Synchronization - Basic (Azure).</p>
<p>The synchronization doesn't run or the Group searching or the Test Connection doesn't work. The following error message can be found in the web application log:</p> <pre>com.microsoft.graph.http.GraphServiceException: Error code: Authorization_RequestDenied Error message: Insufficient privileges to complete the operation.</pre>	<p>The Azure Active Directory connector application's permissions are misconfigured. Grant the required permissions to the configured application with step 17 of the article Registering a Connector App for Azure AD.</p> <p>Then go back to the Active Directory Synchronization profile configuration page in the Verby web application and give admin consent to the new permissions too. To achieve that in the Azure AD login section click on the "Login again" button and log in with your Azure Active Directory administrator account to accept the new permissions.</p>
<p>Error during adding admin consent. After clicking on the "Login" button on the Active Directory Synchronization profile configuration page the browser was redirected to a Microsoft Sign In page. After logging in with an Active Directory user and accepting the application's permission requests, the following error message was shown:</p> <pre>AADSTS50011: The reply URL specified in the request does not match the reply URLs configured for the application: '{{YOUR_APPLICATION_ID}}'.</pre>	<p>There is a misconfiguration in the connector Azure Active Directory application.</p> <p>Go back to the Active Directory Synchronization profile configuration page in the web application. Check the used URL in the browser. Based on the current architecture it can be "localhost", a valid CNAME or IP address. Save this value for later.</p> <p>Visit the connector application configuration page in the Azure Active Directory which was created based on this article: Registering a Connector App for Azure AD. Go to the Authentication menu and check the Redirect URIs under the Web platform.</p> <p>In this list your Verba web application URL, you check previously, must be listed. For one application multiple Redirect URI can be stored. If it doesn't exist, add it to the list with step 5 of the article Registering a Connector App for Azure AD.</p> <p>Otherwise, check the URLs which has been added already and use the Verba web application with one of these URLs.</p> <p>Go back to the Active Directory Synchronization profile configuration page in the Verby web application. Double-check the URL in the browser. Try the log-in process again.</p>

Error during adding admin consent. After clicking on the "Login" button on the Active Directory Synchronization profile configuration page the browser was redirected to a Microsoft Sign In page. This page shows the following error message:

```
AADSTS900023: Specified tenant identifier '{{YOUR_TENANT_ID}}' is neither a valid DNS name, nor a valid external domain.
```

The configured Tenant ID is not valid. Visit the Active Directory Synchronization profile configuration page and proceed with **step 5** of the article [Configuring Active Directory Synchronization - Basic \(Azure\)](#). Try the log-in process again.

Error during adding admin consent. After clicking on the "Login" button on the Active Directory Synchronization profile configuration page the browser was redirected to a Microsoft Sign In page. This page shows the following error message:

```
AADSTS700016: Application with identifier '{{YOUR_APPLICATION_ID}}' was not found in the directory '{{YOUR_TENANT_ID}}'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.
```

The configured Application ID is not valid. Visit the Active Directory Synchronization profile configuration page and proceed with **step 5** of the article [Configuring Active Directory Synchronization - Basic \(Azure\)](#). Try the log-in process again.

New Users' Properties Rules

Above the capabilities of the Active Directory Synchronization Profiles, Verba provides the ability for mapping certain LDAP attributes and security group (or OU) memberships to specific properties of the synchronized AD users. With the New Users' Properties Rules, multiple rule sets can be created in order to fully automatize the user management based on Active Directory. To configure the rules, go to the **Users \ Active Directory Synchronization** menu, then click on the **Manage New Users' Properties Rules** link in the upper right corner

New Users' Properties Rules List

Once the **Manage New Users' Properties Rules** link is clicked, the rule list page will show up. On this page, it's possible to search based on the Name or the Description of the rules.

The list can be exported into XLS, RTF or PDF.

Find and List New Users' Properties Rules

Name ▾	begins with ▾	<input type="text"/>	<input type="button" value="Find"/>
Priority ↕	Name ↕	Description ↕	ID ↕
200	Announcement rules	Announcement groups mapped to Verba users	931BD3A4-700A-4F31-9F40-75F1FDA82C1B
100	Retention rules	Retention groups mapped to Verba users	5B8E9562-58B4-4E9B-91E5-E31C55F707CD

2 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Adding New Rules

New rules can be added by clicking on the **Add New Rule** link in the upper right corner of the New Users' Properties Rules List page.

ID

Priority *
Rules with the higher priority overwrite the lower priority rules.

Name *

Description

Default LDAP Query

Select an AD Profile to validate and list the results of the LDAP Query

Setting Name	Description
ID	Unique ID generated automatically after saving.
Priority	The priority setting determines the execution sequence of the rules. The highest priority will be executed first.
Name	The name of the rule.
Description	Short description of the rule.
Default LDAP Query	The defined rule items will be executed only on the AD users which falls into the LDAP filter defined here.
Validate and Run	Runs the LDAP query provided using the selected Active Directory Synchronization profile, and shows the users found.

New rule items can be added by clicking on the



icon. Once the icon clicked, a new rule item section will appear. Multiple rule items can be added to a single rule. If a rule item is no longer required, then it can be removed by clicking on the **Remove Item** link.

ID

LDAP Query

--Choose-- Validate and Run

Select an AD Profile to validate and list the results of the LDAP Query

Property

Set To

Setting Name	Description
ID	Unique ID generated automatically after saving.
LDAP Query	The LDAP filter for the specific AD user attribute or membership, based on which the Verba side setting will be set.
Validate and Run	Runs the LDAP query provided using the selected Active Directory Synchronization profile, and shows the users found.
Property	The Verba user or extension property to set.
Set To	The value to set at the property set above.

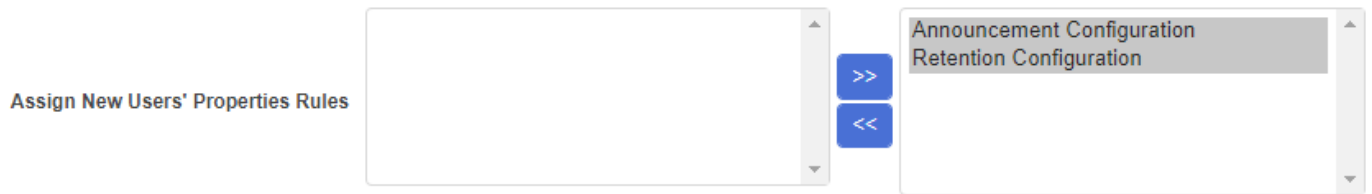
Once all the required rule items configured, click on the **Save** button to save the new Rule.

Assigning the Rules to the Active Directory Synchronization Profiles

Step 1 - Go to the Users \ Active Directory Synchronization menu.

Step 2 - Select the AD Synchronization Profile. (In the case of merged profiles, select the base profile)

Step 3 - At the **Assign New Users' Properties Rules** setting, assign the rules by clicking on the >> icon.



Step 4 - Click **Save**.

Registering a Connector App for Azure AD

In order to use the Verba with Azure Active Directory, a Connector App has to be registered with the proper settings.

Registering a Connector App for Azure AD

Step 1 - Log in to <https://portal.azure.com/>.


Step 2 - In the left menu, select **Azure Active Directory**, then in the next menu level select **App Registrations**.

Step 3 - Click on the **New registration** button.

Step 4 - Provide a **name**, then click on the **Register** button.

Step 5 - Once the app is registered, click on the **Authentication** menu.

Step 6 - Under the **Redirect URIs** section, set the **Type** to **Web**, and set the **Redirect URI** to the Verba web application URL the following way: https://your_verba_mr_server/verba/azureGraphApiAuthenticator.do

TYPE	REDIRECT URI
Web	https://your_verba_mr_server/verba/azureGraphApiAuthenticator.do ✓ 
Web	e.g. https://myapp.com/auth

Step 7 - Under the **Advanced settings** section, the **Logout URL** has to be set. Since Verba is not using this, it can be anything, so just type in the example.

Logout URL  ✓

Step 8 - Click **Save**.

Step 9 - Click on the **Certificates & secrets** menu.

Step 10 - Under the **Client secrets** section, click on the **New client secret** button.

Step 11 - Provide a **description** for the client secret, set the **expiration**, then click on the **Add** button.

Add a client secret

Description

Verba client secret

Expires

- In 1 year
 In 2 years
 Never

Add

Cancel

Step 12 - Once the client secret is created, click on the **copy icon** next to the secret, and save it for later. **It cannot be copied later!**

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	
Verba client secret	12/31/2299	oin!=pJmttVG9YVW]X	

Step 13 - Click on the **API permissions** menu.

Step 14 - Click on the **Add permission** button.

Step 15 - In the right panel, select **Microsoft Graph**, then select **Application permissions**.

Step 16 - Select **Directory.Read.All**, **Group.Read.All** and **User.Read.All**, then click on the **Add permissions** button.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (4)			
Directory.Read.All	Application	Read directory data	Yes Not granted for Verba...
Group.Read.All	Application	Read all groups	Yes Not granted for Verba...
User.Read	Delegated	Sign in and read user profile	-
User.Read.All	Application	Read all users' full profiles	Yes Not granted for Verba...

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

Active Directory Synchronization Configuration Reference

The following tables describe all the configuration items in the Active Directory Synchronization Profiles.

Active Directory General Information Section

Configuration Parameter Name	Description	Sample Value
Description	The profile's talkative name	Recorded Users
Enabled	Disabled profiles will not be synchronized.	Yes
Sequence	Each user will be processed by only one Active Directory Profile, so the Profile with the smaller sequence will process users read from multiple profiles.	100
Active Directory Type	The type of the Active Directory the profile will be connected to. This setting determines whether the LDAP Active Directory or the Azure Active Directory related settings will be shown in the next section.	LDAP

Active Directory Information Section

Configuration Parameter Name	Description	Sample Value
LDAP Host	Hostname of the AD / LDAP server.	ad.mycompany.com
LDAP Port	Port number of the AD / LDAP server. The default port is 389 (636 if SSL is used), Active Directory Global Catalog Forest-Wide port is 3268 (3269 if SSL is used).	389
Use SSL	If enabled Verba uses secure connection to connect to your LDAP host.	
Character Encoding	What character encoding should be used when reading from the AD / LDAP server.	ISO-8859-1
LDAP User Distinguished Name or Domain User Name	The full username that Verba will use when connecting to the AD / LDAP server. This account should have the proper privileges to read the synchronized users. For anonymouslogon, leave it empty.	mycompany\verba_account
LDAP Password	The password that Verba will use when connecting to the AD / LDAP server. For anonymouslogon, leave it empty.	secret
LDAP User Search Base	The DN of the container where the synchronized users can be found. Base DNs can be fetched by the button next to the input field.	OU=Users,DC=mycompany,DC=com
LDAP Search Filter	A valid LDAP Search expression that will be used to filter the entries under LDAP User Search Base.	(&(objectclass=person)(memberOf=CN=Verba_Group,DC=yourdomain,DC=com)) Please make sure that there is no space character at the end!
Search Entry	Fill it with either a simple string like 'Verba_Rec*' or with a valid LDAP filter like (CN=Verba_Rec*)	

Simple Paging	Allows Verba to synchronize more than 10,000 people. Turn this option on if the number of users may exceed 10,000.	
Follow Referrals	Indicates how to handle referrals. If checked Verba follows referrals. If unchecked Verba ignores referrals.	checked
Dereference Policy	<p>The dereference policy is an element of a search quest that specifies how Verba should handle alias entries that may be encountered during search processing.</p> <p>Allowed alias dereference policy values include:</p> <ul style="list-style-type: none"> • Never: Indicates that Verba should not dereference any aliases that it encounters. • Searching: Verba should dereference any entries within the scope of the search operation to determine whether they match the search criteria. The entry specified as the search base DN will not be dereferenced. • Finding: Verba should dereference the entry referenced as the search base DN if it is an alias, but any other alias entries within the scope of the search operation will not be dereferenced. • Always: Verba will dereference any alias entries within the scope of the search operation and will also dereference the base entry if it is an alias. 	Never

Azure AD Information

Configuration Parameter Name	Description	Sample Value
Tenant ID	The ID of the Azure AD tenant which is being used	
Application ID	The ID of the Connector App for Verba	
Application Secret Pass	The secret pass of the Connector App for Verba	
Azure AD Login	Login credentials for Azure AD. The login button will be shown after the profile is saved.	
User Search Filter	Graph API users filter parameter.	department eq 'callcenter'
Decode "userPrincipalName" Attribute	If the checkbox above is checked, then the "userPrincipalName" attribute value of Guest users from the Azure AD will be decoded to a valid email address.	

Merge with Other profiles Section


Observer user for Four Eyes Login	Description	Sample Value
Profiles to be Merged	List of the Active Directory Synchronization profiles to be merged. The merged profiles will add additional properties to the users synchronized by the base profile.	
Merge Extensions	Sets if the extension configuration (Phone Number Section from the LDAP Directory Information tab, and the corresponding Recording Settings, Data Sources, Announcement settings from the New Users' Properties tab) will be merged from the profiles added to the Profiles to beMergedlist.	

Merge Groups	Sets if the group configuration (New Users' Groups setting from the New Users' Properties tab) will be merged from the profiles added to the Profiles to beMergedlist.	
Merge Roles	Sets if the role configuration (Available Roles setting from the New Users' Properties tab) will be merged from the profiles added to the Profiles to beMergedlist.	

Synchronized LDAP Attributes Mapping Section

Configuration Parameter Name	Description	Sample Value
Display Name	LDAP attribute name that stores the users' full name.	cn
Login ID	LDAP attribute name that stores the users' account name.	sAMAccountName
User Matching ID		
E-mail Address	LDAP attribute name that stores the users' email address	mail
Location Attribute	LDAP attribute name that stores the users' location.	co
Location	This setting will be used when the Location Attribute is not set up or the attribute is not filled in for a user in the AD.	
Retention Period (days) Attribute	LDAP attribute name that stores the users' retention period	
Retention Period (days)	This setting will be used when the Retention Period (days) Attribute is not set up or the attribute is not filled in for a user in the AD.	
Automatically Delete Conversations after the Retention Period is Over	Sets if the recorded conversations belonging to the user should be deleted after the retention period is over	

Phone Number Section

Configuration Parameter Name	Description	Sample Value
Synchronize Phone Numbers	If it is not turned on, Verba will not synchronize phone numbers. If the profile stores users who should not have phone numbers, then this setting should be turned on and no extension mapping should be set up.	
Mapping Presets	You can use our Lync preset or you can create your own custom mappings. New extension maps can be added by pressing the  button below.	
LDAP Attribute	LDAP attribute name that stores the users' phone number or SIP address.	msRTCSIP-Line
Pattern to Match	A regular expression that will be replaced.	^[tT][eE][lL]:(.*);ext=.*\$ ^[tT][eE][lL]:.*;ext=(.*)\$
Conversion Rule	The regular expression in "Pattern to Match" setting will be replaced by this text or regular expression.	\$1

Below you can see an example extension mapping setup:

Synchronize Phone Numbers

Mapping Presets Lync Load

	LDAP Attribute	msRTCSIP-PrimaryUserAddress	Pattern to Match	^[sS][iI][pP]:(.*)\$	Conversion Rule	\$1
	Type	Number/Address	Test:	<input type="text"/>	<input type="button" value="→"/>	<input type="text"/>
	LDAP Attribute	msRTCSIP-Line	Pattern to Match	^[tT][eE][lL]:(.*)\$	Conversion Rule	\$1
	Type	Number/Address	Test:	<input type="text"/>	<input type="button" value="→"/>	<input type="text"/>

Verba Groups based on AD Organization Unit Hierarchy Section

Configuration Parameter Name	Description	Sample Value
Enable	If it is enabled Verba will generate hierarchical groups based on Active Directory Organization Unit hierarchy	true
Group Naming - Reverse Order	If this setting is turned on, then the name of the created Verba group will be something like com / company / Organization / Group Name Otherwise it will be Group Name / Organization / company / com	true
Group Naming - Separator	If this field is empty, then the attributes will be concatenated in their original form: CN=GroupName,DC=yourdomain,DC=com	/
Group Naming - Skip Top Level	If the top levels of the Organization should be skipped this field can define the number of skipped level.	1 - In this case, the highest level (DC=com) will be skipped.

Groups Section

Configuration Parameter Name	Description	Sample Value
Synchronize Groups	If it is enabled then Verba will also create groups for the imported users.	true
Verba Groups based on AD Groups	If it is enabled then Verba will follow the AD Group relationships and will create nested groups if required.	true
Synchronized Group Attributes	Comma-separated list of attributes that should be read from a User object.	memberOf
Group Naming - Template	If the created Verba group name should be the simple name of the security group, then set this setting to CN. If the Verba group's name should contain the whole DN of the group, then set this setting to empty.	CN
Group Naming - Reverse Order	If this setting is turned on, then the name of the created Verba group will be something like com / company / Organization / Group Name Otherwise it will be Group Name / Organization / company / com	true

Group Naming - Separator	If this field is empty, then the attributes will be concatenated in their original form: CN=GroupName,DC=yourdomain,DC=com	/
Filtered Synchronization	Possible values are: <ul style="list-style-type: none"> Ignore selected groups: Verba will ignore the selected groups and will only create groups with the remaining ones. Synchronize selected groups only: Verba will only create the selected groups. 	Synchronize selected groups only
Select Group	Select the groups you would like to be (or not to be, it depends on the Narrow option above) synchronized from the Active Directory. You can select multiple groups.	

Manager/Direct Reports Section

Configuration Parameter Name	Description	Sample Value
Generate Groups Based on Manager/Direct Reports	If it is enabled then Verba will also create groups based on the direct reports. (Note: Feature is enabled only on the synchronized users)	true
Group Name	Naming template for the generated groups. The following placeholders can be used: [manager_name] [manager_login] [manager_department] [manager_company]	Direct Reports of [manager_name] ([manager_login])
Add All Parent Managers	If enabled the synchronization will add the manager's manager with the same privileges to the group	true
Manager Roles		
Supervisor	Defines group supervisor permission for the manager(s)	true
Manager	Defines group manager permission for the manager(s)	true
Administrator	Defines group administrator permission for the manager(s)	true

Test Connection Section

This section can be used to quickly test whether the configuration is proper.

Test Connection

Determine Number of Users

Maximum Number of Users to be Listed

[Test Connection](#)

Run Full Synchronization

By default, full synchronization is done only at the first run of the Active Directory Synchronization Profile. After that only differential synchronization will be done. If a full synchronization is needed, the checkbox at the Run Full Synchronization setting has to be ticked. This checkbox ticked automatically when the Active Directory Synchronization profile was modified.

New Users' Properties tab

The New Users' Properties tab can be used to configure what properties should new users be synchronized with to Verba.

A user is considered a new user when it has not previously been synchronized with a certain profile. So for example, if a user was previously synchronized by profile A, but inADit gets moved to another location and now is being synchronized by profile B, then the user is considered a new user. Settings from the new profile replace the settings in the old profile. Previous manual changes are also removed. (The only exception being the Extension assignments)

Active Directory Profile Configuration

LDAP Directory Information	New Users' Properties	Log
----------------------------	------------------------------	-----

The basic user configuration can be set up here such as Password Generation, Language, Timezone, etc. Since these properties are not synchronized from the AD, these can be customized later for the individual users.

Configuration Parameter Name	Description	Sample Value
User type		Standard
Change Password at First Logon		
Verba Password Generation		Login name + 123
Language		English (en)
Default Timezone		GMT-05:00 - Jamaica Eastern Standard Time
Authorization Workflow		
Retention Period (days)		30
Automatically Delete Conversations after the Retention Period is Over		
Observer User (four eyes login)	Observer user for Four Eyes Login	
Observer Group (four eyes login)	Observer group for Four Eyes Login	

Associated Extension Settings section

Configuration Parameter Name	Description	Sample Value
Recording Mode	<p>Here you can select from the available recording modes and apply them to a phone number. The following valid values apply:</p> <ul style="list-style-type: none"> • Full mode - All calls are recorded for the phone number. • On-demand mode - Only marked calls are recorded. • Controlled mode - Gives ability to manually start / stop the recording. • Do not record mode - The given extension will not be recorded at all. • Never Record mode - The calls never will be recorded, even if the other participant is recorded. • Relay Only mode - The call will be relayed but not recorded by the Verba proxy. 	Full

Voice	If enabled, Verba records the imported user's voice.	-
Instant Messaging	If enabled, Verba records the imported user's instant Messages.	-
Video	If enabled, Verba records the imported user's video.	-
Desktop Screen	If enabled, Verba records the imported user's desktop screen.	-
Screen & Application Share	If enabled, Verba records the imported user's screen and application window shares in the meetings.	
Whiteboard	If enabled, Verba records the imported user's whiteboard presentations in the meetings.	
Poll / Q&A	If enabled, Verba records the imported user's poll and Q&A actions in the meetings.	
File Share	If enabled, Verba records the imported user's file shares.	
SMS	If enabled, Verba records the imported user's SMS messages.	
Recorded Directions	Sets which directions of the users' calls will be recorded.	All
Record Calls Answered by 3rd Party	Sets in which scenarios the calls will be recorded when answered by a 3rd party.	All

Data Sources section

Configuration Parameter Name	Description	Sample Value
Record Every Platform	Sets if the users' calls will be recorded regardless the platform.	
Recorded Platforms	If the Record Every Platform setting is turned off, then the list represents the platforms where the users' calls should be recorded.	
Import from Every Source	Sets if the users' calls will be imported regardless the import source.	
Import Sources	If the Import from Every Source setting is turned off, then the list represents the sources where the users' calls should be imported from.	

SfB/Lync Recording Announcement section

In case you have configured the Verba Lync Recording Announcement service then the following settings will turn on the announcement for the imported users.

Configuration Parameter Name	Description	Sample Value
Play Notification for PSTN /Federated Inbound Calls	If enabled and the announcement is configured then Verba will play notification for PSTN and federated inbound calls for the imported users.	-
Play Notification for PSTN /Federated Outbound Calls	If enabled and the announcement is configured then Verba will play notification for PSTN and federated outbound calls for the imported users.	
Play Notification for Conference Calls	If enabled and the announcement is configured then Verba will play notifications for conference calls for the imported users.	-

IM Notification for Conference Calls	If enabled and the announcement is configured then Verba will play IM notifications for conference calls for the imported users.	-
---	--	---

Cisco Recording Announcement section

In case you have configured the Verba Cisco Recording Announcement service then the following settings will turn on the announcement for the imported users.

Configuration Parameter Name	Description	Sample Value
Play Notification for Inbound Calls	If enabled and the announcement is configured then Verba will playnotification for PSTN inbound calls for the imported users.	-
Play Notification for Outbound Calls	If enabled and the announcement is configured then Verba will playnotification for PSTN outbound calls for the imported users.	

Assigned Roles and Available Roles section

Sets which Verba Roles should the newly created users have. Since Verba Roles are not synchronized from the AD, these can be customized later for the individual users.

New Users' Groups section

Here you can view the list of your existing groups inside Verba and you can select to which group(s) you would like to add your imported users.

If you don't select any groups here and you don't use the Groups section from the LDAP Directory Information tab then the users will automatically be assigned to the "default" group.

Advanced Active Directory Synchronization Settings

There are additional settings which help you fine-tune how the Active Directory Synchronization works. In order to reach them, go to the **Administration / Verba Servers** menu, select your **Media Repository** (or Combo) server and go to the **Change Configuration Settings** tab. The settings can be found under the **Web Application / Active Directory Synchronization** node.

Configuration Parameter Name	Description	Sample Value
Run Active Directory Synchronization on Server	If enabled, then the synchronizations will be enabled to run on the server.	Enable
Page Size	Number of users to be read in one cycle.	1000
Enable Reverse Check on Synchronization Attempts	If enabled, then after all of the users read, the first user will be red in reverse order, and it will be compared with the last user red in the first loop. If it does not match, then the synchronization will be rolled back.	Enable
Enable Full Reverse Check on Synchronization Attempts	If enabled, then all of the users will be read in reverse order, and will be compared with the original results.	Disable
Automatic Rollback Threshold on Invalidated Users [%]	If set, then all synchronization runs which changes more percent of the previously synchronized users than the value will be rolled back.	0

Send email notification on successful AD sync runs	If enabled, then a notification email will be sent out after every active directory synchronization runs.	No
--	---	----

Bulk User and Extension Update

Available in version 8.7 and later

Bulk User and Extension Update is accessible from the menu under **Users -> Bulk User and Extension Update**. The Bulk User Update tool lets administrators change the parameters of a group of users without having to change each user one by one.

First, you can define the attributes based on which the system will compile a list of users (and those extensions that do not belong to a user) that match the criteria. Then it will update the user attributes and the attributes of the extensions, that belong to these users. (And extensions that do not belong to users if a certain checkbox is selected as shown below)

This page lists the previously executed Bulk User Updates.

Creating a bulk update profile

A new profile can be created by clicking on the *Add New Bulk User Update Profile* button at the top right corner of the page.

On this page, it can be defined which users' parameters should be updated.

- **Description** - Give a description on what this update will cover
- **Update Extensions that do not belong to a User** - By default only Extensions that match the defined criteria are selected that belong to users. By selecting this option, unassigned Extensions will also be updated.
- **Update Users' Every Extension** - All of the defined users' extensions will be updated, even defining users based on a certain extension that they have. For example, a user has 3 extensions. The filter criterion is to select users where the extension starts with 123. In this case by default the fields are only updated for this one extension. By selecting the "Update Users' Every Extension" option, all 2 extensions of this user will be updated.
- **Filtering Criteria** - Define which users' attributes should be updated
- **Update Fields** - Define which fields of the selected users and extensions should be updated. The new value can be defined here as well.

Once you have set up the profile, click on *Save* to save the profile.

You can quickly check if the criteria that you have set up select the users that you intended by clicking on the *List Affected Users/Extensions* button.

Running a bulk update profile

The *Save and Run* button appears at the bottom, next to the *Save* button. Click on this to run the update.

You can use the *Log* tab at the top left corner to verify the results.

This update profile will appear in the previous list, you can change and run this update again in the future.

Bulk user import

The bulk user import feature is designed to help administrators (the administrator and the system administrators) in adding several users to the system using only a few mouse clicks (e.g. during the initial installation). This feature provides limited capability for modifying users as well.

In order to import users from the above-mentioned sources, select **Administration / Bulk User Import** from the menu. The User Import Wizard appears.

Select data source

As a first step, you have to select the source for the import. Simply click on the desired item and click on the **Next** button.

The following picture shows the User Import Wizard, where you select a source media for the import:

User Import Wizard - Step 1 of 3

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

Before execution you can **review and modify** the planned import. Select what users the review will **show** and **mark for import**.

Please select source media for import:

- CSV File
- Microsoft Active Directory
- General LDAP

Before execution you can **review and modify** the planned import. Select what users the review will **show** and **mark for import**:

- Show all, mark all (add and update)
- Show all, mark new only (add)
- Show all, mark existing only (update)
- Show new only (add)
- Show existing only (update)

[Next](#)

Configure the data source

This step of the User Import Wizard is different for each supported data source:

- [Using CSV user import](#)

Verify the import

The final step of the User Import Wizard gathers all available information for the previously defined source.

Depending on the applied source, not all fields are filled in automatically. e.g. Cisco Unified Communications Manager DC Directory does not contain language settings for a given user. In order to help administrators quickly define missing parameters for all users, the top of the page contains functions to modify all entries at once. You only have to define the field, which you want to set and then by pressing the **Modify** button, the page will be reloaded with the modified information.

You can also modify all entries one by one.

Before importing the users into the Verba database, if any modifications were completed, you have to save the changes by pressing the Enforce Changes button. If your list contains more than 100 records, you can move between the pages, but be careful, because modifications done on a page will be lost by moving to another page (if Enforce Changes button was not pressed).

When you are ready, simply press the **Start Import** button.

After the import operation, you will be directed to a page describing the result of the operation.


Using CSV user import

Overview

You can upload user information using CSV file. Click on the Browse button to locate the CSV file on your hard disk, then press the **Upload** button.

You can export these files from Excel, or create them manually by following the rules below:

- Each record must be on a separate line
- The fields must be separated by commas or semicolons (the appropriate option has to be selected on the upload page)
- If you cannot add a field, leave it empty (do not skip fields at the end of the row, leave them empty e.g. ;;;)
- If you need comma or semicolon or newline character in a field, you have to surround the entire field with quotation marks ("this is a field, with a comma")
- If you need quotation mark in a field, you have to insert double quotation marks instead of one and you also have to surround the entire field with quotation marks ("this is a field with ""quotations" ")
- The system automatically trims spaces from the beginning and the end of the field
- You can leave the header row in the CSV file, but on the upload page, you have to check the Skip First Row (Heading) option

 The CSV file must be **UTF-8 encoded**, otherwise, names with local characters might get corrupted.

After uploading the file you will see the contents of the file in a table format and you can make changes to the values before executing the import.

List of columns in the CSV file

The following table describes the required fields in the CSV file:

 You can download sample CSV file by clicking on the **Download Sample XLS File** link on the top right corner.

Column	Column Name	Description	Value requirements/rules
1	User name	Full name of the user, e.g. used in searches.	Required Maximum 64 characters
2	Login ID	Login name of the user.	Required Maximum 32 characters Only alphanumeric, @and . (dot) - you can use the email address
3	Language	The language of the user interface.	The following valid values apply: en, hu, de, fr, fr_CA
4	E-mail address	Email address of the user used to send requested call information to the user.	Maximum length: 128

5	Valid From yyyy.mm.dd	First date when the user can log in. By default, the user cannot see conversations for associated extensions before this date.	The following date formats can be used: yyyy.mm.dd yyyy-mm-dd yyyymmdd If the field is empty, current date is used.
6	Phone Mapping	List of phone numbers / Extensions associated with the user.	Semicolon separated list of one phone numbers or URIs (e.g. SIP address) If an Extension does not exist it is created using the Recording Mode field (see below)
7	Password (MD5 Hash)	MD5 hash of the user's password.	If empty, the login name is used as password E.g use an online MD5 calculator to calculate it.
8	Change Password at Next Login	Forces users to change their password when they next log in to the system.	1 - password must be changed 0 - no password change required
9	Groups	List of Groups where the user is a member.	Semicolon-separated list of Group names If a Group does not exist it is created
10	Role API Names	List of Roles associated with the user.	Newline (Alt + Enter in Excel) separated list of Role names. E.g.: r_system_supervisor r_user_administrator r_superuser r_system_administrator r_standard_user
11	Recording Mode	Defines how the phone numbers listed in the Phone Mapping field should be recorded.	full - records in always-on mode on-demand - records on-demand manual - records controlled no - do not record
12	Time Zone	Time Zone of the user (e.g. used for displaying time in searches)	Time Zone ID. You can find the timezone IDs on the web interface under Administrator / User on any user configuration page. Use the ID in the second half of the timezone you see in the drop-down list. E.g. if you see "GMT+01:00 - Europe/Stockholm" to Time Zone ID to be used in this field is "Europe/Stockholm".
13	CRM User ID	Customer Relationship Management user Identity Number.	Optional Leave blank or enter the user's Customer Relationship Management ID number.
14	Modalities	Defines the recorded modality for the extension. Only the configured modalities will be recorded for the extension.	The following valid values apply: file_share im poll screen share sms video voice whiteboard
15	Directions	Defines the recorded directions for the extension. Only the configured directions will be recorded for the extension.	The following valid values apply: all conference external federated-in federated-out incoming internal outgoing

16	custom0	Custom user fields. For more information visit this page.	Optional
17	custom1		
18	custom2		
19	custom3		
20	custom4		
21	custom5		
22	custom6		
23	custom7		
24	custom8		
25	custom9		
26	Play Notification for PSTN/Federated Inbound Calls (SfB /Lync)	Play Audio Notification for PSTN Inbound Calls.	1 - enabled 0 - disabled
27	Play Notification for Conference Calls (SfB /Lync)	Play Audio Notification for Conference Calls.	1 - enabled 0 - disabled
28	Audio Notification File for PSTN/Federated Inbound Calls (SfB /Lync)	Audio Notification File for PSTN Inbound Calls.	E.g.: This_Call_Is_Being_Recorded.wma
29	Audio Notification File for Conference Calls (SfB/Lync)	Audio Notification File for Conference Calls.	E.g.: This_Meeting_Is_Being_Recorded.wma
30	Music On Hold File for PSTN/Federated Outbound Calls (SfB /Lync)		
31	IM Notification for Conference Calls (SfB /Lync)	IM Notification for Conference Calls.	E.g.: This meeting is being recorded.
32	Play Notification for PSTN/Federated Outbound Calls (SfB /Lync)		1 - enabled 0 - disabled
33	Audio Notification File for PSTN/Federated Outbound Calls (SfB /Lync)		
34	Play Notification for Inbound Calls (Cisco)		1 - enabled 0 - disabled
35	Media Resource ID for Inbound Calls (Cisco)		
36	Retention Period (days)		

37	Automatically Delete Conversations after the Retention Period is Over		
38	Observer User ID		
39	Observer Group ID		
40	Play Notification for Outbound Calls (Cisco)		
41	Media Resource ID for Outbound Calls (Cisco)		
42	Location		
43	Record Calls Answered by 3rd Party		
44	Recorded Platforms		
45	Import Sources		
46	Recording Rule ID		

Using the Group CSV Import

The Group CSV Import provides the capability for assigning users to groups, configuring their group-related rights and its validity in a bulk way. It allows applying supervisor configurations which cannot be derived from the AD objects or structure (organization units, security groups, manager/delegate configurations). It can be found in the **Users \ Group CSV Import** menu.

Sample XLS

The sample XLS file can be downloaded by clicking on the **Download Sample XLS File** link in the upper right corner. After editing this file, it has to be saved in CSV format, so it will be uploadable into Verba.

	A	B	C	D	E	F	G	H	I	J
	Group Name	Supervisory Person	Description	Supervisor	Investigator	Administrator	Manager	Agent	Valid From	Valid Until
1	Big Bosses' Group	bill.gates@company.com steve.jobs@company.com	They need access to the calls of the agents	1	0	0	0			
2								agent-01@company.com	1900-01-01	2099-12-31
3								agent-02@company.com	1900-01-01	2099-12-31
4								agent-03@company.com	1900-01-01	2099-12-31
5								agent-04@company.com	1900-01-01	2099-12-31
6										
7										
8	Alex's Group	alex.ferguson@company.com	He is retired							
9										
10	Jose's Group	jose.mourinho@company.com								
11				1	0	0	1	lukaku@company.com	1900-01-01	2099-12-31
12				1	0	0	1	pogba@company.com	1900-01-01	2099-12-31

Column Name	Description
Group Name	The Group CSV Import will create the groups provided in this column. If the group already exists, then its members will be modified based on the values provided in the other columns and rows.
Supervisory Person	Verba users to be added to the group described in the Group Name column as a supervisor. Multiple users can be provided, each of them in a new line (within a single cell). The uses have to be created in advance.
Description	The short description of the cause of the action.
Supervisor	If set to 1, the group supervisor right will be given to the users provided in the Supervisory Person column, in the group provided in the Group Name column.
Investigator	If set to 1, the group investigator right will be given to the users provided in the Supervisory Person column, in the group provided in the Group Name column.
Administrator	If set to 1, the group administrator right will be given to the users provided in the Supervisory Person column, in the group provided in the Group Name column.
Manager	If set to 1, the group manager right will be given to the users provided in the Supervisory Person column, in the group provided in the Group Name column.
Agent	Verba users provided here will be assigned to the group provided in the Group Name column in the previous row. Each user has to be provided in a separate row. The users always have to come after the row, in which the group and the supervisors were provided. The uses have to be created in advance.
Valid From	Sets the validity of the user provided in the Agent column.
Valid Until	Sets the validity of the user provided in the Agent column.

Uploading the Group CSV File

Once the CSV file is ready, it can be provided in the web interface.

CSV File*

Reference

Action for current members not listed in the CSV* --Choose--

User Identifier Field* --Choose--

Separator* Semicolon (;) Comma (,)

Skip first row (heading)*

Setting Name	Description
CSV File	The CSV file to upload can be provided here by clicking on the Browse button.
Reference	The short description of the import action. After the import, the reference can be used for searching in the import log.
Action for the current members not listed in the CSV	<ul style="list-style-type: none"> • Delete Membership: Users not listed in the CSV file, but present in the group will be removed from the group entirely. • Close Membership (Update Valid Until): The membership of the users not listed in the CSV file but present in the group will be invalidated, by setting the Valid Until property to the current time. The user will be no longer member of the group but will be listed in the Group Membership History. • Do Nothing: Users not listed in the CSV file, but present in the group will not be modified.
User Identifier Field	The user property that is used in the CSV file for user identification.
Separator	The separator has to be selected which is being used in the CSV file.
Skip first row (heading)	If the first row of the CSV file is used for heading (like in the sample XML), then this setting has to be turned on.
Do not modify Active Directory synchronized groups	If checked, the Group CSV import will not modify the groups synched by Active Directory Synchronization

Once the settings are provided, the import the changes can be reviewed by the **Preview Changes** Button. If the changes are correct, it can be executed by the **Submit** button, otherwise, they can be discarded by the **Cancel** button.

Viewing the Group CSV Import Log

The Group CSV Import Log can be reached by clicking on the View Log link in the upper right corner. Log entries can be searched based on the CSV file name, the **Reference** property of the import, and any users (supervisors or agents) present in the import.

Data management

The system includes powerful tools for automated data management. Data management consists of 3 areas:

- Data retention: data retention policies are responsible for managing the lifecycle of the data in the system. Retention policies allow moving data from one storage location to another, managing retention period, or deleting/disposing of recordings.
- Data processing: data processing policies can provide additional information by analyzing certain aspects of the data (e.g. transcribing speech to text), or convert recordings from one format to another.
- Data import: data import policies drive the data import process which allows ingesting different data into the system.

Data management policies

Administrators are able to define archiving, deletion, and other processing rules based on various filter criteria.

Policy execution is carried out by the various services on the Media Repository and/or Recording Servers.

For more information on [Data Management policies](#), see the corresponding article.

Data retention period configuration

Policies that are managing the lifecycle of recorded media are referred to as Data Retention Policies. The various methods of the configuration of data retention periods are described in the [Data retention](#) article.

Storage and export targets

You can define multiple different folders where media is stored by the system or the media has to be exported to. These are called [Storage and export targets](#).

Storage and export targets can point to Verba Media Repositories, SAN volumes, NAS volumes (with UNC path), NetApp SnapLock, EMC Isilon SmartLock, AWS S3, Azure Storage and many more.

Data management policies that are set up with an action to move or copy media files need a storage target defined to specify the location to move/copy to.

Here are a couple of examples for the use of storage targets with the appropriate data management policies:

- to separate media of different users/groups in your organization
- add additional disks to the system
- offload system disks to e.g. SAN disks automatically

Resilient storage and archiving

The system supports the resiliency and high availability options of the underlying storage platforms. The system also offers a workaround if storage level resiliency is not available. For more information, see [Resilient storage and archiving](#).

Large scale deployments

It is critical to understand how the system should be configured in the case of large-scale deployments where the system needs to potentially handle 100s of millions or billions of calls. For more information, see [Best practices for large databases](#).

Import sources

Data can be imported into the system from several sources. These sources together called [Import sources](#).

Import sources can contain recordings, CDR data, and other archives.

Media upload

There are two ways to upload the recorded media files from the Recording Servers to the final storage infrastructure.

- Configure uploading on the Recording Servers (server-level setting) individually.
To do this, go to Administration > Verba Servers > Select your recording server > Change configuration settings. In the configuration tree expand Storage Management > Upload.
Enable uploading and specify the storage server. This method only works if you use your Verba Media Repository or standard network storage as your media storage.
- Configure uploading via [Data Management Policies](#) using the [Upload policy action](#). This is a system-wide configuration applying to all recording servers (where enabled) which allows you to create filters and upload to multiple storages based on conversation metadata.
This method also supports uploading to NetApp SnapLock, EMC Isilon SmartLock, EMC Centera, Hitachi Content Platform, and others. For the latest list of supported platforms, refer to the [Storage and export targets](#) article.

Data management policies

- [Overview](#)
- [Enabling data management and processing policy execution on servers](#)
- [Enabling data import policy execution on servers](#)
- [Configuring data management policies](#)
 - [Find and list data management policies](#)
 - [Creating a data management policy](#)
 - [Adding Data Management Filtering criteria](#)
 - [Custom Schedules](#)
 - [Modifying and deleting data management policies](#)
- [Alerts](#)
- [Audit log](#)
- [Export Options](#)

Overview

Data management policies are very powerful tools for automated data management. Administrators can define rules that execute various actions based on customizable filtering criteria. The policies are executed by the Verba Storage Management Service and/or the Verba Import Service on either Verba Recording servers or Media Repositories.

Policy execution is turned off by default, it has to be enabled in the server configuration.

The system supports the following data management policy types:

Type	Policies	Description	Executed On	Executed By
Data Retention	Upload	Moves conversation related files (media, metadata file, etc.) from the Recording Servers to the configured storage target.	Recording Server or Media Repository / Application Server	Storage Management Service
	Archive in DB and Move Media	Moves database records to the archive table to reduce database load and moves conversation related files to the configured storage target.	Media Repository / Application Server	Storage Management Service
	Archive in DB	Moves database records to the archive table to reduce database load.	Media Repository / Application Server	Storage Management Service
	Move Media	Moves conversation related files to the configured storage target.	Media Repository / Application Server	Storage Management Service
	Copy Media	Copies conversation related files to the configured storage target and keeps the original copies. Recommended for moving data from a WORM storage target where records are still under retention and cannot be deleted (or moved) to another storage target. It can also be used to dual archive recordings.	Media Repository / Application Server	Storage Management Service

	Delete	Deletes all conversation data including database records and related files on the storage target. Generally, it is not recommended to use the delete policy for data retention, instead, the Data retention configuration should be used.	Media Repository / Application Server	Storage Management Service
	File Verification	Verifies the existence of conversation related files on the storage targets.	Media Repository / Application Server	Storage Management Service
	Increase Retention Period	Increases the data retention period for the conversations.	Media Repository / Application Server	Storage Management Service
	Adjust Retention for Media-Only Records policy	Adjusts the retention of the Media-Only records to the retention of the referencing CDR-Only records. It is only recommended for Genesys Active REcording and BT IPTRade TPO based recording where the retention of the Media-Only records cannot be set based on the available metadata.	Media Repository / Application Server	Storage Management Service
	Delete Communication Policy Events	Deletes the communication policy events (ethical wall audit log).	Media Repository / Application Server	Storage Management Service
	Deduplicate Recordings	Deduplicates recordings for certain integrations in the case of 2N recording.	Media Repository / Application Server	Storage Management Service
	Export	Exports conversations to the configured export target	Media Repository / Application Server or Recording Server (Direct Export)	Storage Management Service
	Advanced IM Export	Provides export functionality specified to Microsoft Teams Chat	Media Repository / Application Server	Storage Management Service
Data Processing	Encrypt and Sign	Encrypts and/or signs conversation related files.	Recording Server or Media Repository / Application Server	Storage Management Service

	Voice Quality Check	Checks voice quality on audio and video recordings.	Recording Server or Media Repository / Application Server	Storage Management Service
	Transcode	Transcodes audio or video files to different formats.	Media Repository / Application Server	Storage Management Service
	Transcription	Transcribes audio conversations.	Speech Analytics Server or Media Repository / Application Server	Speech Analytics Service
Data Import	Data Import	Imports different data into the system	Recording Server or Media Repository / Application Server	Import Service

Enabling data management and processing policy execution on servers

Configured data management policies have to be enabled in the Verba Storage Management Service in order to run them. Please follow the steps below to enable the feature:

Step 1 - Login to the web interface with **System administrator** rights.

Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

Step 3 - Click on the **Change Configuration Settings** tab and find the **Storage Management / Data Retention** section.

Step 4 - Set the **Enabled** setting to **Yes**.

Step 5 - Configure the **Schedule** setting.

Step 6 - Save the changes by clicking on the



icon.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

For further information on the configuration settings, check [Storage management settings](#).

Enabling data import policy execution on servers

Step 1 - Login to the web interface with **System administrator** rights.

Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

Step 3 - Go to the **Service Activation** tab, then activate the **Verba Import Service** by clicking on the



icon.


Step 4 - Go to the **Change Configuration Settings** tab, configure the schedule settings under the **CDR and Archived Content Importer \ CDR Import** and **Archive Import** nodes.

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 7 - Click on the **Service Control** tab.

Step 8 - Start the **Verba Import Service** by clicking on the



icon.


For further information on the configuration settings, check [CDR and Archived Content Importer settings](#).

Configuring data management policies

Find and list data management policies

Select the **Data management / Data Management Policies** menu item. You can use the search form below the title, to filter data retention policies: just select your filter and click **Find**.

Find and List Data Management Policies Add New Data Management Policy
Show Disabled Data Management Policies

 You must add settings on existing or incoming. [Learn how to configure.](#)

Name

Enabled	Name	Conversations older than	Action	Target/Source/Processor	Min/Max/Interval	Priority	ID
Yes	Assurance - Media Check		Video Quality Check			80	10
Yes	Assurance - Media Media Inventory		File Verification			80	9
Yes	UK - Keep Conversations within Jurisdiction		Upload	EU/UK - Dredbit - VerbaAppRecordingProvider		80	7
Yes	US - Separate SDC Conversations		Upload	US West - NDCP1 - VerbaWebInterface		40	5
Yes	Global - Contact Center (Phone) Monitoring	0 (max): 1 (min)	Conversations more recent than	Cloudy PhoneIns (Info call Transcripts)		80	8
Yes	Global - Save Video Storage (save audio only)	0 (max): 00 (min)	Transcode			30	4
Yes	US - Offload to Low-Expense Storage	1 (max)	Archive to CD and Blob Media	US West - NDCP1 - VerbaWebInterface		70	6
Yes	Global - Delete Everything After 7 Years	7 (max)	Delete			10	2

8 items found, displaying all items
Configuration: Local: RTM: 10P

When you click on a policy (or the **Add New Data Management Policy** button to create a new one), the Data Management Policy Configuration page opens.

Creating a data management policy

You can create a new data retention policy by clicking on the **Add New Data Management Policy** link on the **Administration / Data Management Policies** page. After selecting the link, the following page is opened.

The following table describes the policy settings that are common for all types of policies:

Setting	Description	Requirements
Name	The name of the data management policy.	Required field. Minimum length: 3 Maximum length: 256 Must be unique in the system.
Enabled	Indicates whether the policy is enabled or disabled. Only enabled policies are executed.	Required field.
Priority	Defines the execution order of the policies. This should be an integer number. Higher priority policies are processed first if multiple policies apply to the same call.	Required field.
Action	Defines the policy action. Some of the configuration options are only available with certain actions. The layout of the configuration page changes based on the selected action. For more information on each of the actions and their specific configuration options refer to the individual description pages.	Required field.

Next, by adding filtering criteria, you will need to define the calls the policy should apply to.

Adding Data Management Filtering criteria

You can configure a filter that defines what calls should be included in your data management policy.

- **Conversations Older than** (not available for upload and phonetic index related policy actions): This filtering option defines the age of the calls. Only calls older than the defined value will be handled for the policy during execution.
- **Conversations more recent than** (only available for phonetic index related actions): This filtering option defines the age of the calls. Only calls more recent than the defined value will be handled for the policy during execution.


Click on the + icon to add a new filtering option. You can add as many policies as you want. Multiple field filters are used with 'AND' operator.

The rest of the filtering options are based on various metadata or CDR (Call Detail Record) information that is stored in the database for each conversation. The table below contains a list of potentially available filtering options including custom metadata fields.

Category	Field	Description
Participants	From	The number of the caller party in the conversation
	From Info	The number of the called party in the conversation
	From (digits)	The number of digits in the phone number of the initiator of the conversation
	From Device ID	The Device ID of the initiator of the conversation
	From IP	The IP address of the caller party in the conversation
	To	The name of the caller party in the conversation
	To Info	The name of the called party in the conversation
	To (digits)	The number of digits in the phone number of the target of the conversation
	To Device ID	The Device ID of the target of the conversation
	To IP	The IP address of the called party in the conversation
	Both To or From	The number of any party participating in the conversation
	Both To or From Info	The name of any party participating in the conversation
	Dialed Number	The original dialed number
	User	The user associated with the conversation based on the extension configuration
	User Location	The location of the user, defined in the user configuration
	Extension	The extension numbers in a conversation, a selection list of the configured extensions, otherwise similar to the 'Any party number' field below
	Group	The group where a conversation belongs to based on the users associated with the conversations
	User ID	The User/Agent/Trader ID obtained from the recorded platform
	Participating User	The user that participated in the conversation. (advanced instant message data only)
	Participating User Location	The location of the user that participated in the conversation. (advanced instant message data only)
Participating Group	The group of the user that participated in the conversation. (advanced instant message data only)	
Other Participant	Other users participated in the conversation. (advanced instant message data only)	
Details	Start Time (UTC)	The start time of the conversation in UTC timezone
	Recent Than	Only conversations selected where the start time is recent than the defined value. Make sure it is not used with a recurring schedule, otherwise conversations can be skipped if the defined value is close to the recurring period.
	Direction	The direction of the conversation (e.g. internal, inbound, outbound, etc.)
	End Cause	The end cause of the conversation (e.g. normal, hold, transfer, etc.)
	Duration Interval	The length of the conversation

Conversation Type	The type of conversation. Available options: <ul style="list-style-type: none"> • Voice • Video • Instant Messaging • SMS • Desktop Screen • Screen & Application Share (Lync/SfB) • Whiteboard (Lync/SfB) • Poll / Q&A (Lync/SfB) • File Share (Lync/SfB) 	
Instant Message Type	The type of IM conversation (Microsoft Teams only). Available options: <ul style="list-style-type: none"> • Chat • Channel 	
Forward Reason	The forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	
On-demand	Defines whether a call was recorded as on-demand	
Marked for recording	Defines whether an on-demand conversation was marked for recording	
Protected	Defines whether the conversation is protected	
Label	The labels added to the conversation	
Case	The cases containing the conversation	
Encrypted with Certificate	The certificate used to encrypt the conversation	
Signed with Certificate	The certificate used to sign the conversation	
Quality Management Scorecard exits	Checks if there is a Quality Management Scorecard assigned to the conversation	
Analytics	Silence Ratio	The silence ratio in a conversation
	Talkover Ratio	The talkover ratio of the conversation
	Longest Silence	The longest silence present in a conversation
Technical	Recording Server	The hostname of the server that recorded the conversation
	Media File Name	The name of the stored media file
	Storage Target	The current storage location of the media file(s)
	2nd Storage Target	The second storage location of the media file(s) in the case of dual archiving is enabled
	Source Platform	Defines which telephony / unified communications system the conversation was recorded on (Cisco, Sfb, Avaya, etc.)
	Secondary	Defines whether the conversation is recorded on a server marked as secondary (using 2N / duplicate recording)
	CDR/Media Record	Defines whether the conversation is a Standard, CDR-Only or Media-Only record. CDR-Only and Media-Only records are used for trader voice recording.
	Elapsed Time Since Transcoding (UTC)	The time elapsed since transcoding in UTC timezone

	Time of Transcode (UTC)	The date and time of transcoding in UTC timezone
Metadata Fields	Custom Metadata Fields	Custom metadata fields configured in the system, the list of available fields might vary depending on the integration configured and the metadata templates added

 If you do not want a Delete policy to delete protected conversations, you have to **explicitly add a 'Protected' = 'No' filter.**

After filling out the form, click the **Save** button to save the data retention policy into the database.


Custom Schedules


You can set up a custom schedule for each policy.

▼ Scheduling

Custom Schedule

Timezone * ▼
Central European Time
9:30-42
'Time of Next Export' and 'Period Settings' are stored and used in GMT (daylight saving will not be applied).

Time of Next Execution * 
2020.02.14 09:25 (Europe/Budapest) in UTC is 2020.02.14 08:25, in your timezone (Europe/Budapest) it is 2020.02.14 09:25.


Period Settings * 

Under *Period Settings* you can configure the frequency, by clicking on the



button at the end of the line.

The Configuration Wizard will appear, here you can set the desired value.

 If you leave the *Custom Schedule* option unchecked, then the central settings will take effect. By setting a custom schedule, you overwrite the central configuration for this policy.

Modifying and deleting data management policies

To edit a data retention entry, you have to click on the desired row of the list showing registered data management policies. After clicking on the row, a new page opens automatically.

To make changes effective, push the **Save** button. All conditions, which are described in the previous part, have to be met.

You can delete the data management policy by clicking on the **Delete** button.

Alerts

The system raises alerts related to data management policies in the following cases:

- policy execution failed
- policy execution finished
- data management policy is created, updated or deleted.

For more information, see [Alerts](#).

Audit log

The system automatically creates audit logs during policy execution which contains record-level information about the executed action.

For more information, see [Data management policy audit log](#).

Export Options

The system allows users to export the list of configured data management policies.

The RTF and PDF export options will export the list of configured data management policies, please note that these export options will only display the visible column headers, as seen on the Find and List Data Management Policies screen.

AVAILABLE IN VERSION 9.6.13 OR LATER

The Excel export option will export all configured data management policy values, including all configured values within the data management policy details screen.

Upload policy

Overview

This article provides a description of the upload data management policy. A data retention policy configured with the upload action is used for specifying the final storage location of the recorded conversations. Recording Servers store the recorded conversations on their local disk temporarily while recording. After the recording is done, the files need to be moved to the designated storage location(s).

Each policy you define can contain a different storage location ([previously added as a storage target](#)) and a set of filters to determine which conversations should be uploaded to that location. These filters are based on the metadata stored in the database for each conversation. This is a good way to have separate storage locations for conversations of different users, groups, etc.

The Upload policy supports dual archiving which allows storing the files on 2 separate storage targets. For more information, see [Resilient storage and archiving](#).

The system supports 2 types of upload policies:

- **Direct upload policies:** direct upload policies are designed for uploading large amounts of data with minimal impact on the database. It uses the user-extension configuration (instead of the database) to determine which policy has to be applied for the conversation recorded on the server. It is the recommended option, especially if it is a large installation.
- **Upload policies:** normal upload policies are designed to upload data with complex and flexible policy filtering settings. It uses the database to determine which policy has to be applied for the conversation recorded on the server. It is not recommended for large volumes due to the increased database load.

The following table summarizes the two upload policy options:

	Direct Upload Policy	Upload Policy
Place of execution	Recording Server	Recording Server
Suitable for Large Volumes	Yes, recommended	Yes
Data Types and Source Platforms	Any	Any
Database Query / File Based	File	File and Database Query
Filters	Conversation Type Source Platform 2N Source	Any
User Assignment	Yes (policy filter configuration)	Yes (user/extension configuration)
Audit Log	Yes	Yes
Configurable Schedule	No	No
Retention	Set only on the user level	Can be set on the policy level and on the user level

What happens when there is a record with no matching policy?

After the recording service completes the recording process, the Storage Management Service will try to find a matching policy using database queries with the Conversation ID or the local configuration in the case of direct upload policies. If it does not find any matching policy, it will raise an alert and will immediately move the files related to the conversation to the **media/nopolicy** folder. Conversation-related files in the **media/nopolicy** folder are infinitely re-checked with a lower frequency (configurable, 10 minutes by default). The system does not give up the upload after the timeout and will continuously retry. If you receive an alert for upload failure due to no policy

found, it is recommended to check the affected records and the policy filter configuration. After updating the policies, the system automatically tries to upload the files again.

Functionality in earlier versions (pre v9.6.6.6237):

After the recording service completes the recording process, the Storage Management Service tries to find a matching policy using database queries with the Conversation ID or the local configuration in the case of direct upload policies. If it does not find any matching policy, it will raise an alert and will try to find it again in the next cycle. The service tries to find a matching policy until a configurable timeout (120 hours by default). After the timeout expires, the Storage Management Service moves the files related to the call to the **media /nopolicy** folder, and will never try to upload it again. Files can be manually copied back to the standard media folder where the Storage Management Service will try the upload again. It will only try to upload it once since the timeout has already expired based on the call end date-time.

Enabling policy-based upload

Since upload policies are executed by the individual Recording Servers instead of the Media Repository (unlike all other policy types), you will need to enable policy-based uploading on the server level in the configuration of each Recording Server (or using the configuration template).

Step 1 - Open the Verba Web interface, go to **Configuration / Servers**, then select your Recording Server.

Step 2 - Click on the **Change Configuration Settings** tab and in the configuration tree, go to the **Storage Management / Upload** node.

Step 3 - Set **Policy Based Uploading Enabled** to **Yes**.

Step 4 - **Save** the configuration then **repeat** these steps for each recording server in your system. Finally, execute the changes.

Configuring a direct upload policy

To create an upload policy, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Upload** as the action

Step 4 - Enable the **Direct Upload** option

Step 5 - Select the **Destination Storage Target** you created from the list

Step 6 - Optionally enable related actions such as [Voice Quality Check](#), [Encryption and Signing](#).

Step 7 - Configure **Filtering Criteria** to specify which conversations should be uploaded by this policy

Configuring an upload policy

To create an upload policy, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Upload** as the action

Step 4 - Select the **Destination Storage Target** you created from the list

Step 5 - Define the **Retention Period (days)**, **Automatically Delete Conversations after the Retention Period is Over** and **Prefer User's Retention** setting.

Step 6 - Optionally enable related actions such as [Voice Quality Check](#), [Encryption and Signing](#).

Step 7 - Configure **Filtering Criteria** to specify which conversations should be uploaded by this policy

The screenshot shows the 'Data Management Policy Configuration' page. At the top, there are tabs for 'Data Management Policy Data' and 'SQL Query'. The main configuration area includes the following fields and options:

- ID***: 10
- Name***: Assurance - Media Check
- Enabled***: Yes
- Priority***: 90 (Note: Higher priority policies are processed first when the 'older than' dates are equal.)
- Action***: Upload (Note: Upload policies should only be used when there is a requirement for multiple storage targets or WORM storages. In order to use upload policies, the feature must be enabled on the Media Recording Servers. It is also recommended to create an upload policy which does not contain filters, in order to avoid leaving recordings on the Recording Servers. This special policy needs to be configured with the lowest priority (lowest number).)
- Destination Storage Target***: --Choose--
- Retention Period (days)**: [Empty field]
- Automatically Delete Conversations after the Retention Period is Over***:
- Prefer User's Retention***:
- Voice Quality Check***:
- Execute Only on Selected Servers**:
- Server Selection**: A list box containing 'Combo Server 1', 'Media Repository Server 1', and 'WIN-SSVUHCPRB0GG' with navigation arrows.

Configuring an upload policy with dual archiving

To create an upload policy, follow the steps below:

Step 1 - [Create two Storage targets](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Upload** as the action

Step 4 - Select the **Enable Dual Archiving** option

Step 5 - Select the **Destination Storage Target** for both the **First** and **Second** storage targets you created from the list. You can separately define the **Retention Period (days)**, **Automatically Delete Conversations after the Retention Period is Over** and **Prefer User's Retention** settings for each storage target.

The screenshot shows the configuration details for dual archiving. The 'Enable Dual Archiving*' checkbox is checked. The settings are as follows:

- First Storage Target**
 - Destination Storage Target***: UnityVSA - \\unitynas.verbatest.local\TestSMB\dualarchiving
 - Retention Period (days)**: 365
 - Automatically Delete Conversations after the Retention Period is Over***:
 - Prefer User's Retention***:
- Second Storage Target**
 - Destination Storage Target***: netapp - \\netapp\calls
 - Retention Period (days)**: 90
 - Automatically Delete Conversations after the Retention Period is Over***:
 - Prefer User's Retention***:

Step 6 - Optionally enable related actions such as [Voice Quality Check](#), [Encryption and Signing](#).

Step 7 - Configure **Filtering Criteria** to specify which conversations should be uploaded by this policy

Archive in DB and Move Media policy

This article describes the Archive in DB and Move media data management policy.

This action is a combination of the functions of two other actions: 'Archive in DB' and 'Move media'.

It is a way to relocate your conversation media files from their primary storage location to another storage as well as flag the selected conversations as "archived" in the Verba database.

This helps to make searches for conversations faster since standard searches exclude archived conversations. (This default behavior can be changed, however, from the conversation search interface.)

You can define a storage target ([previously created](#)) to move the media files to and a set of filters to specify which conversations should this policy be executed on.

To create a Policy with the Archive in DB and move media action, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select the **Archive in DB and Move media** as the action

Step 4 - Select the storage target you created from the list

Step 5 - Select your filters to specify which conversations should be uploaded by this policy

The screenshot shows the 'Data Management Policy Configuration' page. At the top, there are tabs for 'Data Management Policy Data' and 'SQL Query'. On the right, there are links for 'Add New Data Management Policy' and 'Back to Previous Data Management Policy List'. The main configuration area is titled 'Data Management Policy Data' and contains the following fields and options:

- ID***: 10
- Name***: Assurance - Media Check
- Enabled***: Yes
- Priority***: 90 (Higher priority policies are processed first when the 'older than' dates are equal)
- Action***: Archive in DB and Move Media (This Action is Effective on Online (Non-Archived) Conversations only)
- Destination Storage Target***: --Choose--
- Retention Period (days)**: [Empty field]
- Automatically Delete Conversations after the Retention Period is Over***:
- Prefer User's Retention***:
- Execute Only on Selected Servers**:

At the bottom, there is a list of servers: 'Combo Server 1', 'Media Repository Server 1', and 'WIN-SOVLUHCPCBOGG'. There are navigation arrows (>> and <<) next to the list.

Archive in DB policy

This article describes the Archive in DB data management policy.

A policy with this action will flag the selected conversations as "archived" in the Verba database.

This helps to make searches for conversations faster since standard searches exclude archived conversations. (This default behavior is changeable, however, from the conversation search interface.)

i The actual files in the storage for the conversations on which this policy is executed do not get moved or changed in any way. This operation happens on the database level only.

To create a policy with the Archive in DB action, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [\[LINK\]](#)

Step 2 - Select **Archive in DB** as the action

Step 3 - Select your filters to specify which conversations should be uploaded by this policy

Data Management Policy Configuration [Add New Data Management Policy](#)
[Back to Previous Data Management Policy List](#)

[Data Management Policy Data](#) [SQL Query](#) ?

▼ Data Management Policy Data

ID* 10

Name* Assurance - Media Check

Enabled* Yes

Priority* 90
Higher priority policies are processed first when the 'older than' dates are equal.

Action* Archive in DB
This Action is Effective on Online (Non-Archived) Conversations only.

Execute Only on Selected Servers

Combo Server 1
Media Repository Server 1
WIN-55VUHCPBOGG


>> <<

Move Media policy

This article describes the move media data management policy.

Move Media policies provide a way to relocate your conversation media files from their existing storage location to another storage (for archiving purposes). You can define a storage target ([previously created](#)) to move the media files to and a set of filters to specify which conversations should this policy be executed on.

The Move Media policy supports dual archiving which allows storing the files on 2 separate storage targets. For more information, see [Resilient storage and archiving](#).

 A Move Media policy will only move the actual files in the file system, it will not mark the conversations as archived in the Verba database. This means that from the perspective of the Verba Web interface (particularly searching for calls) this process has no visible impact at all.
To create a policy that moves the files and also marks them as archived use the [Archive in DB and move media](#) action instead.

Configuring a move media policy

To create a move media policy, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Move Media** as the action

Step 4 - Select the **Destination Storage Target** you created from the list

Step 5 - Define the **Retention Period (days)**, **Automatically Delete Conversations after the Retention Period is Over** and **Prefer User's Retention** setting.

Step 6 - Configure **Filtering Criteria** to specify which conversations should be uploaded by this policy

ID*
 Name*
 Enabled* ▼
 Priority*
Higher priority policies are processed first when the 'older than' dates are equal.
 Action* ▼
 Which Copy of Dually Archived Records Should be Processed* ▼
 Enable Dual Archiving*
 Destination Storage Target* ▼
 Retention Period (days)
 Automatically Delete Conversations after the Retention Period is Over*
 Prefer User's Retention*
 Execute Only After Another Policy Executed ▼
 Execute Only After This Export Executed ▼
 Execute Only on Selected Servers

TESTMR4.VERBATEST.LOCAL
 TESTRS1.VERBATEST.LOCAL

Configuring a move media policy with dual archiving

To create a move media policy with dual archiving, follow the steps below:

Step 1 - [Create two Storage targets](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Move Media** as the action

Step 4 - Select the **Enable Dual Archiving** option

Step 5 - Select the **Destination Storage Target** for both the **First** and **Second** storage targets you created from the list. You can separately define the **Retention Period (days)**, **Automatically Delete Conversations after the Retention Period is Over** and **Prefer User's Retention** settings for each storage target.

Step 6 - Configure **Filtering Criteria** to specify which conversations should be uploaded by this policy

Enable Dual Archiving*

First Storage Target

Destination Storage Target* ▼

Retention Period (days)

Automatically Delete Conversations after the Retention Period is Over*

Prefer User's Retention*

Second Storage Target

Destination Storage Target* ▼

Retention Period (days)

Automatically Delete Conversations after the Retention Period is Over*

Prefer User's Retention*

Copy Media policy

This article describes the Copy Media data management policy. The Copy Media policy has two modes:

- **Dual Archiving:** the policy creates a copy of the media files on the new storage target and links them as second copies in the database. We recommend using this option to duplicate the media files on another storage target for dual archiving. For more information, see [Resilient storage and archiving](#).
- **Copy and Forget:** the policy creates a copy of the media files on the new storage target and rewrites the link in the database to the new storage target. The original copy is left intact. We recommend using this option when the original copy is under retention on a WORM storage and the files have to be moved to a new storage location. This means that the system will no longer manage the original copies and will not apply any policies including data retention or offer playback and download.

You can define a storage target ([previously created](#)) to copy the media files to and a set of filters to specify which conversations should this policy be executed on.

To create a Copy Media policy, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Copy Media** as the action

Step 4 - Select the **Mode** to define if the **Dual Archiving** or **Copy and Forget** mode should be used for the policy

Step 5 - If the **Copy and Forget** mode selected, the **Which Copy of Dually Archived Records Should be Processed** option defines if the First or Second copy should be copied if the record is already dual archived.

Step 6 - Select the **Destination Storage Target** you created from the list

Step 7 - Select the filters to specify which conversations should be copied by this policy

The screenshot shows the configuration interface for a Copy Media policy. The fields are as follows:

- ID***: 2
- Name***: uploadTest
- Enabled***: Yes
- Priority***: 10
Higher priority policies are processed first when the 'older than' dates are equal.
- Action***: Copy Media
- Mode***:
 - Copy and Forget**
Creates a copy of the media files on the new storage target and rewrites the link in the database to the new storage target. The original copy is left intact. We recommend using this option when the original copy is under retention on a WORM storage and the files have to be moved to a new storage location.
 - Dual Archiving**
Creates a copy of the media files on the new storage target and links them as second copies in the database. We recommend using this option to duplicate the media files on another storage target for dual archiving.
- Which Copy of Dually Archived Records Should be Processed***: First Only
- Destination Storage Target***: UnityVSA - \\unitynas.verbatest.local\TestSMB\dualarchiving
- Execute Only After Another Policy Executed**: --Choose--
- Execute Only After This Export Executed**: --Choose--
- Execute Only on Selected Servers**:
- Server Selection**: A list of servers with two buttons: >> and <<. The list contains: TESTMR4.VERBATEST.LOCAL and TESTRS1.VERBATEST.LOCAL.

Delete policy


This article describes the Delete data management policy. There are different ways to delete conversations from the system and manage data retention, for more information, refer to [Data retention](#).

A delete data retention policy allows defining a set of filters to find conversations that have to be deleted from the system.

Once the policy is executed on conversations that match the filtering criteria, the conversations will be deleted from the storage location along with all related metadata from the database.

The system also allows deleting specific files only by defining the file extensions. When one or more file extensions are defined, other remaining files and the database record will not be deleted, only the files with the defined extensions. If you define the file extension of the only media file for the conversations, the system will not execute the deletion action.

It is possible to delete media files only and keep all CDR and metadata.

 Conversations deleted by a delete data management policy are not recoverable and cannot be undone. It is very important to verify and check all settings before saving to ensure only the necessary conversations will be removed.

To set up a deleting data management policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data retention policies](#)

Step 2 - Select **Delete** as the action.

Step 3 - Optionally enable **Delete Files and Keep CDR Information**, to delete media files only and keep all CDR and meta information.

Step 3 - Optionally define the file extensions under **File Extension(s)**, to delete specific files only related to the selected conversations. When you define a file extension filter, other remaining files and the database record will not be deleted, only the files with the defined extensions. Multiple extensions can be defined separated by commas (,) as follows:

To delete *.vf files only, define: *vf*

To delete *.vf and *.vmf files only, define: *vf,vmf*

Step 4 - Select your filters to specify which conversations should be deleted by this policy.

Step 5 - Click on the **Check Effect** button to verify the number of conversations affected by the policy. In this way, you can avoid misconfiguration and unwanted deletion of conversations.

Step 6 - Click on the **Save** button to save the policy configuration. Once the policy is saved it is effective and will be executed according to the policy execution schedule.

Name*

Enabled*

Priority*
Higher priority policies are processed first when the 'older than' dates are equal.

Action*

Delete Files Only and Keep CDR Information*

File Extension(s)

Execute Only on Selected Servers

TESTMR2.SUB.VERBATEST.LOCAL	>>	
	<<	

File Verification policy

This article describes the File Verification data management policy.

The File Verification storage policy is implemented to check media inventory and detect missing files. The new policy sends email alerts.

The idea behind this feature is to detect missing recordings that were accidentally removed or deleted from the storage location. The best practices for using it are as follows.

- Configure daily checks for the recordings created the same day, it can detect storage related configuration issues
- Configure weekly or monthly checks for the entire media inventory, run this check during off-hours, you might need to segment the inventory and configure multiple checks

i This is a very disk-intensive task. For higher call volumes this can take a very long time to complete. Make sure this is run out of business hours, or only for smaller call volumes. It is advised to use the Custom Schedule option.

Configuring File Verification policy

To create a File Verification policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **File Verification** as the action

Step 3 - Select your filters to specify which conversations should be checked by this policy

Step 4 - Click on Save. The policy will run periodically

Data Management Policy Configuration Add New Data Management Policy
Back to Previous Data Management Policy List

Data Management Policy Data SQL Query ?

▼ Data Management Policy Data

ID* 7

Name* LUK - Keep Conversations within Jurisdiction

Enabled* Yes

Priority* 60
Higher priority policies are processed first when the 'older than' dates are equal.

Action* File Verification

Execute Only on Selected Servers

Combo Server 1
Media Repository Server 1
WIN-SOVIJURCPBLOGG

▼ Scheduling

Custom Schedule

Increase Retention Period policy

This article describes the Increase Retention Period data retention policy action.

The Increase Retention Period storage policy is implemented to allow increasing the retention period configured on the storage targets.

The new retention setting is updated on the supported storage platforms as well, using the API integration: NetApp SnapLock, EMC Isilon SmartLock, EMC Centera, and Hitachi Content Platform.

Reducing the Retention Period is not possible when user-based or policy-based retention is used, for more information see [Data retention](#).

Configuring the Increase Retention Period policy

To create an Increase Retention Period policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **Increase Retention Period** as the action

Step 3 - Set the **Increase Retention Period (by day)** field

Step 4 - Select your filters to specify which conversations should be affected by this policy

Step 5 - Click on **Save**

Data Management Policy Configuration Add New Data Management Policy
Back to Previous Data Management Policy List

[Data Management Policy Data](#) [SQL Query](#) ?

▼ Data Management Policy Data

ID* 7

Name* UK - Keep Conversations within Jurisdiction

Enabled* Yes

Priority* 60
Higher priority policies are processed first when the 'older than' dates are equal.

Action* Increase Retention Period

Increase Retention Period (by days)*

Execute Only on Selected Servers

Combo Server 1
Media Repository Server 1
WIN-55VUHCPCBOGG

>>> <<<

Delete Communication Policy Events policy

This article describes the Delete Communication Policy Events data management policy.

A deletion policy allows you to define a set of filters to find communication policy events that are no longer needed and should be deleted.

Once the policy is executed on the events that match the filtering criteria, those events will be deleted from the database, leaving no trace behind.

 Events deleted by a data retention policy are not recoverable.

To set up a deletion data retention policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data retention policies](#)

Step 2 - Select **Delete Communication Policy Events** as the action.

Step 3 - Select your filters to specify which events should be deleted by this policy.

Data Management Policy Configuration Add New Data Management Policy
Back to Previous Data Management Policy List

[Data Management Policy Data](#) [SQL Query](#) ?

▼ Data Management Policy Data

ID* 7

Name* UK - Keep Conversations within Jurisdiction

Enabled* Yes

Priority* 60
Higher priority policies are processed first when the 'older than' dates are equal

Action* Delete Communication Policy Events

Execute Only on Selected Servers

Comba Server 1
Media Repository Server 1
WIN-55VUHCPBOGG

>> <<


Once the policy is saved it is effective and will be executed according to the policy execution schedule.

Deduplicate Recordings policy


The deduplication policy allows correlating 2N/dual-stream recordings and keeping the better quality record only (and deleting the other copy). To determine which copy/instance is better, either the voice quality check results (if available) or the number of RTP packets processed counter is used. The correlation of the records is based on the telephony platform call ID (which can be ambiguous) and the start - end time of the record.


Supported integrations:

- Skype for Business voice/video/screen share recording
- Network port mirroring based SIP/SCCP based voice/video recording
- Cisco proxy-based voice/video recording
- BT IPTrade recording
- Speakerbus recording
- IPC Unigy recording
- Avaya DMCC (multiple registration) based voice recording

 Deduplication does not remove any copy in case of the following ambiguous situations:

- The clock of the Recording Servers are out of sync, the start time of the two records differ more than 5 seconds.
- The length of recorded media files differs for more than 3 seconds.
- The RTP packet counters differ more than 200 RTP packets.
- There is a mid-call failover at one of the recorders. This scenario leads to violating the first 3 requirements for the ongoing records involved in the failover.
- For trading turret integrations, when one recorder starts later than the other leading to starting the recording of the ongoing calls later than the other. This scenario leads to violating the first 3 requirements for those records.

 The deduplication policy does not support custom metadata or markers added by users. It means that if this information is added to the copy (primary, secondary) which will not be kept, the data will be lost.

 The clock of the Recording Servers must be synchronized, a maximum of 5 seconds drift is allowed for 2N correlation. If the record is under retention (e.g. on WORM storage), the policy will skip the deduplication for the record.

To create a Deduplication Policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **Deduplicate Recordings** as the action

Step 3 - Select your filters to specify which conversations should be processed by this policy

Data Management Policy Configuration

[Add New Data Management Policy](#)
[Back to Previous Data Management Policy List](#)

Data Management Policy Data SQL Query ?

▼ **Data Management Policy Data**

ID*

Name*

Enabled*

Priority*
Higher priority policies are processed first when the 'older than' dates are equal.

Action*

Execute Only on Selected Servers

▼ **Scheduling**

Custom Schedule

▼ **Data Management Filtering Criteria**

Conversations older than* year(s) day(s) : hour(s) : minute(s)

Conversation Detail Fields

Export policy

This article provides a description of the export data management policy. The system provides multiple options to export data from the platform. Export policies are recommended when large volumes of data have to be exported from the system on an ongoing basis. For more information on the available export options and their comparison, see [Export](#).

The export policies are executed by the Storage Management Service on the Media Repository/Application Servers. The system also allows executing the export policies directly on the Recording Servers when the Direct Export option is enabled. The following table provides an overview of the 2 options:

	Export Policy	Direct Export Policy
Place of execution	Media Repository / Application Server	Recording Server
Suitable for Large Volumes	Yes	Yes, recommended
Data Types and Source Platforms	Any	All Voice, Video, Screen and Application Share integrations All trader voice integrations except BT ITS Skype for Business Instant Message, File Transfer Symphony Instant Message, File Transfer
Database Query / File Based	Database Query	File
Filters	Any	Conversation Type Source Platform 2N Source
User Assignment	Yes (policy filter configuration)	Yes (user/extension configuration)
Available from Search	No	No
Custom CDR File	No	No
Manifest File	No	No
Audit Log	Yes	Yes
Configurable Schedule	Yes	No
Supports imported records	Yes	No
Simultaneous Execution	A single export policy can run on multiple servers, data is split across the servers.	No

An export data management policy creates a copy of the selected conversations and places the data to a configurable storage/export location. It consists of a ([previously created](#)) storage/export target, a set of filters to choose which conversations should be exported, and an optional file format choice should you decide to create the copies in another format. Policies with the export action do not modify or impact the original conversations in any way. The exported data is not accessible in any way from the system.

Creating an export policy

To create an export data management policy, follow the steps below:

Step 1 - [Create a Storage target](#) for the export policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Export** as the action

Step 4 - Select the **Destination Storage Target** you created from the list

Step 5 - Configure policy specific settings as follows:

Name	Description
Decrypt Encrypted Conversations	If a conversation related files are encrypted, the system can automatically decrypt the files before exporting. Original files remain encrypted.
Generate Media Files for CDR-Only Conversations	For trader voice recordings, the system can stitch related media files together for the CDR-Only records. If not enabled, the system will export the metadata file only for the CDR-Only records.
Export Attachments in IM Conversations	For specific integrations (Skype for Business, Symphony), the system can automatically export file attachments with instant message conversations.
File Extension(s)	The comma (,) separated list of file extensions. The export policy exports only those conversation related files where the extension of the file is matching the list. Example: wav,vtr will export the audio file and the transcript file for the conversations
Voice Format	Voice recordings can be optionally transcoded to the selected format.
Video Format	Video recordings can be optionally transcoded to the selected format.
Desktop Recording and Screen /Application Sharing Format	Screen share recordings can be optionally transcoded to the selected format.

Step 6 - Configure **Custom Schedule** if you want to run the export in a specified time

Step 7 - Configure **Filtering Criteria** to specify which conversations should be exported by this policy

Data Management Policy Data
SQL Query
?

▼ Data Management Policy Data

Name*

Enabled* Yes

Priority* 130
Higher priority policies are processed first when the 'older than' dates are equal.

Action* Export

Destination Storage Target* --Choose--

Retention Period (days)

Decrypt Encrypted Conversations*

Generate Media Files for CDR-Only Conversations*

File Extension(s)

Execute Only After Another Policy Executed --Choose--

Execute Only After This Export Executed --Choose--

Execute Only on Selected Servers

Combo Server 1

Media Repository Server 1

Recording Server 1

verbateamsdemo

>>

<<

>

<

Voice Format* No transcoding

Video Format* No transcoding

Desktop Recording and Screen/Application Sharing Format* No transcoding

Custom Schedule

Conversations older than* 0 year(s) 0 day(s) 00 hour(s) 00 minute(s)

Conversation Detail Fields

+

Save
Check Effect

Creating a direct export policy

To create a direct export data management policy, follow the steps below:

Step 1 - [Create a Storage target](#) for the export policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Export** as the action

Step 4 - Enable the **Direct Export** option

Step 5 - Select the **Destination Storage Target** you created from the list

Step 6 - Configure policy specific settings as follows:

Name	Description
Decrypt Encrypted Conversations	If a conversation related files are encrypted, the system can automatically decrypt the files before exporting. Original files remain encrypted.
Export Attachments in IM Conversations	For specific integrations (Skype for Business, Symphony), the system can automatically export file attachments with instant message conversations.

Step 7 - Configure **Filtering Criteria** to specify which conversations should be exported by this policy

Step 8 - Assigning the policy to users on the [User Configuration](#) page or using [Active Directory synchronization](#)

Voice Quality Check policy

This article describes the Voice Quality Check data management policy.

The Voice Quality Check storage policy is implemented to check the quality of the voice recordings and detect noise, garbled voice, and other problems.

It is available as part of the upload policy (similar to the encryption/signing) and as a stand-alone policy.

It is recommended to configure quality checks with the upload policy. Otherwise, during the process, the system will download the media file to the Verba server running the process and check the quality of the recording.

Running the quality check puts an extra ~15% load on the recording servers.

For more information refer to the [Voice Quality Check](#) article.

Configuring the Voice Quality Check with Upload policy

To create an upload policy with Voice Quality Check, follow the steps below:

Step 1 - [Create a Storage target](#) for your policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Upload** as the action

Step 4 - Select the storage target you created from the list

Step 5 - Check the **Voice Quality Check** checkbox

Step 6 - Optionally define a value for the **Send Alerts When Score(s) are Below the Following Thresholds** setting to allow sending alerts when the overall or the individual voice quality check scores are below the configured value(s). The alert will be triggered if any of values are below the configured threshold. The greyed values represent the recommended threshold for each setting.

Step 7 - Select your filters to specify which conversations should be uploaded and checked by this policy

Step 8 - Click on **Save**

Upload

Action* Upload policies should only be used when there is a requirement for multiple storage targets or WORM storages. To use upload policies, the feature must be enabled on the Verba Recording Servers. It is also recommended to create an upload policy which does not contain filters, to avoid leaving recordings on the Recording Servers. This special policy needs to be configured with the lowest priority (lowest number).

Destination Storage Target* VoXcheck - C:\teststorage

Retention Period (days)

Automatically Delete Conversations after the Retention Period is Over*

Prefer User's Retention*

Voice Quality Check*

Send Alerts When Score(s) are Below the Following Thresholds

Total Score	75
Configure threshold values ▼	
RTP Loss	90
SRTP Decryption Errors	95
Decoding Errors	95
Media Mixing Errors	90
Volume	60
Silence	65
Noise	60
Beeps and Clicks	60
Sharp Amplitude Changes	65

Configuring the Voice Quality Check policy

To create a Voice Quality Check policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **Voice Quality Check** as the action

Step 3 - Optionally define a value for the **Send Alerts When Score(s) are Below the Following Thresholds** setting to allow sending alerts when the overall or the individual voice quality check scores are below the configured value(s). The alert will be triggered if any of values are below the configured threshold. The greyed values represent the recommended threshold for each setting.

Step 4 - Select your filters to specify which conversations should be affected by this policy

Step 5 - Click on **Save**

Disable Voice Quality Check for Skype for Business screen share recordings

It is possible to disable the scoring of the SfB screen share recordings in the service configuration:

Step 1 - Open the Verba Web Interface and go to the **System \ Servers** menu.

Step 2 - Select the Recording Server / Single Server from the list, then go to the **Change Configuration Settings** tab.

Step 3 - Set the **Storage Management \ Voice Quality Check \ Process Skype For Business Appshare Conversations** setting to **No**.

Step 4 - Click on the



icon.

Step 5 - Repeat steps 2-4 on all Recording Servers / Single Servers where Skype for Business recording is configured.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, and you will be redirected to the **Configuration Tasks** tab. Review the list of affected services and if service restarts are required (or the service is able to reread the new settings without a service restart). Click on the **Execute** button in order to execute the changes.

Transcode policy

This article describes the transcode data management policy.

The transcode action for a policy allows you to change the format of your audio call recordings and create a set of filters to specify which conversations should this format be applied to.

During the execution of policies with this action, the original recordings are converted to the new format and then deleted, so the audio files will only be accessible in the new format afterward.

To create a transcoding policy, follow the steps below:

Step 1 Follow the generic policy creation steps described on the [Data management policies](#) page

Step 2 Select **Transcode** as the action

Step 3 Select the format you wish to convert the files to.

Step 4 Select your filters to specify which conversations should be transcoded by this policy

Data Management Policy Configuration Add New Data Management Policy
Back to Previous Data Management Policy List

[Data Management Policy Data](#) [SQL Query](#) ?

▼ Data Management Policy Data

ID* 7

Name* UK - Keep Conversations within Jurisdiction

Enabled* Yes

Priority* 60
Higher priority policies are processed first when the 'older than' dates are equal.

Action* Transcode

Decrypt Encrypted Conversations*

Execute Only on Selected Servers

Combo Server 1
Media Repository Server 1
WIN-55VUHCFB0GG

>> <<

Voice Format* Uncompressed PCM 16 bit in WAV
The original files will be deleted.

Data Import policy

This article describes the Data import policy.

To set up a Data import policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **Data Import** as an action.

Step 3 - Select the **Import Source Type** according to the location from where the data will be imported.

The screenshot shows a configuration form for a Data Import policy. The fields are as follows:

- Name***: Import
- Enabled***: Yes
- Priority***: 10
Higher priority policies are processed first when the 'older than' dates are equal.
- Action***: Data Import
- Import Source Type***: (Empty dropdown menu)
- Execute Only on Selected Servers**:
- Server Selection**: A list of servers with a right arrow button (>>) and a left arrow button (<<). The server `AUTOTEST2.VERBATEST.LOCAL` is currently in the list.

Step 4 - If applicable, configure the **Enable Recording Rules** option.

Once the policy is saved it is effective and will be executed according to the policy execution schedule.

Advanced IM Export policy

This article provides a description of the Advanced IM Export data management policy. The system provides multiple options to export data from the platform. Export policies are recommended when large volumes of data have to be exported from the system on an ongoing basis. For more information on the available export options and their comparison, see [Export](#).

The export policies are executed by the Storage Management Service on the Media Repository/Application Servers.

An export data management policy creates a copy of the selected conversations and places the data in a configurable storage/export location. It consists of a ([previously created](#)) storage/export target, and a set of filters to choose which conversations should be exported. Policies with the export action do not modify or impact the original conversations in any way. The exported data is not accessible in any way from the system.

Creating an Advanced IM Export policy

To create an export data management policy, follow the steps below:


Step 1 - [Create a Storage target](#) for the export policy

Step 2 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 3 - Select **Advanced IM Export** as the action

Step 4 - Select the **Destination Storage Target** you created from the list. **Only SMTP Storage Target is supported!**

Step 5 - Configure policy-specific settings as follows:

Name	Description
Decrypt Encrypted Conversations	If conversation-related files are encrypted, the system can automatically decrypt the files before exporting. Original files remain encrypted.
Export Attachments in IM Conversations	Export file attachments with instant message conversations.
Export Conversations Based on	<ul style="list-style-type: none">• Users: Participant-based export will produce data for each configured user or participant (depending on configuration) which will result to data duplication.• Channels/Chats: Conversation-based export will produce data only once for exported conversations avoiding duplications. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p> The chat/channel based export option should not be used with the Export API based integrations. Due to limitations in the Microsoft Export API, the export process might not be able to identify all relevant data for the export and messages will be missing from the export. The chat/channel based export was primarily designed and implemented for DLP / Webhook based integrations.</p></div>

Step 6 - Configure **Custom Schedule** if you want to run the export in a specified time

Step 7 - Configure **Filtering Criteria** to specify which conversations should be exported by this policy

▼ Data Management Policy Data

Name*

Enabled* Yes No

Priority* 250
Higher priority policies are processed first when the 'older than' dates are equal.

Action* Advanced IM Export

Destination Storage Target* Teams Advanced IM Export

Decrypt Encrypted Conversations*

Export Attachments in IM Conversations*

Export Conversations Based on* Users Channels/Chats

Export Messages According to Timezone* GMT+00:00 - GMT
Greenwich Mean Time
17:18:11

Successfully Exported up To

Execute Only on Selected Servers

Combo Server 1 Media Repository Server 1 Recording Server 1 verbateamsdemo	>> <<	
---	----------	--

Adjust Retention for Media-Only Records policy

This article describes the Adjust Retention for Media-Only Records data retention policy action.

The Adjust Retention for Media-Only Records policy is implemented to allow adjusting the retention of the Media-Only records with the retention of the referencing CDR-Only records. This policy should only be used when the retention of the Media-Only records cannot be set directly with an upload policy for some reason (Genesys Active Recording, BT IPTrade TPO based recording). For instance, the retention of the recorded conversations depends on additional metadata which is only available on the CDR-Only records. In that case, the upload policy for the CDR-Only records will set the retention based on the user/group information or based on a custom metadata field (e.g. call center queue name in the Genesys call center). The upload policy for the Media-Only records should either set the retention to the lowest used by the system or not set at all. And once the records are uploaded, the Adjust Retention for Media-Only Records policy can be scheduled to synchronize the retention. This policy must run after the retention is set for the CDR-Only records, otherwise, the system will not be able to adjust the retention for the Media-Only records. The best practice is to schedule the Adjust Retention for Media-Only Records policy for the night hours.

The new retention setting is updated on the supported storage platforms as well, using the API integration, see [WORM](#) for more information.

Reducing the Retention Period is not possible when user-based or policy-based retention is used, for more information see [Data retention](#).

The Adjust Retention for Media-Only Records policy is a new type of policy that is implemented in a different way than the other policies. The policy maintains two timestamps in order to reduce the number of database record scans:

- **Processed up to Recording Start Time:** when the processing is done for a given point in time, the system notes the Start Time of the latest processed recording and will not scan the records before this time.
- **Processed up to Update Timestamp:** when certain CDR data changed, the records should be re-evaluated by the policies. For example, if the record was moved to a storage target, or got a label, then the policies that did not match previously should be checked again if they match it after the change. When such change occurs, the Update Timestamp of the record will be set to the current time, and the policies will reevaluate the record

Configuring the Adjust Retention for Media-Only Records policy

To create an Adjust Retention for Media-Only Records policy, follow the steps below:

Step 1 - Follow the generic policy creation steps described on the following page: [Data management policies](#)

Step 2 - Select **Adjust Retention for Media-Only Records** as the action

Step 3 - Select your filters to specify which conversations should be affected by this policy. It is recommended to use filters such as **Source Platform** to narrow down the records affected by the policy

Step 4 - Click on **Save**

Data retention


- [Retention period management](#)
 - [Deletion policy based](#)
 - [Policy-based retention period](#)
 - [User-based retention period](#)
- [Legal Hold](#)
- [Data retention for advanced data models](#)


Retention period management

With Data Retention we refer to the process of maintaining records based on a pre-configured, automatic basis. This covers the deletion of conversations after a given amount of time, moving conversations to archive locations, creating backups of the stored media, etc.

The retention period refers to the duration for which a certain conversation needs to be kept after being recorded and must not be deleted. There are 3 main ways to configure this period in Verba, as shown in the sections below. Conversations that have a defined retention time can be configured to be deleted automatically when their period expires.

	User-based retention period	Policy-based retention period	Deletion policy
Set when recording is finished	Yes	Yes	No
Set on supported WORM storages	Yes	Yes	No
Storage target support	All	All	All
Recordings protected during the retention period	Yes	Yes	No
AD sync support	Yes	No	No
User-level configuration available	Yes	Yes, but complex	Yes, but complex
Requires retention policy	Yes (Upload, Move)	Yes (Upload, Move)	Yes (Delete)
The retention period can be increased	Yes	Yes	Yes
The retention period can be decreased	No	No	Yes
Manual delete during the retention period	No	No	Yes
Deletion is executed by Verba	Yes	Yes	Yes
Legal hold support	Yes	Yes	Yes

 The system is not able to protect files from system administrators having full access to a specific folder and delete/modify files. If the drive should be physically protected as well, then we recommend using WORM storage instead.

 Deletion policies have an additional confirmation window showing the number of affected conversations, which helps ensure that only the intended users are covered by this policy.

Deletion policy based

Separate deletion policies can be configured to periodically delete conversations that are older than the specified value. The setup is very easy, but a misconfiguration can easily lead to the unintended deletion of certain calls.

There is no retention period configured for the conversations stored in the system, so an Administrator is able to delete conversations from the web interface if he has the right to do so.

⚠ Separate deletion policies should only be configured when the retention period (Policy- or User-based) cannot be set for some reason.

For configuration information refer to the [Delete policy](#) article.

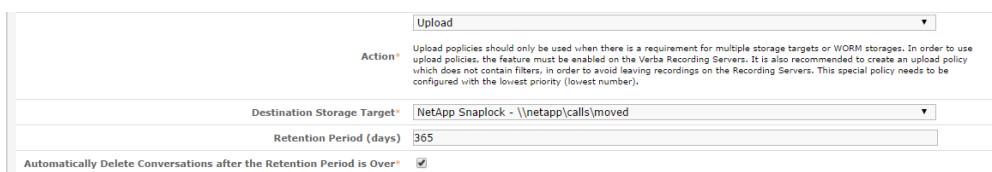
Policy-based retention period

The retention period setting in the upload and move policies allows setting the retention period right after the system compiles the recorded file. This protects the recording from accidental or intentional deletion attempts until the retention period expires.

The retention period is set on the supported WORM storages (for more information, see [WORM](#)) and enforced on ANY other storage target by Verba. Customers can use a simple SMB folder on the network and the Verba system will enforce the retention time.

The retention period setting in the upload and move policies should be used whenever possible, as shown in the image below. No separate deletion policies should be used in these cases to enforce retention time.

Once the retention period is over, a hidden background deletion process will delete the conversation, no separate policy configuration is required. The retention period cannot be reduced, it can only be increased by a separate data retention policy.



For configuration information refer to the [Move Media policy](#) or [Upload policy](#) articles.

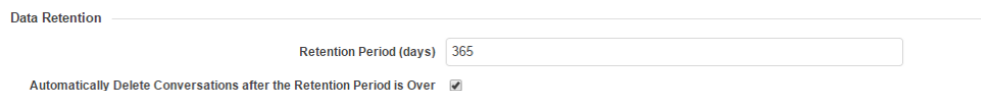
User-based retention period

The retention period can be configured on a user level, that can be used to override any policy-based retention configuration. This simplifies configuration in large deployments.

The retention period setting is set on the supported WORM storages (for more information, see [WORM](#)) and enforced on ANY other storage target by Verba. Customers can use a simple SMB folder on the network and the Verba system will enforce the retention time.

The retention period setting should be used whenever possible, as shown in the image below. No separate deletion policies should be used in these cases to enforce retention time.

Once the retention period is over, a hidden background deletion process will delete the conversation, no separate policy configuration is required. The retention period cannot be reduced, it can only be increased by a separate data retention policy.



Legal Hold

Verba provides the ability to place conversations on Legal/Litigation Hold, ensuring that no automated policies or even people with sufficient rights can delete these conversations. This option effectively overwrites the configured retention times in the system and can also apply the Legal Hold on conversations stored on supported WORM storages, see [Storage and export targets](#).

For more information refer to the [Legal Hold](#) article.


Data retention for advanced data models

For more information on the available data models, see [Data models](#)

The advanced data models are based on 2 separate record types: CDR-Only and Media-Only records. These data models are used by multiple integrations (trader voice, Genesys, Microsoft Teams Instant Messaging, etc.) where there is no way to correlate conversation data records to a single media entry or file. In this model, the retention period of the 2 record types is set separately. In most cases, the Media-Only records are automatically linked to the recorded users, the same way as CDR-Only records. However, there are exceptions, where a single Media-Only records can be referenced by multiple CDR-Only entries belonging to different users. This makes defining the retention period of the Media-Only records more difficult which requires further considerations for choosing the right retention period configuration. The following table summarizes the information about the data retention configuration for supported integration using the advanced data model:

Integrations with Advanced Data Model	Data Retention Configuration
BT ITS	<p>Both CDR-Only and Media-Only records can be linked to recorded users by configuring the recorded extensions. The upload policy configuration can be used to set the retention time based on recorded users/traders for both record types.</p> <p>Deletion policies can also be used, but not recommended.</p>
BT IP Trade turret based recording	<p>Both CDR-Only and Media-Only records can be linked to recorded users by configuring the recorded extensions. The upload policy configuration can be used to set the retention time based on recorded users/traders for both record types.</p> <p>Deletion policies can also be used, but not recommended.</p>
BT IP Trade TPO based recording	<p>CDR-Only records can be linked to recorded users by configuring the recorded extensions, but not all Media-Only records. In the case of open lines, the system only creates a single Media-Only record which is referenced by multiple CDR-Only entries belonging to different users. The recommendation is to set the retention period of these Media-Only records to the highest/longest retention period in the system. This can be achieved by either assigning the TPO lines (recorded extensions in the system) to a technical user which defines the retention period or using upload policy filters to apply the retention period for these Media-Only records.</p>
IPC Unigy	<p>Both CDR-Only and Media-Only records can be linked to recorded users by configuring the recorded extensions. The upload policy configuration can be used to set the retention time based on recorded users/traders for both record types.</p> <p>Deletion policies can also be used, but not recommended.</p>
Speakerbus	<p>Both CDR-Only and Media-Only records can be linked to recorded users by configuring the recorded extensions. The upload policy configuration can be used to set the retention time based on recorded users/traders for both record types.</p> <p>Deletion policies can also be used, but not recommended.</p>
Cloud9 Call Data API	<p>Both CDR-Only and Media-Only records can be linked to recorded users by configuring the recorded extensions. The upload policy configuration can be used to set the retention time based on recorded users/traders for both record types.</p> <p>Deletion policies can also be used, but not recommended.</p>

Genesys active recording	<p>CDR-Only records can be linked to recorded users by configuring the recorded extensions, but Media-Only records cannot always be linked to single users. For various call scenarios (multiple recorded agents are on the same conference call), the system creates a single Media-Only record which is referenced by multiple CDR-Only entries belonging to different users. The recommendation is to set the retention period of these Media-Only records to the highest/longest retention period in the system. This can be achieved by either assigning the Genesys directory numbers (recorded extensions in the system) to a technical user which defines the retention period or using upload policy filters to apply the retention period for these Media-Only records.</p>
Microsoft Teams Instant Messaging	<p>CDR-Only records can be linked to recorded users by configuring the recorded extensions, but Media-Only records (representing the chat messages for a day for a chat conversation/room) cannot be linked to users. The system automatically applies the retention period configuration on the Media-Only records according to the following priority. The retention period can only be applied through the recorded extension or user configuration. The upload policy cannot be used to set the retention because the system does not generate files on the Recording Servers (except attachments).</p> <ol style="list-style-type: none"> 1. Data Retention setting of the recorded extension of the user which is linked to the related CDR-Only record (the longest one will be selected if there are multiple related CDR-Only entries) 2. Data Retention setting of the user which is linked to the related CDR-Only record (the longest one will be selected if there are multiple related CDR-Only entries) 3. In Multi-Tenant mode, the Data Retention setting of the Environment which is linked to the Microsoft Teams tenant

 On deletion, the system does not check if a Media-Only record has CDR-Only records referencing it or not. It will delete the Media-Only records according to the defined retention period or deletion policy configuration. It is highly recommended to carefully consider the retention period configuration to ensure that Media-Only records are always retained until all the related CDR-Only records.

WORM

Overview

WORM (Write Once Read Many) storages are specifically designed for strict regulatory requirements where the data must be locked for a period of time. WORM storages have the following characteristics:


- When data is uploaded to the storage, the retention period must be defined.
- During the retention period, the data is immutable, it cannot be altered or deleted.
- During the retention period, the data can be read or downloaded at any time.
- The retention period of the data cannot be decreased, it can only be increased.
- Many vendors provide legal hold or litigation hold which can override the retention period of the data in such a way that even when the retention period expires, the data will still be locked until the legal hold is active on the data.
- Some vendors only provide WORM support on a folder/container/bucket level and not for individual data. In this case, the system cannot be integrated directly with the storage WORM features. Alternatively, the system can be configured to align the application level retention configuration with the settings on the storage. For example [Immutable Blob Storage](#).

The system provides WORM capabilities on 2 levels:

1. Application level: the system can enforce WORM specific features (data locking under the retention period, legal hold, etc.) in the application layer. While these features can ensure that the data is locked for the retention period and cannot be altered or deleted through the application, if the data is stored on non-WORM capable storage infrastructure, the data can be potentially directly accessible on the storage level and subject to modification or deletion if the user has the necessary privileges. For more information, see [Data retention](#).
2. Storage level: if the storage system supports WORM specific features, the system will also automatically use those capabilities to lock the data for the retention period or to add/remove the legal hold for selected records.

The system supports the following storage solutions with WORM capabilities:

Storage Vendor	Storage Model	File Operations	WORM Operations	Retention Period	Increase Retention	Legal Hold
Dell EMC	Centera	SDK	SDK	Yes	Yes	Yes
	ECS using the Centera API /SDK	SDK	SDK	Yes	Yes	Yes
	Unity FLR	SMB	SMB File Attributes	Yes	Yes	No
	Isilon SmartLock	SMB	REST	Yes	Yes	No
NetApp	SnapLock	SMB	SDK	Yes	Yes	No
Hitachi	Content Platform	REST	REST	Yes	Yes	Yes
iTernity	iCAS	SMB	SMB File Attributes	Yes	Yes	No
Amazon	AWS S3	REST	REST	Yes	Yes	Yes
IBM	COS	REST (AWS S3)	REST	Yes	Yes	Yes

 Many of the WORM storage platforms support a default (or minimum) retention setting on the container/bucket level. This setting is not compatible with the system and cannot be used because the system can upload additional files to the storage (e.g. transcription file, transcoded video file) in which case the retention of these files is adjusted to match the original recording. If default/minimum retention is configured, the retention of these files could be longer than required which will cause unnecessary alerts in the system, because the system will not be able to delete these additional files when the retention of the recording expires.

WORM features in data management policies

Data management policies have certain features related to the WORM capabilities of the system:

Data Management Policy	Description
Upload	<p>The upload policy can set the retention period for the data. When retention is set and the storage target is WORM capable, the system will automatically set the retention on the storage platform using the available methods (SDK, REST API or SMB file attribute change).</p> <p>If the retention period is not set during upload and the data is uploaded to a WORM capable storage target, the data will be still uploaded but the retention period will not be set. This could cause issues if there is a minimum retention period configured on the storage system (some storage solutions can enforce a minimum retention period).</p>
Delete	<p>The system does not allow deleting data under retention. The system automatically filters out the records which are under retention or legal hold. This is the case also when the filter options are matching the records in the policy configuration.</p>
Increase Retention	<p>When the increase retention policy is matching records stored on a WORM storage target, the system will automatically update the retention on the storage platform using the available methods (SDK, REST API or SMB file attribute change).</p>
Copy Media	<p>The Copy Media policy has two modes:</p> <ul style="list-style-type: none">• Dual Archiving: the policy creates a copy of the media files on the new storage target and links them as second copies in the database. For more information, see Resilient storage and archiving. When dual archiving is used, either or both of the storage targets can be a WORM capable storage. No restrictions apply.• Copy and Forget: the policy creates a copy of the media files on the new storage target and rewrites the link in the database to the new storage target. The original copy is left intact. We recommend using this option when the original copy is under retention on a WORM storage and the files have to be moved to a new storage location. This means that the system will no longer manage the original copies and will not apply any policies including data retention or offer playback and download.
Move Media	<p>Not supported for data under retention</p>
Archive in DB	<p>The database record is moved to the archive table. It has no impact on the files stored on WORM storage.</p>
Archive in DB and Move Media	<p>Not supported for data under retention</p>
Encryption, Signing	<p>Not supported for data under retention</p>
Transcription	<p>Supported, except for data on EMC Centera under retention</p>
Voice Quality Check	<p>Supported, no restrictions apply</p>
Transcode	<p>Not supported for data under retention</p>
File Verification	<p>Supported, no restrictions apply</p>
Deduplicate Recordings	<p>Not supported for data under retention</p>

Export (Advanced Export, Policy- basedExport, Policy-based Direct Export)	Supported, no restrictions apply
--	----------------------------------

Network Storage (SMB/CIFS, DFS)	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
NetApp SnapLock	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
EMC Isilon SmartLock	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
EMC Centera	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	N/A
EMC Elastic Cloud Storage	EMC Elastic Cloud Storage (ECS) is supported via EMC Centera SDK or S3 Compatible Storage API														
EMC Unity with FLR	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Hitachi Content Platform	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Amazon S3	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
S3 Compatible Storage	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Microsoft Azure File Storage	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Microsoft Azure Blob Storage	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
iTernity iCAS	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes
	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
IBM COS	IBM Cloud Object Storage (COS) is supported via the S3 Compatible API														
IBM Tivoli Storage Manager	Under Retention	N/A	Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes	No	Yes	Yes

	Not Under Retention	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Bloomberg Vault: Instant Messaging	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Bloomberg Vault: Voice	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
External Verba Media Repository	-	Yes	Yes	No	No	No	No	No	No	No	No	No	No	No	No
SMTP	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Microsoft O365 Compliance Archive	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
SFTP	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No
Verint WFO	-	No	Yes	No	No	No	No	No	No	No	No	No	No	No	No

License requirements

The use of some of the storage targets requires a **specific license**. For more information, contact your Verba representative.

Managing storage and export targets

Find and list storage targets

Select the **Administration / Storage Targets** menu item. You can use the search form below the title, to filter data retention policies: just select your filter and click **Find**.

Creating a storage target

You can create a new storage target policy by clicking on the **Add New Storage Target** link on the **Data Management / Storage targets** page. After selecting the link, the following page opens.

Add New Storage Target
Back to Previous Storage Target List

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

?

▼ Storage Target Data

Name*

Type* Verba Media Repository Local Disk

Path*

Please set up this section if you want to use this folder for Online Conversations recorded on stand-alone Recording Servers.

Host Name or IP Address

Port

▼ Export Target

Export Target

▼ Drive Usage

Drive Usage

The layout of the interface to create your new storage target is determined by the storage technology you are going to be using. Please refer to the individual storage technology guides for instructions on how to configure them.

When you finished configuring your storage target, click **Save**. After this point, the storage target will be available for use by data retention policies.

Using custom windows credentials at storage targets

In most of the cases, accessing a storage resource on the network requires windows domain credentials. When using a custom credential is required, tick the "**Use custom credentials for accessing file share**" checkbox, and provide the **Login Name** (domain\user or UPN) and the **Password**.

Use custom credentials for accessing file share

Login Name

Password

Modifying and deleting storage targets

To edit a storage folder entry, you have to click on the appropriate row of the list showing the registered storage target folders. After clicking on the row, a new page opens automatically.

To make changes effective, click on the **Save** button.

When you change the folder of a storage target, it is always your responsibility to move the files in the file system, otherwise, the calls cannot be played back from the web interface.

You can delete the storage target folder by clicking on the **Delete** button.

Media Repository Local Disk

This page provides a guide to configuring a Verba Media Repository as a Storage Target in the system. You can use this type of storage target in upload policies when recording servers upload the recorded media files to a Media Repository server. For file transfer, the system uses its own property secure file transfer protocol.

This storage target cannot be used in the case there are multiple Media Repositories deployed in the system because only the local applications can access the media files on the Media Repository server (e.g. playback will not work from other Media Repository servers). alternatively, a network share can be created on one of the Media Repository servers and added as a network storage target.

For a general description of storage targets, please refer to [Storage and export targets](#).

Follow the steps below to create a new Storage target for a Verba Media Repository:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.


Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Verba Media Repository Local Disk
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)
Host Name or IP Address	Name or address of the Verba Media Repository
Port	Port used to access the Verba Media Repository (default: 20111)

Step 4 - Click **Save** to save the settings

Storage Target Configuration [Add New Storage Target](#)
[Back to Previous Storage Target List](#)

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

Storage Target Data ?

Name*

Type* Verba Media Repository Local Disk

Path*

Please set up this section if you want to use this folder for Online Conversations recorded on stand-alone Recording Servers.

Host Name or IP Address

Port 20111

Export Target

Export Target

Drive Usage

Drive Usage

When you change the folder of a storage target, it is always your responsibility to move the files in the file system, otherwise the conversations can not be played back from the web interface.

After this point, the storage target is available for use by other Verba components (e.g. [Data management policies](#)).

External Verba Media Repository

Available in version 8.4 and later

This page provides a guide to configuring an External Verba Media Repository as a Storage Target in Verba. The External Verba Media Repository storage target should be used only when the target Media Repository server belongs to a separate Verba system (with separate database)! If the target Media Repository is in the same system as the

[Network Storage](#), the storage target should be used.

For a general description of storage targets, please refer to [Storage and export targets](#).

Follow the steps below to create a new Storage target for an External Verba Media Repository:

Step 1 - Open the Verba Web interface then select **Data > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select External Verba Media Repository
Host Name or IP Address	Name or address of the External Verba Media Repository
Port	Port used to access the External Verba Media Repository (default: 20111)

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name* External repository 1

Type* External Verba Media Repository

Host Name or IP Address HR2

Port 20111

▼ Export Target

Export Target

[Save](#)

Network Storage

This page provides a guide to configuring standard network storage as a Storage Target in Verba. The system supports the following network file protocols:

- SMB/CIFS shares: version and feature support depends on the underlying Windows Operating System, for more information, see <https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>
- DFS namespaces: version and feature support depends on the underlying Windows Operating System, for more information, see <https://docs.microsoft.com/en-us/windows-server/storage/dfs-namespaces/dfs-overview>

For a general description of storage targets, please refer to [Storage and export targets](#).

Follow the steps below to create a new storage target for your network storage:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Network Storage
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)
Use custom credentials for accessing file share	<p>Defines if the system will use custom credentials to access the network storage. Enable this setting if you want to use credential-based authentication for the network storage.</p> <p>If unchecked, the system will use the service logon user to authenticate when connecting to the network storage. The service logon user has to be set for the following services on all servers:</p> <ul style="list-style-type: none">• Verba Storage Management Service• Verba Web Application Service• Verba Media Streamer and Content Server Service• Verba Screen Capture Multiplexer Service• Verba Media Utility Service
Login Name	Login name of the user authorized to access the network storage
Password	Password for the user
Export Target	When enabled, the storage target is available as an export target for all or specific users.

Step 4 - Click **Save** to save the settings

Storage Target Configuration

[Add New Storage Target](#)
[Back to Previous Storage Target List](#)



Storage Target Data

Environment* 0000 - Reference environment

ID* 56

Name* US West - NAS #1

Type* Network Storage

Path* \\uswestnas\larchive

Use custom credentials for accessing file share

Login Name

Password *****

Export Target

Export Target

Everyone Selected Users/Groups

[Save](#) [Delete](#)

i When you change the folder of a storage target, it is always your responsibility to move the files in the file system, otherwise the conversations cannot be played back from the web interface.

After this point, the storage target is available for use by other Verba components (e.g. [Data management policies](#)).

NetApp SnapLock

This page provides a guide to configuring a NetApp SnapLock storage as a Storage Target in Verba.

SnapLock is an alternative to the traditional optical "write once, read many" (WORM) data. SnapLock is used for the storage of read-only WORM data. SnapLock is a license-based, disk-based, open-protocol feature that works with application software to administer non-rewritable storage of data. The primary objective of this Data ONTAP feature is to provide storage-enforced WORM and retention functionality by using open file protocols such as CIFS. SnapLock can be deployed for protecting data in strict regulatory environments in such a way that even the storage administrator is considered an untrusted party. SnapLock provides special purpose volumes in which files can be stored and committed to a nonerasable, non-rewritable state either forever or for a designated retention period. SnapLock allows this retention to be performed at the granularity of individual files through standard open file protocols such as CIFS.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official NetApp SnapLock guide to deploy and configure the NetApp system.

Verba uses the NetApp Manageability SDK to access the WORM specific features of the Data ONTAP API.

- [NetApp SnapLock permissions](#)
 - [Configuring the DATA ONTAP API permissions on NetApp v9.x or later \(cluster mode\)](#)
 - [Configuring the DATA ONTAP API permissions on NetApp v8.x or earlier \(7-mode\)](#)
- [NetApp SnapLock compliance clock](#)
- [Creating a NetApp SnapLock target](#)
- [Configuring SSL certificates for the SnapLock Data ONTAP API connection](#)

NetApp SnapLock permissions

The system uses standard SMB protocol for file operations. The following permissions must be enabled:

- read,
- write,
- delete,
- list.

The system requires permission for the following Data ONTAP API calls:

- Cluster mode (NetApp v9.x or later with cluster mode enabled):
 - snaplock-get-node-compliance-clock
 - snaplock-set-file-retention
 - snaplock-get-file-retention
- 7-mode (NetApp v8.x or earlier):
 - snaplock-get-system-compliance-clock
 - file-set-snaplock-retention-time
 - file-get-snaplock-retention-time

Configuring the DATA ONTAP API permissions on NetApp v9.x or later (cluster mode)

Follow the steps below to create a user account on NetApp with the necessary permissions:

Step 1 - Login to the cluster **OnCommand System Manager**

Step 2 - Navigate to **Settings** by pressing the gear icon on the top right

Step 3 - Create a new cluster-level role. Click on the **Roles** link on the right panel under the **Management** section, press **Add**. In the new window define the **Role Name** and add the **Role Attributes** by clicking on the **Add** button as follows:

Command	Query	Access Level
---------	-------	--------------

snaplock compliance-clock show		All
volume file retention		All

Step 4 - Press **Add** to save the new role

Step 5 - Create a new cluster-level user. Click on the **Users** link on the right panel under the **Management** section, press **Add**. In the new window define the **Username**, **Password** and add the **User Login Method** by clicking on the **Add** button as follows:

Application	Authentication	Role
ontapi	Password	The name of the previously create cluster-level role

Step 6 - Press **Add** to save the new user

Configuring the DATA ONTAP API permissions on NetApp v8.x or earlier (7-mode)

Follow the steps below to create a user account on NetApp with the necessary permissions:

Step 1 - Login to the NetApp server via SSH

Step 2 - Run the following commands to create a new role with the required permissions:

```
useradmin role add your_new_verba_role_name -a login-http-admin,api-snaplock-get-system-complianc
```

Step 3 - Run the following commands to create a new group and assign the new role to the group:

```
useradmin group add your_new_verba_group_name -r your_new_verba_role_name
```

Step 4 - Run the following commands to create a new user and add the user to the new group:

```
useradmin domainuser add your_new_user_name -g your_new_verba_group_name
```

NetApp SnapLock compliance clock

When Verba uploads / moves media files to a NetApp SnapLock storage target, setting the retention period with auto-delete it takes the clock drift of SnapLock into account at the point of the file move. If the storage goes down at any time during the retention period (between the upload / move and the date of auto-deletion) Verba will not be able to retrieve that information, thus will try to delete the files in question earlier than SnapLock would allow it. As a result, auto-deletion by Verba policies might fail.

Creating a NetApp SnapLock target

Follow the steps below to create a new Verba Storage target for NetApp SnapLock:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select NetApp SnapLock
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)
Volume Path	<p>Specify the NetApp specific volume path. Run the following command to find out the volume path:</p> <pre>volume show</pre> <p>Example:</p> <pre>verba::> volume show Vserver Volume Aggregate State Type Size Available Used% ----- verba-01 vol0 aggr0_verba_01 online RW 3.16GB 2.05GB 31% vs1.verbatest.local test_volume vfs online RW 342.5MB 50.46MB 8% vs1.verbatest.local svm_root vmd online RW 20MB 17.48MB 7%</pre> <p>The Volume Path value is:</p> <pre>/vol/test_volume</pre>
Host Name or IP Address	<p>The connection string used by the application to connect to the NetApp SnapLock Data ONTAP API.</p> <p>Depending on the version of the NetApp SnapLock system, 7-mode or cluster mode can be configured.</p>

For 7-mode NetApp SnapLock systems:

- **7-mode system with a connection to the NetApp server:** define the FQDN or IP address of the NetApp server without defining the protocol (it will be HTTPS by default)

```
netapp_server_address
```

- **7-mode system with a connection to the vFiler:** define the hostname or IP address of the NetApp vFiler, HTTP protocol must be defined

```
http://netapp_vfiler_address
```

- **7-mode system with vFiler tunneling to allow HTTPS connections:** define the hostname or IP address of the NetApp server and the instance name of the vFiler after a comma (,) or semicolon (;), without defining the protocol (it will be HTTPS by default)

```
netapp_server_address;instancename
```

For **cluster mode**, further parameters are needed which can be advertised in the Host Name or IP Address field:

- cluster FQDN or IP address
- cluster_mode=1, which enables cluster mode in the API
- vservers, the name of the vServer hosting the storage folder
- node=node hosting the vserver

The parameters should be concatenated either with ; or ,

```
netapp_server_address;cluster_mode=1,vserver=vserver_name,node=node_name
```

The parameters can be determined from NetApp console with the following commands:

- *vserver show*
- *node show*

Example:

The IP address of the server is 10.2.1.13

```
verbalabs::> vserver show
Admin Operational Root
Vserver Type Subtype State State Volume Aggregate
test data default running running test_root test_root
verbalabs admin - - - - -
verbalabs-01
node - - - - -
```

```
verbalabs::> node show
Node Health Eligibility Uptime Model Owner Location
verbalabs-01 true true 1 days 15:54 SIMBOX
```

Then hostname field value is:

```
10.2.1.13;cluster_mode=1;vserver=test;node=verbalabs-01
```

Port	The access port of the NetApp SnapLock Data ONTAP API (443 by default)
API User	User name of the API user configured for Verba access in NetApp SnapLock
API Password	Password of the API user configured for Verba access in NetApp SnapLock
Use custom credentials for accessing the file share	It is possible to use credentials other than the service user for each NetApp SnapLock storage. Provide the username and password credentials for accessing the storage through SMB.

Step 4 - Click **Save** to save the settings

ID*	<input type="text" value="3"/>
Name*	<input type="text" value="netapp"/>
Type*	<input type="text" value="NetApp SnapLock"/>
Path	<input type="text" value="\\netapp\calls"/>

Volume Path	<input type="text" value="/vol/verbavol"/>
Host Name or IP Address	<input type="text" value="netapp"/>
Port	<input type="text" value="443"/>
API User	<input type="text" value="verba"/>
API Password	<input type="password" value="*****"/>

Use custom credentials for accessing file share

Login Name	<input type="text" value="netapp_target_user"/>
Password	<input type="password" value="*****"/>

Export Target

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

Configuring SSL certificates for the SnapLock Data ONTAP API connection

NetApp SnapLock can be configured to accept SSL connections from trusted sources only. You can configure the trusted and signed certificates used by the Verba system on the servers directly. If you intend to use multiple NetApp SnapLock systems for Verba, you need to use the same certificates for all, because it is a server-side setting in the Verba system. By default, Verba uses its own self-signed certificates for the SSL connection.

Follow the steps below to configure the certificates.

Step 1 - Copy the X.509 certificate and key files to the Verba server

Step 2 - Navigate to the **Configuration / Servers**

Step 3 - Click on the Verba server you would like to configure

Step 4 - Click on the **Change Configuration Settings** tab

Step 5 - Open the **Storage Management / Upload Targets / NetApp SnapLock** tree on a Verba Recording Server or the **Storage Management / Storage Targets / NetApp SnapLock** tree on a Verba Media Repository server or on a Verba Media Repository and Recording Server

Step 6 - Configure a trusted custom X.509 certificate for the connection

Step 7 - Click the **Save** icon and follow the instructions on the page to apply the configuration on the server

Step 8 - Repeat the steps above on all Verba servers where you move files to NetApp SnapLock

EMC Isilon SmartLock

Available in version 8.1 and later

This page provides a guide to configuring an EMC Isilon SmartLock storage as a Storage Target in the Verba Recording System.

EMC Isilon SmartLock helps you protect your critical data against accidental, premature, or malicious alteration or deletion. Because SmartLock is a software-based approach to Write Once Read Many (WORM) data protection, you can store SmartLock-protected data alongside other data types in your Isilon scale-out storage environment with no effect on performance or availability, and without the added cost of purchasing and maintaining specialty WORM-capable hardware.

SmartLock operates in either an Enterprise mode or a Compliance mode. The Compliance mode provides an extra level of protection against malicious modification of data by disabling logins by the root user. This way, you can meet regulatory compliance requirements to provide absolute retention and protection of business-critical data—including stringent SEC 17a-4 requirements.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official EMC Isilon SmartLock guide to deploy and configure the storage system. For your reference you can access OneFS 7.2 Administration guide here: <http://isiblog.emc.com/2014/11/new-features-emc-isilon-onefs-7-2/>

Verba uses the OneFS RESTful Access to the Namespace (RAN) application programming interface (API).

Creating an EMC Isilon SmartLock target

Follow the steps below to create a new Verba storage target for EMC Isilon SmartLock:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select EMC Isilon SmartLock
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)
API URL	Specify the EMC Isilon SmartLock specific share path
API User	User name of the API user configured for Verba access in EMC Isilon SmartLock
API Password	Password of the API user configured for Verba access in EMC Isilon SmartLock

Step 4 - Click **Save** to save the settings

▼ **Storage Target Data**

ID*

Name*

Type* ▼

Path

API URL

API User

API Password

Use custom credentials for accessing file share

Login Name

Password

After this point, the storage target is available for use by other Verba components (e.g. [Data retention policies](#)).

Configuring SSL certificates for the API connection

EMC Isilon SmartLock can be configured to accept SSL connections from trusted sources only. You can configure the trusted and signed certificates used by the Verba system on the servers directly. If you intend to use multiple EMC Isilon SmartLock systems for Verba, you need to use the same certificates for all, because it is a server-side setting in the Verba system. By default, Verba uses its own self-signed certificates for the SSL connection.

Follow the steps below to configure the certificates.

Step 1 - Copy the X.509 certificate and key files to the Verba server

Step 2 - Navigate to the **System / Servers**

Step 3 - Click on the Verba server you would like to configure

Step 4 - Click on the **Change Configuration Settings** tab

Step 5 - Open the **Storage Management / Upload Targets / EMC Isilon SmartLock** tree on a Verba Recording Server or the **Storage Management / Storage Targets / EMC Isilon SmartLock** tree on a Verba Media Repository server or on a Verba Media Repository and Recording Server

Step 6 - Configure a trusted custom X.509 certificate for the connection

Step 7 - Click the **Save** icon and follow the instructions on the page to apply the configuration on the server

Step 8 - Repeat the steps above on all Verba servers where you move files to EMC Isilon SmartLock

Using custom credentials for accessing file share (available from Verba 8.5)

It is possible to use credentials other than the service user for each EMC Isilon SmartLock storage. If you want to use custom credentials, check the "**Use custom credentials for accessing the file share**" checkbox, then provide the credentials.

EMC Centera

Available in version 8.7 and later

This page provides a guide to configuring an EMC Centera storage as a Storage Target in the Verba system.

Using magnetic hard disks (SATA drives) as a data storage medium, Centera provides fast, secure, on-line access to digital content such as scanned document and check images, electronic statements and other computer-generated reports, e-mail message archives, medical images, Microsoft Office documents, and many other data types that require long-term storage with immediate access.

Based on a sophisticated set of software API functions that control the creation, storage, retrieval, and retention management of data objects, EMC Centera offers a secure storage platform that satisfies regulatory compliance requirements for laws such as SEC 17a-4, Sarbanes-Oxley, and HIPAA to name a few.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official EMC Centera guide to deploy and configure the storage system.

Verba uses the EMC Centera SDK application programming interface (API) v3.4.

PEA configuration requirements

Verba needs the following capabilities:

- read (r)
- write (w)
- delete (d)
- exist (e)
- query (q)

Verba must not have the following capability:

- privileged delete (D), as this allows audited removal of information that is still under retention.

Port requirements

The following ports must be open within any customer firewalls or proxies to enable UDP and TCP traffic for both direction between the Verba servers (Media Repositories and Recording Servers) and Centera:

- ports 3682 and 3218 for CentraStar version 2.4 and later,
- port 3218 for CentraStar version 2.3 and below,
- port 3218 for EMC ECS

Creating an EMC Centera storage target

Follow the steps below to create a new Verba storage target for EMC Centera:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select EMC Centera
PEA path	Specify the path where the PEA configuration file is located. This PEA file always needs to be present at this path on each of the Verba servers (Media Repositories and Recording Servers).
Primary Cluster Address(es)	Specify the IP addresses of the Primary Centera cluster servers, separated with a comma (,)
Secondary Cluster Address(es)	Specify the IP addresses of the Secondary (Replica) Centera cluster servers, separated with a comma (,)

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name*

Type*

PEA path

You can enter multiple addresses separated by comma (,)

Primary Cluster Address(es)

Secondary Cluster Address(es)

After this point, the Storage target is available for use by other Verba components (e.g. [Data retention policies](#)).

Workflow

First, the Verba Recording Servers will try to upload the media files using the Primary Cluster Address(es). The Media Repositories will also try to read the data from these IP addresses. The system queries the IP address(es) of the Replica Clusters and saves them.

If the Primary Cluster does not respond, then the recording servers will try to write the data to the Replica Cluster. When the Primary Cluster comes online, the Recording Servers will switch back to those servers.

If the Primary Cluster does not respond, then the Media Repositories will read the data from the Secondary Cluster. When the Primary Cluster comes online, the Media Repositories will switch back to those servers.

EMC ECS

Available in version 9.0 and later

This page provides a guide to configuring an EMC ECS storage as a Storage Target in the Verba Recording System.

ECS provides comprehensive protocol support for unstructured (Object and File) workloads on a single, cloud-scale storage platform. With ECS, you can easily manage your globally distributed storage infrastructure under a single global namespace with anywhere access to content. ECS features a flexible software-defined architecture that is layered to promote limitless scalability. Each layer is completely abstracted and independently scalable with high availability and no single points of failure. Any organization can now realize true cloud-scale economics in their own data centers.

For a general description of storage targets, please refer to [Storage and export targets](#).

Verba can use the following API aspects of the EMC ECS:

EMC ECS API	Verba Storage Target type	Limitation	Example Configuration
AWS S3	S3 Compatible Storage	<ul style="list-style-type: none">No retention on storageNo legal hold on storage	<ul style="list-style-type: none">Bucket: new-bucket-512dd431Public Endpoint: http://131497703122355426.public.ecstestdrive.com/Access Key: 131497703122355426@ecstestdrive.emc.comSecret Key1: BhcdaM2FlfM2NApPqgv3XQ/je3g5zHrwtUIZ/rYS <p>For details configuration guide, see S3 Compatible Storage</p>
Centera CAS (Recommended)	EMC Centera		<ul style="list-style-type: none">You need to download the '.PEA' file from ECS. This PEA file always needs to be present at this path on each of the Verba servers (Media Repositories and Recording Servers).Primary Cluster Address(es): enter the list of ECS endpoints FQDN or IP address based on the ECS configuration <p>For detailed configuration guide, see EMC Centera</p>

There is no specific EMC ECS storage target available in the Storage Targets drop-down in the Verba interface. You have to choose one of the API options mentioned above and use the corresponding knowledge base page to configure it.

EMC Unity FLR

Available in version 9.4.1 and later

This page provides a guide to configuring an EMC Unity storage as a Storage Target in the system.

File-Level Retention (FLR) provides a software infrastructure in the Dell EMC Unity system for files to be locked, that is, protected from deletion or modification by users or storage administrators. This functionality is also known as Write Once, Read Many (WORM). FLR is available on the physical Dell EMC Unity family as well as Dell EMC UnityVSA systems. This feature is only available for file systems and is not available for VMware NFS datastores. FLR provides a cost-effective solution for NAS files throughout their life cycle. The File-Level Retention (FLR) process can be compliant with the regulatory requirements of the United States Securities and Exchange Commission (SEC) Rule 17a-4 (f) for digital storage. FLR is enabled per file system at creation time so that you have the flexibility to use regular file systems and FLR-enabled file systems within the same NAS Server. Keep in mind that FLR cannot be modified (enabled or disabled) after the creation of the file system. Once FLR is enabled, it cannot be disabled. For which reason, it is critical to be certain that the use of FLR is required. The administrator can distinguish FLR-enabled file systems by the level of protection required: self-regulation or compliance. Individual files within FLR-enabled file systems can be locked with their own unique retention dates. Only when the retention date of a locked file has expired can that file be deleted.

For more information on the FLR feature in EMC Unity, see https://www.dell.com/resources/en-us/asset/white-papers/products/storage/h17523-dell_emc_unity_file_level_retention_flr.pdf

The Verba system automatically applies the retention period on the files, using the FLR feature described above, when the files are moved /uploaded to EMC Unity. The system uses the standard SMB protocol for file operations. Note: make sure the retention period configured in Verba is not longer than the maximum allowed retention configured in EMC UnityVSA, otherwise retention will not be applied to the files uploaded (EMC UnityVSA does not apply retention at all if the retention period would be longer than maximum allowed).

If you don't want to use the FLR feature, you need to setup a standard network storage target pointing to EMC Unity, see [Network Storage](#).

For a general description of storage targets, please refer to [Storage and export targets](#).

Creating an EMC Unity target

Follow the steps below to create a new Verba storage target for EMC Unity:

Step 1 - Open the Verba Web interface then select **Data Management > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select EMC Unity
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)

Step 4 - Click **Save** to save the settings

After this point, the Storage target is available for use by other Verba components (e.g. [Data retention policies](#)).

Using custom credentials for accessing file share

It is possible to use credentials other than the service user for each EMC Unity storage. If you want to use custom credentials, check the "**Use custom credentials for accessing the file share**" checkbox, then provide the credentials.

Hitachi Content Platform

Available in version 8.7 and later

This page provides a guide to configuring the Hitachi Content Platform as a Storage Target in the Verba System.

Hitachi Content Platform (HCP) is a distributed storage system designed to support large, growing repositories of fixed-content data. An HCP system consists of both hardware (physical or virtual) and software.

An HCP repository is partitioned into namespaces. Each namespace consists of a distinct logical grouping of objects with its own directory structure. Namespaces are owned and managed by tenants.

HCP has implemented WORM (Write Once Read Many) capabilities. WORM describes a data storage device in which information, once written, cannot be modified. This protection assures that the data will not be tampered with once it is written to the device.

Verba supports the WORM features of the platform, Retention Period can be defined for recorded files.

Litigation Hold: Should compliance authorities request that the deletion of existing files be prohibited, the retention time of Litigation Hold can be set on a file or a set of files. This prevents them from being deleted regardless of their current retention status.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the [Hitachi Content Platform guide](#) to configure your service.

Creating a Hitachi Content Platform target

Follow the steps below to create a new Verba Storage target for HCP:

Step 1 - Open the Verba Web interface then select **Data > Data Management > Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**


Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Hitachi Content Platform
Service URL	The URL address, where the Verba System can upload and download the recordings. <code>https://namespace.tenant.hostname/rest</code> (e.g. <code>https://0000.contoso.hcp.contoso.com/rest</code>)
API User	API user for the Verba System
API Password	Password of the API user

Step 4 - Click **Save** to save the settings

Storage Target Configuration

[Add New Storage Target](#)
[Back to Previous Storage Target List](#)

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



Storage Target Data

Name*	<input type="text" value="Hitachi"/>
Type*	<input type="text" value="Hitachi Content Platform"/>
Service URL	<input type="text" value="https://0000.contoso.hcp.contoso.com/rest"/>
API User	<input type="text" value="API"/>
API Password	<input type="password" value="*****"/>

[Save](#)

After this, the Storage Target is available for use by other Verba components (e.g. [Data retention policies](#)).

Microsoft Azure Storage

This page provides a guide for configuring an Azure Storage service (Azure Files and Azure Blobs) as a Storage Target in Verba.

The Azure file storage can be accessed with two different methods:

- Azure Files and Azure Blobs can be accessed through a REST API
- Alternatively, Azure Files can be accessed via SMB protocol. Both SMB 2.1 and SMB 3.0 are supported.

Configuration guidance is shown for both options below.

The advantages of using Azure Storage are:

- Highly scalable: Storage keeps pace with your growing data needs, delivering petabytes of storage for the largest scenarios. Whether you're building modern applications or a high-scale big data application, Storage can handle it.
- Data is accessible globally: Storage is available in a lot of regions, letting you store your data where it makes the most business sense. Scale up or across data centers as needed, and be closer to your customers for faster access and better performance.
- Durable and highly available: Storage automatically replicates your data and maintains multiple copies—either in a single region or globally with geo-redundancy—to help guard against unexpected hardware failures.

For a general description of storage targets, please refer to [Storage and export targets](#).

Immutable Blob Storage

For more information regarding the use of Immutable Blob Storages, see: [Immutable Blob Storage](#)

Accessing Azure Files through a REST API

Creating an Azure Storage target

Follow the steps below to create a new Verba storage target for Azure Storage:

Step 1 - Open the Verba Web interface then select **Data > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system
Type	Select Microsoft Azure Storage
Azure Service	Azure Files
File Share Name	There is an access URL shown in Azure. From this URL, the <share name> attribute should be specified here. <a href="https://<storage account>.file.core.windows.net/<share name>/">https://<storage account>.file.core.windows.net/<share name>/
Access Key	Select either "Azure Storage Account Details" or "Azure Storage Connection String" based on your authentication preference.

Account Name	(If Account Details is selected.) There is an access URL shown in Azure. From this URL, the <storage account> attribute should be specified here. <a href="https://<storage account>.file.core.windows.net/<share name>/">https://<storage account>.file.core.windows.net/<share name>/
Account Key	(If Account Details is selected.) Specify the access key
Azure Storage Connection String	(If Connection String is selected.) Specify the connection string that you can find under Storage Account / Access keys menu on the Microsoft Azure Portal.

Step 4 - Click **Save** to save the settings

Name*

Type* ▼

Azure Service Azure Files Azure Blobs

File Share Name

The file share name that you have created under Storage Account / File Service menu on the Microsoft Azure Portal.

Access Key Azure Storage Account Details Azure Storage Connection String

Account Name

Account Key

The connection details (Storage account name, key) that you can find under Storage Account / Access keys menu on the Microsoft Azure Portal.

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

Accessing Azure Blobs through a REST API

Creating an Azure Storage target


Follow the steps below to create a new Verba storage target for Azure Storage:

Step 1 - Open the Verba Web interface then select **Data > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system
Type	Select Microsoft Azure Storage
Azure Service	Azure Blobs

Blob Container Name	The container name that you have created under Storage Account / Blob Service menu on the Microsoft Azure Portal. <div style="border: 1px solid #ccc; padding: 5px; background-color: #fff9e6;">  Do not specify folders or subfolders, the system does NOT support subfolders, only the root folder of the container is supported. </div>
Access Key	Select either "Azure Storage Account Details" or "Azure Storage Connection String" based on your authentication preference.
Account Name	(If Account Details is selected.) There is an access URL shown in Azure. From this URL, the <storage account> attribute should be specified here. https://<storage account>.file.core.windows.net/<share name>/
Account Key	(If Account Details is selected.) Specify the access key
Azure Storage Connection String	(If Connection String is selected.) Specify the connection string that you can find under Storage Account / Access keys menu on the Microsoft Azure Portal.

Step 4 - Click **Save** to save the settings

Name*

Type* ▼

Azure Service Azure Files Azure Blobs

File Share Name
The file share name that you have created under Storage Account / File Service menu on the Microsoft Azure Portal.

Access Key Azure Storage Account Details Azure Storage Connection String

Account Name

Account Key
The connection details (Storage account name, key) that you can find under Storage Account / Access keys menu on the Microsoft Azure Portal.

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

Accessing Azure Files using the SMB Protocol

Creating an Azure Storage using Network Storage Target

Follow the steps below to create a new Verba Storage target for Azure Storage:

Step 1 - Visit the [Microsoft Documentation](#) and create your file share. You should get an address in the following format:

\\<storage-account-name>.file.core.windows.net\<share-name>

Step 2 - Open the Verba Web interface then select **Data > Storage Targets** from the top menu.

Step 3 - Click on **Add New Storage Target**

Step 4 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Network Storage
Path	This is the path where you want to store the media files. \\<storage-account-name>.file.core.windows.net\<share-name>
Use custom credentials for accessing file share	Checked
Login Name	Account name of the Azure storage user. <storage-account-name>
Password	Access Key of the Azure storage account. To find the storage account access key, click Settings of your storage account, and then click Access keys.

Step 5 - Click **Save** to save the settings

Name* Azure Files SMB

Type* Network Storage

Path* \\verbastoragetest.file.core.windows.net\verba-test

Use custom credentials for accessing file share

Login Name verbatest

Password

Creating an Azure Storage by mounting it as a Drive

Follow the steps below to create a new Verba Storage target for Azure Storage:

Step 1 - Visit the [Microsoft Documentation](#) and create your file share. You should get a mount command in the following format:

```
net use <drive-letter>: \\<storage-account-name>.file.core.windows.net\<share-name> /u:<storage-a
```

Step 2 - Persist your storage account credentials for the virtual machine. Before mounting to the file share, first persist your storage account credentials on the virtual machine. This step allows Windows to automatically reconnect to the file share when the virtual machine reboots. To persist your account credentials, run the cmdkey command from the PowerShell window on the virtual machine. Replace <storage-account-name> with the name of your storage account, and <storage-account-key> with your storage account key:

```
cmdkey /add:<storage-account-name>.file.core.windows.net /user:<storage-account-name> /pass:<stor
```

Step 3 - Mount the file share using the persisted credentials. Once you have a remote connection to the virtual machine, you can run the net use command to mount the file share, using the following syntax. Replace <storage-account-name> with the name of your storage account, and <share-name> with the name of your File storage share:

net use <drive-letter>: \\<storage-account-name>.file.core.windows.net\<share-name>

Since you persisted your storage account credentials in the previous step, you do not need to provide them with the net use command. If you have not already persisted your credentials, then include them as a parameter passed to the net use command, as shown in the first step.

Step 4 - Open the Verba Web interface then select Policies > Storage Targets from the top menu.

Step 5 - Click on Add New Storage Target

Step 6 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Verba Media Repository Local Disk
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)

Step 4 - Click Save to save the settings

Storage Target Configuration [Add New Storage Target](#)
[Back to Previous Storage Target List](#)

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

▼ Storage Target Data ?

Name*

Type*

Path*

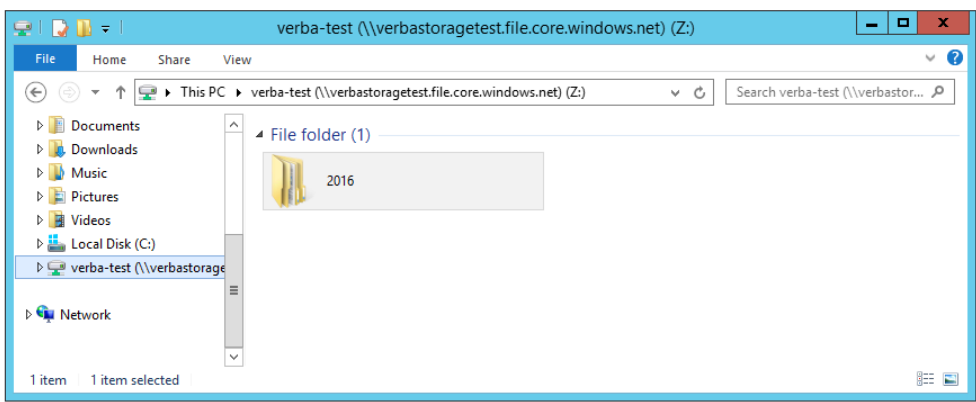
Please set up this section if you want to use this folder for Online Conversations recorded on stand-alone Recording Servers.

Host Name or IP Address

Port

▼ Export Target Export Target

▼ Drive Usage Drive Usage



After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

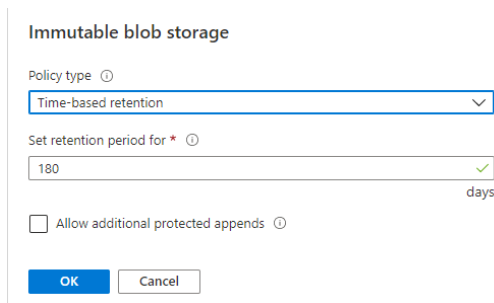
Immutable Blob Storage

Verba supports the use of [Immutable Blob storages](#). Since the Verba application cannot set the retention time of the Blob container programmatically, it has to be set in advance on the Azure side. The recommended way to use Immutable Blob Containers is creating multiple containers in advance based on how many different retention times will be used in the system.

Configuring Immutable Blob Storage

The retention time can be set at the **Access Policy** configuration of the Blob Container. In order to set it, go to the **Storage Account**, select the container in the **Containers** menu, then go to the **Access Policy** menu. Under the **Immutable blob storage** section, click on the **Add policy** button.

Set the **Policy type** to **Time-based retention**, set the retention period, then click **OK**.



Immutable blob storage

Policy type ⓘ
Time-based retention

Set retention period for * ⓘ
180 days

Allow additional protected appends ⓘ

OK Cancel

Once the retention policy is set, click on the three dots on the right, then click **Lock policy**. A separate Blob Container should be created for each retention time being used, and the proper retention period should be set for each one.

Once the Blob Containers are created and the retention times are set, the same retention times should also be set on the Verba side. Create a new [upload policy](#) for each Blob Container / retention time, and set the Retention Period setting according to the Access Policy setting of the Blob Container:



Destination Storage Target * Azure storage - container1

Retention Period (days) 180

Configure the **Data Management Filtering Criteria** section of the policy so that the right recordings will be uploaded to the right Blob Container.

A separate Upload policy has to be created for each Blob Container / retention time. If the Prefer User's Retention setting is set at the upload policy, then make sure that the proper Retention Period setting is set on the user level.

Increasing retention period

The retention period can be increased with Immutable Blob Storages also, but it also works only on the container level. If the [Increase Retention Period](#) policy is being used, then make sure that it is applied to all recordings within the Blob Container. The retention time has to be modified manually on the Azure side also by modifying the **Access Policy** setting of the container.

Moving / copying recordings to Immutable Blob Storage

When a recording is [moved](#) or [copied](#) to an Immutable Blob Container later, then its retention time on the Azure side will start from the point the files are created on the Blob Container. Therefore, retention time should be set / extended on the Verba side also according to that by using the Increase Retention Period policy.

The same happens in the case of new files when the [Transcode](#) policy is being used on recordings stored in the Blob Container.

Microsoft Office 365 Compliance Archive

Available in version 8.6 and later

This page provides a guide to configuring an O365 Exchange Web Service (EWS) Storage Target in the Verba Recording System.


Creating an Exchange Web Services (EWS) target

Follow the steps below to create a new Verba Storage target for EWS:

Step 1 - Open the Verba Web interface then select **Policies > Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Storage Target Data	
Name	Name your storage target. This name will identify this target across the system.
Type	Exchange Web Services (EWS)
Host Name or IP Address	https://office365ingestionsvc.gble1.protection.outlook.com/service/ThirdPartyIngestionService.svc You check the URL here: Archiving third-party data in Office 365
TLS Encryption	Checked
Port	443
Login Name	Third-party data mailbox username
Password	Third-party data mailbox password
Headers	
From (Header)	This is the <u>from header</u> of the message, the recipient client displays this value.
To (Header)	This is the <u>to header</u> of the message, the recipient client displays this value.
CC (Header)	This is the <u>CC header</u> of the message, the recipient client displays this value.
 (add new header)	You can specify your own key-value headers here.
Content	
Subject	This is the subject of your e-mail.
Body	This is the body content of your e-mail.
Attachments	



(add new attachment)

You can add 3 different kind of attachments with the following attributes:

- Metadata:
 1. Content-Type
- Media:
 1. Content-Type
- Text file:
 1. Content-Type
 2. Filename
 3. Content

If you leave the Content-Type field empty the default application/x-msdownload will be used.

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name*	<input type="text" value="Exchange Web Services Storage Target"/>
Type*	<input type="text" value="Exchange Web Services (EWS)"/>
Email Template	<input type="text" value="Exchange Web Services"/> <input type="button" value="Load"/>
Host Name or IP Address	<input type="text" value="https://office365ingestionsvc.gble1.protection.outlook.com/service/ThirdPartyIngestionService.svc"/>
TLS Encryption	<input checked="" type="checkbox"/>
Port	<input type="text" value="443"/>
Login Name	<input type="text" value="mailbox@yourdomain.com"/>
Password	<input type="password" value="••••••"/>

▼ Headers

From (Header)	<input type="text"/>
To (Header)	<input type="text"/>
CC (Header)	<input type="text"/>
	<input type="button" value="+"/>

▼ Content

Subject	<input type="text" value="Verba Technologies -- Export Action"/>
Body	VerbaConversationID:[VerbaConversationID] PlatformConversationID:[PlatformConversationID] From:[From] FromName:[FromName] FromIP:[FromIP] FromDeviceID:[FromDeviceID] FromRtpCount:[FromRtpCount] To:[To] ToName:[ToName] ToIP:[ToIP] ToDeviceID:[ToDeviceID] ToRtpCount:[ToRtpCount] StartDateTime:[StartDateTime] EndDateTime:[EndDateTime] Duration:[Duration] MediaLength:[MediaLength] RecordedParty:[RecordedParty] RecordingServer:[RecordingServer] Direction:[Direction] EndCause:[EndCause] RecordingFailed:[RecordingFailed] MediaError:[MediaError] AgentID:[AgentID] Conference:[Conference] MeetingID:[MeetingID] SilenceRatio:[SilenceRatio] TalkoverRatio:[TalkoverRatio] LongestSilence:[LongestSilence]

▼ Attachments

<input type="button" value="🗑"/>	Media File	▼	Content-Type	<input type="text"/>
				<input type="button" value="+"/>

▶ Hint

▼ Export Target

Export Target	<input type="checkbox"/>
---------------	--------------------------

After this, the Storage Target is available for use by other Verba components (e.g. [Data management policies](#)).

How to enable archiving third-party data in Office 365

Please follow the instructions provided by Microsoft on this page: [Archiving third-party data in Office 365](#)

Hint and default values

In the Headers, Content and Attachments input fields you can use the following strings to include call related metadata information:

- [VerbaConversationID]
- [PlatformConversationID]

- [From]
- [FromName]
- [FromIP]
- [FromDeviceID]
- [FromRtpCount]

- [FromLoginName]
- [FromEmailAddress]
- [FromUserCustomField0]
- [FromUserCustomField1]
- [FromUserCustomField2]
- [FromUserCustomField3]
- [FromUserCustomField4]

- [To]
- [ToName]
- [ToIP]
- [ToDeviceID]
- [ToRtpCount]

- [ToLoginName]
- [ToEmailAddress]
- [ToUserCustomField0]
- [ToUserCustomField1]
- [ToUserCustomField2]
- [ToUserCustomField3]
- [ToUserCustomField4]

- [ConferenceParticipants]

- [StartDateTime]
- [EndDateTime]

- [Duration] format: days hours:minutes:seconds

- [MediaLength]
- [RecordedParty]
- [RecordingServer]
- [Direction]
- [EndCause]

- [RecordingFailed]
- [MediaError]

- [AgentID]
- [Conference]
- [MeetingID]

- [SilenceRatio]
- [TalkoverRatio]
- [LongestSilence]

- [IMTranscript]

- [Year]
- [Month]

- [Day]
- [Hour]
- [Minute]
- [Second]
- [DateTime] format: "%yyyy.%MM.%dd %HH:%mm:%ss"

You can use the following syntax to insert the first not empty value from a range of values:

- ISNULL([value1] , [value2] , [value3])

If you leave blank fields then Verba will use the following default values:

- Header From = ISNULL([FromEmailAddress],[From],[FromName],[FromDeviceID],[FromIP],[FromLoginName],[FromUserCustomField0])
- Header To = ISNULL([ToEmailAddress],[To],[ToName],[ToDeviceID],[ToIP],[ToLoginName],[ToUserCustomField0])
- Header CC = [ConferenceParticipants]
- Title = Verba Technologies - Export action (<policy_name>) - [VerbaConversationID]

This is because there are mandatory fields (From, To) that mustn't left empty: [Mandatory fields](#).

Amazon S3

This page provides a guide to configuring an Amazon S3 service as a Storage Target in the Verba Recording System.

Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. Amazon S3 stores data as objects within buckets.

Buckets are containers for objects. You can have one or more buckets. For each bucket, you can control access to it (who can create, delete, and list objects in the bucket), view access logs for it and its objects, and choose the geographical region where Amazon S3 will store the bucket and its contents.

WORM features are also supported, which allows putting retention or legal hold on the objects created by the system. Default retention is also supported. Versioning is not supported. For more information, see [WORM](#) and <https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock-overview.html>.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official guide to configure your service: <http://docs.aws.amazon.com/AmazonS3/latest/gsg/GetStartedWithS3.html>



Creating an Amazon S3 target

Follow the steps below to create a new Verba Storage target for Amazon S3:

Step 1 - Open the Verba Web interface then select **Data / Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Amazon S3
Bucket	The name of your Bucket in Amazon S3 <div data-bbox="304 1509 1096 1659"><p> Bucket Naming Bucket names must contain only lowercase letters, numbers, periods (.) and dashes (-).</p></div> <div data-bbox="304 1733 1096 1852"><p> Do not specify folders or subfolders, the system does NOT support subfolders, only the root folder of the bucket is supported.</p></div>

Region	<p>Region-specific endpoints that Amazon S3 supports.</p> <p>For more information, see http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</p>
Enable Object Lock and Legal Hold	Select the checkbox if the object lock feature will be used for retention and legal hold.
Object Lock mode	<p>For using the Object Lock feature of Amazon S3 for retention and Legal Hold, it also has to be enabled on the Amazon side. This can be done at the setting of the bucket. For more information, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html</p> <p>There are two levels:</p> <ul style="list-style-type: none"> • Governance: Users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period. • Compliance: A protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.
Addressing Mode	<p>Specifies the used for connecting to the Amazon S3 bucket. For more information, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/VirtualHosting.html</p> <p>Virtual Hosted Style: Changes the HTTP <input type="text" value="HOST"/> header to include the bucket name. For example https://bucketname.s3.region.amazonaws.com/key-name</p> <p>Path Style: Sets the bucket in the <input type="text" value="URL"/>.</p> <p>For example https://s3.region.amazonaws.com/bucket-name/key-name</p>
Access Key Id	Access Key Id of your Amazon S3
Secret Access Key	Secret Access Key of your Amazon S3

Step 4 - Click **Save** to save the settings

Name* Amazon storage

Type* Amazon S3

Bucket recordingbucket

Region eu-west-1

Enable Object Lock and Legal Hold

Object Lock mode Compliance

Access Key Id ASDLIOWRE754Q6ASLKW34

Secret Access Key

Forward proxy configuration

In order to configure a forward proxy for the Amazon S3 connections, follow the steps below:

In the Verba menu, navigate to **System / Servers**, select the appropriate server, then click on the **Change Configuration** tab.

On this tab, fill in the configuration under **Storage Management / Storage Targets / Amazon S3**. See the table below for reference.

Configuration item	Description
Forward Proxy Address	IP address or FQDN of the forward proxy. When defined, the system will connect through a forward proxy.
Forward Proxy Port	The port of the forward proxy
Forward Proxy Username	Username for basic authentication for the forward proxy server
Forward Proxy Password	Password for basic authentication for the forward proxy server

TLS connection configuration

By default, Verba uses the server certificate for the TLS connection. Its details can be found under the **Server Certificate** node in the server configuration.

When needed, a custom certificate can be used instead, and other connection properties can be also changed.

In the Verba menu, navigate to **System / Verba Servers**, select the appropriate server, then click on the **Change Configuration** tab.

On this tab, fill in the configuration under **Storage Management / Storage Targets / Amazon S3**. See the table below for reference.

Configuration item	Description
Use Https Protocol	Set to yes, if a secure connection should be used

Storage Class	<p>Specifies what storage class should be used. Available options:</p> <p>Standard</p> <p>Reduced Redundancy</p> <p>Reduced Redundancy Storage (RRS) is a new storage option within Amazon S3 that enables customers to reduce their costs by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. It provides a cost-effective, highly available solution for distributing or sharing content that is durably stored elsewhere, or for storing thumbnails, transcoded media, or other processed data that can be easily reproduced.</p>
Connection Timeout (ms)	Defines the connection timeout value in milliseconds.
TLS Key password	Password for the certificate
TLS Key file	Path to the certificate Key file
TLS Certificate	Path to the certificate
TLS CA Certificate	Path to the CA certificate

S3 Compatible Storage

This page provides a guide to configuring S3 Compatible storage as a Storage Target in Verba. Verint does not certify S3 compatible storage platforms unless it is specified otherwise. Customers successfully deployed Verba with the following storage platforms using the S3 Compatible storage target:

- EMC ECS
- IBM COS
- Caringo

Verba supports both the V2 (REST) and V4 authentication types.

WORM features are also supported in the case of IBM COS storage, which allows putting retention or Legal Hold on the objects created by Verba. For more information, see [WORM](#).

For a general description of storage targets, please refer to [Storage and export targets](#).




Creating an S3 Compatible storage target

Follow the steps below to create a new Verba Storage target for S3 Compatible storage target:

Step 1 - Open the Verba Web interface then select **Data / Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select S3 Compatible Storage
Bucket	The name of your bucket <div data-bbox="384 1391 1485 1509"><p> Bucket Naming Bucket names must contain only lowercase letters, numbers, periods (.) and dashes (-).</p></div> <div data-bbox="384 1585 1485 1691"><p> Do not specify folders or subfolders, the system does NOT support subfolders, only the root folder of the bucket is supported.</p></div>
REST Endpoint	Specify the S3 compatible API endpoint. It can be found in the documentation of the storage platform. <div data-bbox="384 1883 1485 1957"><p> Do not specify folders or subfolders, the system does NOT support subfolders.</p></div>

Enable Object Lock and Legal Hold	Select the checkbox if the object lock feature will be used for retention and legal hold. This is supported only in the case of IBM COS storage.
Addressing Mode	Specifies the addressing mode used for connecting to the bucket. Virtual Hosted Style: Changes the HTTP <input type="text" value="HOST"/> header to include the bucket name. For example https://bucketname.rest-endpoint.com/key-name Path Style: Sets the bucket in the <input type="text" value="URL"/> . For example https://rest-endpoint.com/bucket-name/key-name
Request Authentication	Select either "AWS Signature Version 2" or "AWS Signature Version 4" according to the supported authentication type of the storage target being used. In the case of IBM COS storage, select "AWS Signature Version 4 IBM".
Access Key Id	Access Key Id of the S3 compatible storage
Secret Access Key	Secret Access Key of the S3 compatible storage
Region	The region of the bucket. Only required if V4 authentication is being used. In the case of on-prem storage, it can be anything.

Step 4 - Click **Save** to save the settings

Name*
 Type*
 Bucket
 REST Endpoint
 Enable Object Lock and Legal Hold
 Request Authentication
 Access Key Id
 Secret Access Key
 Region

Forward proxy configuration

In order to configure a forward proxy for the S3 Compatible storage connections, follow the steps below:

In the Verba menu, navigate to **System / Verba Servers**, select the appropriate server, then click on the **Change Configuration** tab.

On this tab, fill in the configuration under **Storage Management / Storage Targets / S3 Compatible**. See the table below for reference.

Configuration item	Description
Forward Proxy Address	IP address or FQDN of the forward proxy. When defined, the system will connect through a forward proxy.
Forward Proxy Port	The port of the forward proxy

Forward Proxy Username	Username for basic authentication for the forward proxy server
Forward Proxy Password	Password for basic authentication for the forward proxy server

TLS connection configuration

By default, Verba uses the server certificate for the TLS connection. Its details can be found under the **Server Certificate** node in the server configuration.

When needed, a custom certificate can be used instead, and other connection properties can be also changed.

In the Verba menu, navigate to **System / Servers**, select the appropriate server, then click on the **Change Configuration** tab.

On this tab, fill out the configuration under **Storage Management / Storage Targets / S3 Compatible**. See the table below for reference.

Configuration item	Description
Use Https Protocol	Set to yes, if a secure connection should be used
Connection Timeout (ms)	Defines the connection timeout value in milliseconds.
TLS Key password	Specify the password for the file that contains the certificate keys
TLS Key file	Specify the file where the certificate key is stored
TLS Certificate	Path to the certificate
TLS CA Certificate	Path to the CA certificate

Bloomberg Vault - Instant Messaging

Available in version 8.4 and later

This page guides the users through the configuration of a Bloomberg Vault service as a Storage Target in the system.

Bloomberg Vault is a cloud-based information management service that delivers compliance, eDiscovery, and enterprise, archiving by leveraging the scalability and reliability of Bloomberg's global infrastructure. Organizations use Bloomberg Vault to manage and archive a broad range of enterprise communications and collaboration data, including email, instant message (IM), mobile, files, voice data and social media. The SaaS solution provides information governance and information analytics solutions, including enterprise archiving, surveillance, eDiscovery, trade reconstruction and data analytics.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official Bloomberg Vault guide to configure the cloud service.

⚠ In Bloomberg Vault: Instant Messaging, only IM recordings can be stored.

Supported Data Management Policies	Export
Supported Record Types / Modalities	Instant Message SMS

Creating a Bloomberg Vault: Instant Messaging target

Follow the steps below to create a new Verba Storage target for Bloomberg Vault:

Step 1 - Open the Verba Web interface then select **Data > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Bloomberg
Target Email Address	Specify the Email Address of the Bloomberg Vault service
Source Email Address	Specify the Email Address that should be used to send the data to the Bloomberg Vault
SMTP Server	Address of the SMTP Server
SMTP TLS Encryption	Check the checkbox if you want to turn on SMTP TLS Encryption
Port	SMTP Port

Login Name	Email Login Name of the Source Email Address
Password	Email Password of the Source Email Address

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name*	Bloomberg Storage
Type*	Bloomberg Vault
Source Email Address	storage@bloomberg.com
Target Email Address	sender@gmail.com
SMTP Server	smtp.gmail.com
TLS Encryption	<input checked="" type="checkbox"/>
Port	465
Login Name	sender@verba.com
Password	*****

▼ Export Target

Export Target

[Save](#)

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

Bloomberg Vault - Voice

Available in version 9.3 and later

This page guides the users through the configuration of a Bloomberg Vault service as a Storage Target in the system.

Bloomberg Vault is a cloud-based information management service that delivers compliance, eDiscovery, and enterprise, archiving by leveraging the scalability and reliability of Bloomberg's global infrastructure. Organizations use Bloomberg Vault to manage and archive a broad range of enterprise communications and collaboration data, including email, instant message (IM), mobile, files, voice data and social media. The SaaS solution provides information governance and information analytics solutions, including enterprise archiving, surveillance, eDiscovery, trade reconstruction and data analytics.

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official Bloomberg Vault guide to configure the cloud service.

Supported Data Management Policies	Advanced Export
Supported Record Types / Modalities	Voice

Reconciliation

The Bloomberg Vault platform has a reconciliation feature which indicates if an uploaded record was successfully processed and ingested into the archive or not.

The reconciliation process can take up to 2 hours, it is not an instantaneous process. The export job only marks the export successful for a record when the Bloomberg Vault successfully reconciled the uploaded file.

The Bloomberg Vault generates a response XML with the processed media file hashes. If this is not a match with Verba media file hashes the Verba Storage Service will re-try the upload. This re-try can only occur 5 times after this the Verba Storage Service will log that the upload as failed and it will start the (5) tries again in the export task's next schedule time. Also, after 5 failed upload tries the Bloomberg Vault creates an alert and the Bloomberg staff will investigate what caused the failure on their side.

Due to the reconciliation feature in Bloomberg Vault, the system caches the exported files on the local disk of the Media Repository until the Bloomberg Vault system processes the uploads. It is recommended to allocate at least the size of the total export as free space always available for the system.

Creating a Bloomberg Vault: Voice target

Follow the steps below to create a new Verba Storage target for Bloomberg Vault:

Step 1 - Open the Verba Web interface then select **Data > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.

Type	Select Bloomberg Vault: Voice
SFTP Server	IP address or hostname or FQDN of the SFTP server
Port	SFTP Port
SFTP User	Login name
SFTP Password	Login password
SFTP Custom ID	The custom ID received from Bloomberg Vault. This helps Bloomberg distinguish ingested media records from different vendors/applications.

Step 4 - Click **Save** to save the settings

▼ **Storage Target Data**

Name* Bloomberg SFTP Storage

Type* Bloomberg Vault: Voice ▼

SFTP Server ftpcom.bloomberg.com

SFTP Custom ID vr73559

Port 30216

SFTP User bvtu812060930

SFTP Password

▼ **Export Target**

Export Target

Everyone Selected Users/Groups

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

SMTP

Available in version 8.6 and later

This page provides a guide for configuring an SMTP service as a Storage Target in the Verba Recording System.

SMTP target can be used for e.g. **Micro Focus Digital Safe**, **Global Relay** and any other archive that provides email injection capability. Verba offers a generic SMTP Storage Target which is highly customizable to allow companies to export the recorded calls from Verba to their own storage.

For a general description of storage targets, please refer to [Storage and export targets](#).

Currently, there are two preconfigured templates available:

- HP Digital Safe
- Global Relay

When using these templates, the emails to these storage targets will be sent in the format that these systems expect.

There is a third SMTP-based storage template implemented in the system for Bloomberg Vault. For the usage of this storage target, refer to the [Bloomberg Vault - Instant Messaging](#) article.

Creating an SMTP target



Follow the steps below to create a new Verba Storage target for SMTP:

Step 1 - Open the Verba Web interface then select **Policies > Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Storage Target Data	
Name	Name your storage target. This name will identify this target across the system.
Type	Select SMTP
Email Template (optional)	You can load pre-configured templates to the Storage Target Configuration page.
Source Email Address	This is the source e-mail address for the SMTP protocol.
Target Email Address	This is the target e-mail address for the SMTP protocol.
CC Email Address	This is the CC e-mail address for the SMTP protocol.
TLS Encryption	You can enable the TLS encryption for the SMTP protocol here.
Port	Specify the SMTP port here.
Login name	Enter the login name of your SMTP user.
Password	Enter the password for your SMTP user.

Headers	
From (Header)	This is the <u>from header</u> of the message, the recipient client displays this value.
To (Header)	This is the <u>to header</u> of the message, the recipient client displays this value.
CC (Header)	This is the <u>CC header</u> of the message, the recipient client displays this value.
 (add new header)	<p>You can specify your own key-value headers here.</p> <p>If the Date header is not used, then it will be auto-generated in the format of "%dd %MMM %yyyy %HH:%mm:%ss" , for example 07 Jan 2021 14:29:51 -0000 (UTC)</p> <p>If a [StartDateTime] or [EndDateTime] macros are used, the resulting format will be "%ddd, %dd %MMM %yyyy %HH:%mm:%ss" for exampe Thu, 07 Jan 2021 14:29:51 -0000 (UTC)</p> <p>Warning: do not use DATETIME() expression in the Date header. ISNULL() can be used.</p>
Content	
Subject	This is the subject of your e-mail.
Body	This is the body content of your e-mail.
Attachments	
 (add new attachment)	<p>You can add 3 different kind of attachments with the following attributes:</p> <ul style="list-style-type: none"> • Metadata: <ol style="list-style-type: none"> 1. Content-Type • Media: <ol style="list-style-type: none"> 1. Content-Type • Text file: <ol style="list-style-type: none"> 1. Content-Type 2. Filename 3. Content <p>If you leave the Content-Type field empty the default application/x-msdownload will be used.</p>

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name* SMTP export target

Type* SMTP

Email Template Global Relay Load

Source Email Address export@verba.com

Target Email Address export.mycompand@domain.com

CC Email Address

SMTP Server smtp.mycompany.com

TLS Encryption

Port 465

Login Name smtpAccountName

Password

▼ Headers

From (Header) ISNULL([FromEmailAddress],[From],[FromName])

To (Header) ISNULL([ToEmailAddress],[To],[ToName])

CC (Header)

 Date = [EndDateTime]

 X-Head = [VerbaConversationID]

 X-Head = myValue1



▼ Content


Subject [Modality], [NumberOfParticipants] Users, [NumberOfMessages] Messages, [DurationInMinutes] Minu

Body
From: [From]
To: [To]
Duration: [Duration] ([StartDateTime] - [EndDateTime])
Direction: [Direction]
Recorded party: [RecordedParty]

[IMTranscript HTML InUserTimezone]


▼ Attachments

 Mec ▾ Content-Type application/x-msdownload

 Met ▾ Content-Type application/x-msdownload

Content-Type text/plain

File Name extra-metadata.txt

 Tex ▾ Content
Extra metadata information in attached file:
From: [From]
To: [To]
Duration: [Duration] ([StartDateTime] - [EndDateTime])
Direction: [Direction]
Recorded party: [RecordedParty]



Additional SMTP target settings


The following settings are applies to all SMTP type storage targets (global settings):

Step 1 - Open the Verba Web interface then navigate to your media repository server

Step 2 - Click on **Change Configuration Settings**

Step 3 - Navigate to **Storage Management > Storage Targets > SMTP**

SMTP

Connection timeout (ms):	<input type="checkbox"/>	300000
TLS Key password:	<input type="checkbox"/>
TLS Key file:	<input type="checkbox"/>	
TLS Certificate:	<input type="checkbox"/>	
TLS CA Certificate:	<input type="checkbox"/>	
Enable Start TLS:	<input type="checkbox"/>	Yes 

After this point, the Storage target is available for use by other Verba components (e.g. [Data management policies](#)).

In the Headers, Content and Attachments input fields you can use these strings to include call-related metadata information: [SMTP placeholder fields](#).

SMTP: Sending EML as attachment.

- Add a text file as an attachment using the + in the Attachment section
- Give .eml as extension to the filename
- In the content field include an eml header, then the content

Example:

```
thread-index: [PlatformConversationID]
Content-Class: urn:content-classes:message
Importance: normal
Priority: normal
Date: [StartDateTime]
From: [From]
To: [To]
Message-ID: [PlatformConversationID]
Subject: Conversation [PlatformConversationID] [VerbaConversationID]
MIME-Version: 1.0
Content-Type: text/html;
charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
[IMTranscript4_HTML]
```

Screenhots:

V Conversations Quality Management Workflows Communication Policies Reports Users Data System

Storage Target Configuration

[Add New Storage Target](#)
[Back to Previous Storage Target List](#)

⚠ Your email monitoring settings have changed. Email verification is required. [Send me a verification email.](#)

?

▼ Storage Target Data

ID* 11

Name* SMTP

Type* SMTP

Email Template Global Relay **Load**

Source Email Address info@verint.com

Target Email Address gabor.vass@verba.com

CC Email Address

SMTP Server smtp.gmail.com

TLS Encryption

Port 587

Login Name


Password


▼ Headers


From (Header)

To (Header)

CC (Header)

 X-Global =

 Date =





▼ Content


Subject

Body

▼ Attachments


 Medi ▼ Content-Type

 Meta ▼ Content-Type

 Text ▼ Content-Type

File Name

Content



► Hint

▼ Export Target

Export Target

Everyone Selected Users/Groups

Figure: Example configuration for SMTP storage target with eml format attachment.

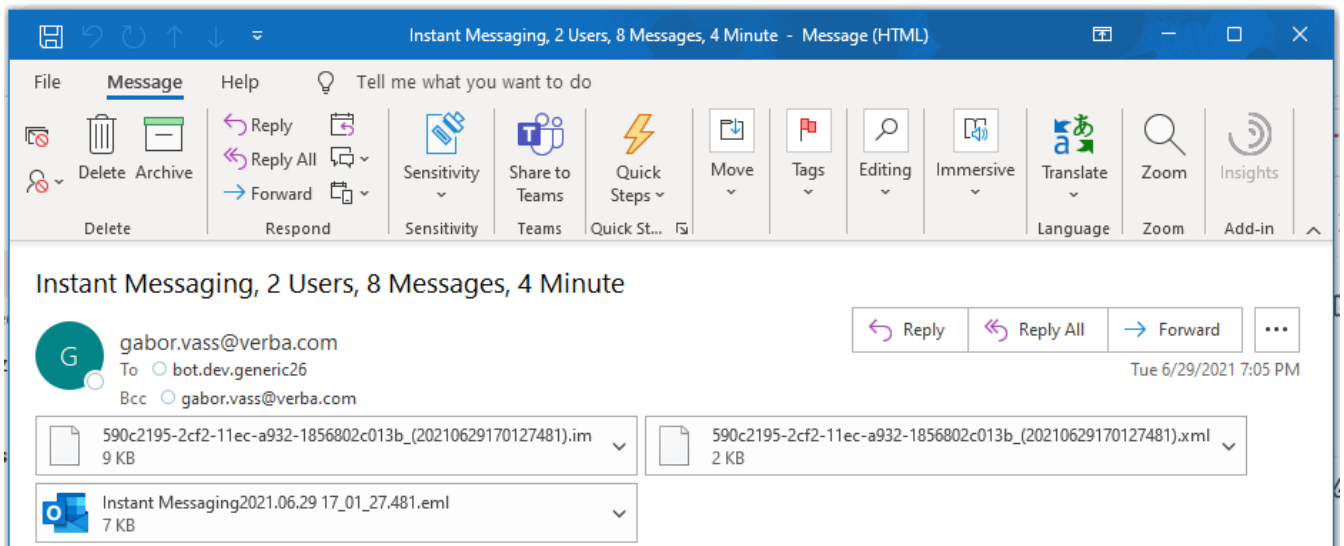


Figure: an example email containing the .im, .xml and the .eml file

SMTP Field: IMTranscript

These placeholders insert the chat messages with the following format:

Timezone: GMT

IM Dialog:

2021.08.07 18:50:27 Smith: Entered Conversation

2021.08.07 18:50:27 Smith: How may I help you?

2021.08.07 18:50:53 Joe: Entered Conversation

2021.08.07 18:50:53 Joe: Question on my Checking account

2021.08.07 18:50:57 Joe: What is that transfer fee?

2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you have an average balance of \$11,00 in your checking account. If you open a 2 year CD for \$5,000 with us you can avoid all fees.

2021.08.07 18:51:55 Joe: What is the interest rate?

2021.08.07 18:52:04 Smith: Currently it is 4.25%.

2021.08.07 18:54:20 Joe: Sounds good what do I have to do?

2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you would like to do?

2021.08.07 18:54:34 Joe: Yes

2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the new account. Anything else I can help you with?

2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.

2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?acclid=a45d7d3ffd2>

2021.08.07 18:58:43 Joe: Yeah, I got the page up.

2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.

2021.08.07 18:58:49 Smith: Left Conversation

2021.08.07 18:58:49 Joe: Left Conversation

Possible variants are:

Placeholder	Description
[IMTranscript]	Displays the IM transcript with the timezone of the Verba user who created this policy
[IMTranscript_InUserTimezone]	Displays the IM transcript in the recorded user's timezone
[IMTranscript_NoLeaveJoin]	Excludes the "Entered Conversation" and "Left Conversation" messages
[IMTranscript_NoLeaveJoin_InUserTimezone]	Excludes the "Entered Conversation" and "Left Conversation" messages in the recorded user's timezone
[IMTranscript_HTML]	Displays the messages using HTML formatting in GMT timezone
[IMTranscript_HTML_InUserTimezone]	Displays the messages using HTML formatting in the recorded user's timezone
[IMTranscript_HTML_NoLeaveJoin]	Displays the messages using HTML formatting and excludes the "Entered Conversation" and "Left Conversation" messages in GMT timezone

[IMTranscript_HTML_NoLeaveJoin_InUserTimezone]

Displays the messages using HTML formatting and excludes the "Entered Conversation" and "Left Conversation" messages in the recorded user's timezone

Example Codes:

IMTranscript

Timezone: GMT

IM Dialog:

```
2021.08.07 18:50:27 Smith: Entered Conversation
2021.08.07 18:50:27 Smith: How may I help you?
2021.08.07 18:50:53 Joe: Entered Conversation
2021.08.07 18:50:53 Joe: Question on my Checking account
2021.08.07 18:50:57 Joe: What is that transfer fee?
2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you h
2021.08.07 18:51:55 Joe: What is the interest rate?
2021.08.07 18:52:04 Smith: Currently it is 4.25%.
2021.08.07 18:54:20 Joe: Sounds good what do I have to do?
2021.08.07 18:54:30 Smith: I can open the account now and transfer $5,000. Is that what you would
2021.08.07 18:54:34 Joe: Yes
2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the
2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.
2021.08.07 18:56:01 Smith: URL pushed: https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2
2021.08.07 18:58:43 Joe: Yeah, I got the page up.
2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.
2021.08.07 18:58:49 Smith: Left Conversation
2021.08.07 18:58:49 Joe: Left Conversation
```

IMTranscript InUserTimezone

Timezone: Europe/London

IM Dialog:

```
2021.08.07 18:50:27 Smith: Entered Conversation
2021.08.07 18:50:27 Smith: How may I help you?
2021.08.07 18:50:53 Joe: Entered Conversation
2021.08.07 18:50:53 Joe: Question on my Checking account
2021.08.07 18:50:57 Joe: What is that transfer fee?
2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you h
2021.08.07 18:51:55 Joe: What is the interest rate?
2021.08.07 18:52:04 Smith: Currently it is 4.25%.
2021.08.07 18:54:20 Joe: Sounds good what do I have to do?
2021.08.07 18:54:30 Smith: I can open the account now and transfer $5,000. Is that what you would
```

2021.08.07 18:54:34 Joe: Yes

2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the

2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.

2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

2021.08.07 18:58:43 Joe: Yeah, I got the page up.

2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.

2021.08.07 18:58:49 Smith: Left Conversation

2021.08.07 18:58:49 Joe: Left Conversation

[IMTranscript NoLeaveJoin](#)

Timezone: GMT

IM Dialog:

2021.08.07 18:50:27 Smith: How may I help you?

2021.08.07 18:50:53 Joe: Question on my Checking account

2021.08.07 18:50:57 Joe: What is that transfer fee?

2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you h

2021.08.07 18:51:55 Joe: What is the interest rate?

2021.08.07 18:52:04 Smith: Currently it is 4.25%.

2021.08.07 18:54:20 Joe: Sounds good what do I have to do?

2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you would

2021.08.07 18:54:34 Joe: Yes

2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the

2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.

2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

2021.08.07 18:58:43 Joe: Yeah, I got the page up.

2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.

[IMTranscript NoLeaveJoin InUserTimezone](#)

Timezone: Europe/London

IM Dialog:

2021.08.07 18:50:27 Smith: How may I help you?

2021.08.07 18:50:53 Joe: Question on my Checking account

2021.08.07 18:50:57 Joe: What is that transfer fee?

2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you h

2021.08.07 18:51:55 Joe: What is the interest rate?

2021.08.07 18:52:04 Smith: Currently it is 4.25%.

2021.08.07 18:54:20 Joe: Sounds good what do I have to do?

2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you would

2021.08.07 18:54:34 Joe: Yes

2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the

2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.

2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

2021.08.07 18:58:43 Joe: Yeah, I got the page up.

2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.

IMTranscript HTML

<i>Timezone: GMT</i>

<h5>IM Dialog:</h5>

<p>2021.08.07 18:50:27 Smith: Entered Conversation</p>

<p>2021.08.07 18:50:27 Smith: How may I help you?</p>

<p>2021.08.07 18:50:53 Joe: Entered Conversation</p>

<p>2021.08.07 18:50:53 Joe: Question on my Checking account</p>

<p>2021.08.07 18:50:57 Joe: What is that transfer fee?</p>

<p>2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice yo

<p>2021.08.07 18:51:55 Joe: What is the interest rate?</p>

<p>2021.08.07 18:52:04 Smith: Currently it is 4.25%.</p>

<p>2021.08.07 18:54:20 Joe: Sounds good what do I have to do?</p>

<p>2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you wo

<p>2021.08.07 18:54:34 Joe: Yes</p>

<p>2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of t

<p>2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.</p>

<p>2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

<p>2021.08.07 18:58:43 Joe: Yeah, I got the page up.</p>

<p>2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.<

<p>2021.08.07 18:58:49 Smith: Left Conversation</p>

<p>2021.08.07 18:58:49 Joe: Left Conversation</p>

IMTranscript HTML InUserTimezone

<i>Timezone: Europe/London</i>

<h5>IM Dialog:</h5>

<p>2021.08.07 18:50:27 Smith: Entered Conversation</p>

<p>2021.08.07 18:50:27 Smith: How may I help you?</p>

<p>2021.08.07 18:50:53 Joe: Entered Conversation</p>

<p>2021.08.07 18:50:53 Joe: Question on my Checking account</p>

<p>2021.08.07 18:50:57 Joe: What is that transfer fee?</p>

<p>2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice yo

<p>2021.08.07 18:51:55 Joe: What is the interest rate?</p>

<p>2021.08.07 18:52:04 Smith: Currently it is 4.25%.</p>

<p>2021.08.07 18:54:20 Joe: Sounds good what do I have to do?</p>

<p>2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you wo

<p>2021.08.07 18:54:34 Joe: Yes</p>

<p>2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of t

<p>2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.</p>

<p>2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

<p>2021.08.07 18:58:43 Joe: Yeah, I got the page up.</p>

<p>2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.<

<p>2021.08.07 18:58:49 Smith: Left Conversation</p>

<p>2021.08.07 18:58:49 Joe: Left Conversation</p>

IMTranscript HTML NoLeaveJoin

<i>Timezone: GMT</i>

<h5>IM Dialog:</h5>

<p>2021.08.07 18:50:27 Smith: How may I help you?</p>

<p>2021.08.07 18:50:53 Joe: Question on my Checking account</p>

<p>2021.08.07 18:50:57 Joe: What is that transfer fee?</p>

<p>2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice yo

<p>2021.08.07 18:51:55 Joe: What is the interest rate?</p>

<p>2021.08.07 18:52:04 Smith: Currently it is 4.25%.</p>

<p>2021.08.07 18:54:20 Joe: Sounds good what do I have to do?</p>

<p>2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you wo

<p>2021.08.07 18:54:34 Joe: Yes</p>

<p>2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of t

<p>2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.</p>

<p>2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

<p>2021.08.07 18:58:43 Joe: Yeah, I got the page up.</p>

<p>2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.<

[IMTranscript HTML NoLeaveJoin InUserTimezone](#)

<i>Timezone: Europe/London</i>

<h5>IM Dialog:</h5>

<p>2021.08.07 18:50:27 Smith: How may I help you?</p>

<p>2021.08.07 18:50:53 Joe: Question on my Checking account</p>

<p>2021.08.07 18:50:57 Joe: What is that transfer fee?</p>

<p>2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice yo

<p>2021.08.07 18:51:55 Joe: What is the interest rate?</p>

<p>2021.08.07 18:52:04 Smith: Currently it is 4.25%.</p>

<p>2021.08.07 18:54:20 Joe: Sounds good what do I have to do?</p>

<p>2021.08.07 18:54:30 Smith: I can open the account now and transfer \$5,000. Is that what you wo

<p>2021.08.07 18:54:34 Joe: Yes</p>

<p>2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of t

<p>2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.</p>

<p>2021.08.07 18:56:01 Smith: URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

<p>2021.08.07 18:58:43 Joe: Yeah, I got the page up.</p>

<p>2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.<

Example Mailbox:

SMTP Field: IMTranscript2

These placeholders insert the chat messages with the following format:

```
# IM Dialog Timezone: GMT

# Start of interaction

# Participant Smith entered on 2021-08-07T18:50:27+0000
Smith (2021-08-07T18:50:27+0000): How may I help you?
# Participant Joe entered on 2021-08-07T18:50:53+0000
Joe (2021-08-07T18:50:53+0000): Question on my Checking account
Joe (2021-08-07T18:50:57+0000): What is that transfer fee?
Smith (2021-08-07T18:51:45+0000): It was for two wire transfers you did during the month. I notice you have an average balance of $11,00 in your checking account. If you open a 2 year CD for $5,000 with us you can avoid all fees.
Joe (2021-08-07T18:51:55+0000): What is the interest rate?
Smith (2021-08-07T18:52:04+0000): Currently it is 4.25%.
Joe (2021-08-07T18:54:20+0000): Sounds good what do I have to do?
Smith (2021-08-07T18:54:30+0000): I can open the account now and transfer $5,000. Is that what you would like to do?
Joe (2021-08-07T18:54:34+0000): Yes
Smith (2021-08-07T18:55:07+0000): I am sending you the web page link so you can accept the terms of the new account. Anything else I can help you with?
Joe (2021-08-07T18:55:14+0000): Thanks, I got it. That's all.
Smith (2021-08-07T18:56:01+0000): URL pushed: https://www.GoldenWestBank/newacc.asp?acctid=a45d7d3ffd2
Joe (2021-08-07T18:58:43+0000): Yeah, I got the page up.
Smith (2021-08-07T18:58:49+0000): Thank you for using Golden West Bank. We appreciate your business.

# Participant Smith left on 2021-08-07T18:58:49+0000
# Participant Joe left on 2021-08-07T18:58:49+0000

# End of interaction
```

Possible variants are:

Placeholder	Description
[IMTranscript2]	Displays the IM transcript in plain text format in GMT timezone
[IMTranscript2_InUserTimezone]	Displays the IM transcript in plain text format in the recorded user's timezone
[IMTranscript2_HTML]	Displays the IM transcript using HTML formatting in GMT timezone
[IMTranscript2_HTML_InUserTimezone]	Displays the IM transcript using HTML formatting in the recorded user's timezone Example codes

Example Codes:

IMTranscript2

```
# IM Dialog Timezone: GMT
# Start of interaction
```

Participant Smith entered on 2021-08-07T18:50:27+0000
Smith (2021-08-07T18:50:27+0000): How may I help you?
Participant Joe entered on 2021-08-07T18:50:53+0000
Joe (2021-08-07T18:50:53+0000): Question on my Checking account
Joe (2021-08-07T18:50:57+0000): What is that transfer fee?
Smith (2021-08-07T18:51:45+0000): It was for two wire transfers you did during the month. I notice
Joe (2021-08-07T18:51:55+0000): What is the interest rate?
Smith (2021-08-07T18:52:04+0000): Currently it is 4.25%.
Joe (2021-08-07T18:54:20+0000): Sounds good what do I have to do?
Smith (2021-08-07T18:54:30+0000): I can open the account now and transfer \$5,000. Is that what you
Joe (2021-08-07T18:54:34+0000): Yes
Smith (2021-08-07T18:55:07+0000): I am sending you the web page link so you can accept the terms
Joe (2021-08-07T18:55:14+0000): Thanks, I got it. That's all.
Smith (2021-08-07T18:56:01+0000): URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3>
Joe (2021-08-07T18:58:43+0000): Yeah, I got the page up.
Smith (2021-08-07T18:58:49+0000): Thank you for using Golden West Bank. We appreciate your business
Participant Smith left on 2021-08-07T18:58:49+0000
Participant Joe left on 2021-08-07T18:58:49+0000
End of interaction
[IMTranscript2_InUserTimezone](#)
IM Dialog Timezone: Europe/London
Start of interaction
Participant Smith entered on 2021-08-07T18:50:27+0000
Smith (2021-08-07T18:50:27+0000): How may I help you?
Participant Joe entered on 2021-08-07T18:50:53+0000
Joe (2021-08-07T18:50:53+0000): Question on my Checking account
Joe (2021-08-07T18:50:57+0000): What is that transfer fee?
Smith (2021-08-07T18:51:45+0000): It was for two wire transfers you did during the month. I notice
Joe (2021-08-07T18:51:55+0000): What is the interest rate?
Smith (2021-08-07T18:52:04+0000): Currently it is 4.25%.
Joe (2021-08-07T18:54:20+0000): Sounds good what do I have to do?
Smith (2021-08-07T18:54:30+0000): I can open the account now and transfer \$5,000. Is that what you
Joe (2021-08-07T18:54:34+0000): Yes
Smith (2021-08-07T18:55:07+0000): I am sending you the web page link so you can accept the terms
Joe (2021-08-07T18:55:14+0000): Thanks, I got it. That's all.
Smith (2021-08-07T18:56:01+0000): URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3>

Joe (2021-08-07T18:58:43+0000): Yeah, I got the page up.

Smith (2021-08-07T18:58:49+0000): Thank you for using Golden West Bank. We appreciate your busine

Participant Smith left on 2021-08-07T18:58:49+0000

Participant Joe left on 2021-08-07T18:58:49+0000

End of interaction

IMTranscript2_HTML

<h5># IM Dialog Timezone: GMT</h5>

<p># Start of interaction</p>

<p># Participant Smith entered on 2021-08-07T18:50:27+0000</p>

<p>Smith (2021-08-07T18:50:27+0000): How may I help you?</p>

<p># Participant Joe entered on 2021-08-07T18:50:53+0000</p>

<p>Joe (2021-08-07T18:50:53+0000): Question on my Checking account</p>

<p>Joe (2021-08-07T18:50:57+0000): What is that transfer fee?</p>

<p>Smith (2021-08-07T18:51:45+0000): It was for two wire transfers you did during the month. I no

<p>Joe (2021-08-07T18:51:55+0000): What is the interest rate?</p>

<p>Smith (2021-08-07T18:52:04+0000): Currently it is 4.25%.</p>

<p>Joe (2021-08-07T18:54:20+0000): Sounds good what do I have to do?</p>

<p>Smith (2021-08-07T18:54:30+0000): I can open the account now and transfer \$5,000. Is that what

<p>Joe (2021-08-07T18:54:34+0000): Yes</p>

<p>Smith (2021-08-07T18:55:07+0000): I am sending you the web page link so you can accept the ter

<p>Joe (2021-08-07T18:55:14+0000): Thanks, I got it. That's all.</p>

<p>Smith (2021-08-07T18:56:01+0000): URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d>

<p>Joe (2021-08-07T18:58:43+0000): Yeah, I got the page up.</p>

<p>Smith (2021-08-07T18:58:49+0000): Thank you for using Golden West Bank. We appreciate your bus

<p># Participant Smith left on 2021-08-07T18:58:49+0000</p>

<p># Participant Joe left on 2021-08-07T18:58:49+0000</p>

<p># End of interaction</p>

IMTranscript2_HTML_InUserTimezone

<h5># IM Dialog Timezone: Europe/London</h5>

<p># Start of interaction</p>

<p># Participant Smith entered on 2021-08-07T18:50:27+0000</p>

<p>Smith (2021-08-07T18:50:27+0000): How may I help you?</p>

<p># Participant Joe entered on 2021-08-07T18:50:53+0000</p>

<p>Joe (2021-08-07T18:50:53+0000): Question on my Checking account</p>

<p>Joe (2021-08-07T18:50:57+0000): What is that transfer fee?</p>

<p>Smith (2021-08-07T18:51:45+0000): It was for two wire transfers you did during the month. I no

<p>Joe (2021-08-07T18:51:55+0000): What is the interest rate?</p>

<p>Smith (2021-08-07T18:52:04+0000): Currently it is 4.25%.</p>

<p>Joe (2021-08-07T18:54:20+0000): Sounds good what do I have to do?</p>

<p>Smith (2021-08-07T18:54:30+0000): I can open the account now and transfer \$5,000. Is that what

<p>Joe (2021-08-07T18:54:34+0000): Yes</p>

<p>Smith (2021-08-07T18:55:07+0000): I am sending you the web page link so you can accept the ter

<p>Joe (2021-08-07T18:55:14+0000): Thanks, I got it. That's all.</p>

<p>Smith (2021-08-07T18:56:01+0000): URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d>

<p>Joe (2021-08-07T18:58:43+0000): Yeah, I got the page up.</p>

<p>Smith (2021-08-07T18:58:49+0000): Thank you for using Golden West Bank. We appreciate your bus

<p># Participant Smith left on 2021-08-07T18:58:49+0000</p>

<p># Participant Joe left on 2021-08-07T18:58:49+0000</p>

<p># End of interaction</p>

Example Mailbox:

SMTP Field: IMTranscript3

This IM transcript format is only available for Teams chat recordings because it is using our advanced IM data structures from the database.

These placeholders insert the chat messages with the following format:

Joe

Conversation Identifier: e5ed989a-4ec3-11ec-9be5-84fdd16620a5
Platform Call ID: 20c3bb69-7df8-4615-8b93-b2e4c5354417_19:094be214c80f4746b945e7c2cfae7fd0@thread.tacv2
Date and time: 2021.08.07 18:50:27
From Info: Joe
To Info: Smith
Participants:
Smith (smith@goldenwestbank.net), Joe (joe@litrq.site)

Smith 2021.08.07 18:50:27:
How may I help you?

Joe 2021.08.07 18:50:53:
Question on my Checking account

Joe 2021.08.07 18:50:57:
What is that transfer fee?

Smith 2021.08.07 18:51:45:
It was for two wire transfers you did during the month. I notice you have an average balance of \$11,00 in your checking account. If you open a 2 year CD for \$5,000 with us you can avoid all fees.

Joe 2021.08.07 18:51:55:
What is the interest rate?

Smith 2021.08.07 18:52:04:
Currently it is 4.25%.

Joe 2021.08.07 18:54:20:
Sounds good what do I have to do?

Smith 2021.08.07 18:54:30:
I can open the account now and transfer \$5,000. Is that what you would like to do?

Joe 2021.08.07 18:54:34:
Yes

Smith 2021.08.07 18:55:07:
I am sending you the web page link so you can accept the terms of the new account. Anything else I can help you with?

Joe 2021.08.07 18:55:14:
Thanks, I got it. That's all.

Smith 2021.08.07 18:56:01:
URL pushed: <https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2>

Joe 2021.08.07 18:58:43:
Yeah, I got the page up.

Smith 2021.08.07 18:58:49:
Thank you for using Golden West Bank. We appreciate your business.

Possible variants are:

Placeholder	Description
[IMTranscript3]	Displays the advanced IM transcript in GMT timezone
[IMTranscript3_HTML]	Displays the advanced IM transcript in the recorded user's timezone

Header Description:

Field name	Description
<blueish background first line>	<ul style="list-style-type: none">• for peer to peer chats: The name of the recorded user• for group chats: The list of participants• for channels: The "team name / channel name"
Conversation Identifier	The unique Verba identifier of the conversation
Platform Call ID	The unique room identifier of the platform
Date and time	The date and time of the very first recorded message for this conversation
From Info	The name of the recorded user
To Info	<ul style="list-style-type: none">• for peer to peer and group chats: The list of participants• for channels: The "team name / channel name"
Participants	The full list of conversation participants separated by a comma

Example Codes:

IMTranscript3

```
2021.08.07 18:50:27 Smith: How may I help you?
2021.08.07 18:50:53 Joe: Question on my Checking account
2021.08.07 18:50:57 Joe: What is that transfer fee?
2021.08.07 18:51:45 Smith: It was for two wire transfers you did during the month. I notice you h
2021.08.07 18:51:55 Joe: What is the interest rate?
2021.08.07 18:52:04 Smith: Currently it is 4.25%.
2021.08.07 18:54:20 Joe: Sounds good what do I have to do?
2021.08.07 18:54:30 Smith: I can open the account now and transfer $5,000. Is that what you would
2021.08.07 18:54:34 Joe: Yes
2021.08.07 18:55:07 Smith: I am sending you the web page link so you can accept the terms of the
2021.08.07 18:55:14 Joe: Thanks, I got it. That's all.
2021.08.07 18:56:01 Smith: URL pushed: https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2
2021.08.07 18:58:43 Joe: Yeah, I got the page up.
2021.08.07 18:58:49 Smith: Thank you for using Golden West Bank. We appreciate your business.
```

IMTranscript3_HTML

```
<h3 style="background-color:#D4E6F1;"> Joe </h3>
<table style="width:100%">
  <tr>
    <td><b>Conversation Identifier:</b></td>
    <td>e5ed989a-4ec3-11ec-9be5-84fdd16620a5</td>
  </tr>
  <tr>
    <td><b>Platform Call ID:</b></td>
    <td>20c3bb69-7df8-4615-8b93-b2e4c5354417_19:094be214c80f4746b945e7c2cfae7fd0@thread.tacv2</td>
  </tr>
  <tr>
    <td><b>Date and time:</b></td>
    <td>2021.08.07 18:50:27</td>
  </tr>
  <tr>
    <td><b>From Info:</b></td>
    <td>Joe</td>
  </tr>
  <tr>
    <td><b>To Info:</b></td>
    <td>Smith</td>
  </tr>
</table>
```

Participants:
Smith (smith@goldenwestbank.net), Joe (joe@litrq.site)
<hr style="height:3px;background-color:#333;border:none">
<p>Smith 2021.08.07 18:50:27:
How may I help you?</p>
<p>Joe 2021.08.07 18:50:53:
Question on my Checking account</p>
<p>Joe 2021.08.07 18:50:57:
What is that transfer fee?</p>
<p>Smith 2021.08.07 18:51:45:
It was for two wire transfers you did during the m</p>
<p>Joe 2021.08.07 18:51:55:
What is the interest rate?</p>
<p>Smith 2021.08.07 18:52:04:
Currently it is 4.25%.</p>
<p>Joe 2021.08.07 18:54:20:
Sounds good what do I have to do?</p>
<p>Smith 2021.08.07 18:54:30:
I can open the account now and transfer \$5,000. Is</p>
<p>Joe 2021.08.07 18:54:34:
Yes</p>
<p>Smith 2021.08.07 18:55:07:
I am sending you the web page link so you can acce</p>
<p>Joe 2021.08.07 18:55:14:
Thanks, I got it. That's all.</p>
<p>Smith 2021.08.07 18:56:01:
URL pushed: <https://www.GoldenWestBank/newacc.asp?></p>
<p>Joe 2021.08.07 18:58:43:
Yeah, I got the page up.</p>
<p>Smith 2021.08.07 18:58:49:
Thank you for using Golden West Bank. We appreciat</p>

Example Mailbox:

SMTP Field: IMTranscript4

These placeholders insert the chat messages with the following format:

Room Name: Conversation identifier=d7526721-ea74-4f18-aceb-60d52cc6c61a

Sent Time	From	Message
2021-08-07T18:50:27-0000	Smith	Entered Conversation
2021-08-07T18:50:27-0000	Smith	How may I help you?
2021-08-07T18:50:53-0000	Joe	Entered Conversation
2021-08-07T18:50:53-0000	Joe	Question on my Checking account
2021-08-07T18:50:57-0000	Joe	What is that transfer fee?
2021-08-07T18:51:45-0000	Smith	It was for two wire transfers you did during the month. I notice you have an average balance of \$11,00 in your checking account. If you open a 2 year CD for \$5,000 with us you can avoid all fees.
2021-08-07T18:51:55-0000	Joe	What is the interest rate?
2021-08-07T18:52:04-0000	Smith	Currently it is 4.25%.
2021-08-07T18:54:20-0000	Joe	Sounds good what do I have to do?
2021-08-07T18:54:30-0000	Smith	I can open the account now and transfer \$5,000. Is that what you would like to do?
2021-08-07T18:54:34-0000	Joe	Yes
2021-08-07T18:55:07-0000	Smith	I am sending you the web page link so you can accept the terms of the new account. Anything else I can help you with?
2021-08-07T18:55:14-0000	Joe	Thanks, I got it. That's all.
2021-08-07T18:56:01-0000	Smith	URL pushed: https://www.GoldenWestBank/newacc.asp?accId=a45d7d3ffd2
2021-08-07T18:58:43-0000	Joe	Yeah, I got the page up.
2021-08-07T18:58:49-0000	Smith	Thank you for using Golden West Bank. We appreciate your business.
2021-08-07T18:58:49-0000	Smith	Left Conversation
2021-08-07T18:58:49-0000	Smith	Left Conversation

Possible variants are:

Placeholder	Description
[IMTranscript4_HTML]	Displays the messages using HTML formatting in GMT timezone, formatted table

[IMTranscript4_HTML_InUserTimezone]

Displays the messages using HTML formatting in user timezone, formatted table

Example Codes:

[IMTranscript4_HTML](#)

=EF=BB=BF

```
<html>
  <head>
    <META http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">
    <style type=3D"text/css">=09=09=09=09=09th {BACKGROUND-COLOR: #E0E0EE}=09=09=09=09=09td{BAC
  </head>
  <body>
    <table width=3D"auto" table-layout=3D"fixed">
      <tr valign=3D"top">
        <td> Room Name: Conversation identifier=3Dd7526721-ea74-4f18-aceb-60d52cc6c61a</td>
      </tr>
    </table>
    <table width=3D"auto" table-layout=3D"fixed">
      <th text-align=3D"center">
        <tr>
          <th padding=3D"0.5mm">Sent Time</th>
          <th padding=3D "0.5mm">From</th>
          <th padding=3D"0.5mm">Message</th>
        </tr>
      </th>
      <tbody>
        <tr valign=3D"top">
          <td>2021-08-07T18:50:27-0000</td>
          <td>Smith</td>
          <td> Entered Conversation</td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:50:27-0000</td>
          <td>Smith</td>
          <td>
            <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
          </td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:50:53-0000</td>
          <td>Joe</td>
          <td> Entered Conversation</td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:50:53-0000</td>
          <td>Joe</td>
          <td>
            <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
          </td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:50:57-0000</td>
          <td>Joe</td>
          <td>
            <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
          </td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:51:45-0000</td>
          <td>Smith</td>
          <td>
            <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
          </td>
        </tr>
        <tr valign=3D"top">
          <td>2021-08-07T18:51:55-0000</td>
          <td>Joe</td>
          <td>

```

```
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:52:04-0000</td>
    <td>Smith</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:54:20-0000</td>
    <td>Joe</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:54:30-0000</td>
    <td>Smith</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:54:34-0000</td>
    <td>Joe</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:55:07-0000</td>
    <td>Smith</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:55:14-0000</td>
    <td>Joe</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:56:01-0000</td>
    <td>Smith</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:58:43-0000</td>
    <td>Joe</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" cl
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:58:49-0000</td>
    <td>Smith</td>
    <td>
        <pre><html><body><div data-format=3D"PresentationML" data-version =3D"2.0" clas
    </td>
</tr>
<tr valign=3D"top">
    <td>2021-08-07T18:58:49-0000</td>
    <td>Smith</td>
    <td> Left Conversation</td>
```

```
</tr>
<tr valign="top">
  <td>2021-08-07T18:58:49-0000</td>
  <td>Smith</td>
  <td> Left Conversation</td>
</tr>
</td>
<td></td>
</tr>
</tbody>
</table>
</body>
</html>
```

Example Mailbox:

SMTP Placeholder Fields

In the SMTP configuration fields one can put placeholders and macros (expressions) that will be replaced by call-related metadata information when the actual e-mail is constructed.

Here is the list of available placeholder fields with their description:

Caller Party	
[From]	Phone number or address of the caller party
[FromName]	The display name of the caller party
[FromIP]	The IP address of the caller party
[FromDeviceID]	The device identifier of the caller party
[FromRTPCount]	The RTP packet count of the caller party
Verba From Party	
[FromLoginName]	The login ID of the Verba user associated with the caller party
[FromVerbaName]	The display name of the Verba user associated with the caller party
[FromEmailAddress]	The email address of the Verba user associated with the caller party
[FromUserCustomField0], [FromUserCustomField1], ... [FromUserCustomField9]	The custom user field 0, 1, ... 9 of the Verba user associated with the caller party
Called Party	
[To]	Phone number or address of the called party
[ToName]	The display name of the called party
[ToIP]	The IP address of the called party
[ToDeviceID]	The device identifier of the called party
[ToRTPCount]	The RTP packet count of the called party
Verba To Party	
[ToLoginName]	The login ID of the Verba user associated with the called party
[ToVerbaName]	The display name of the Verba user associated with the called party
[ToEmailAddress]	The email address of the Verba user associated with the called party
[ToUserCustomField0], [ToUserCustomField1], ... [ToUserCustomField9]	The custom user field 0, 1, ... 9 of the Verba user associated with the called party
Conversation IDs	
[VerbaConversationID]	Verba unique conversation identifier
[PlatformConversationID]	Conversation identifier provided by the communication platform

Conference	
[Conference]	In the case of conference recording, it shows "true" otherwise "false"
[ConferenceParticipants]	A comma-separated list of phone numbers (and e-mail addresses when available), e.g.: "testuser1" <testuser1@verbatest.local>, "testuser2" <testuser2@verbatest.local>, "John Doe", "Jane Doe"
[NumberOfParticipants]	The number of conference participants
[MeetingID]	Meeting identifier provided by the communication platform
Conversation Time	
[StartDateTime]	The start datetime of the conversation in GMT, e.g.: 2019.05.31 16:56:16.388
[StartDate]	The start date of the conversation in GMT, e.g.: 2019.05.31
[StartTime]	The start time of the conversation in GMT, e.g.: 16:56:16.388
[EndDateTime]	The end datetime of the conversation in GMT, e.g.: 2019.05.31 16:56:46.848
[EndDate]	The end date of the conversation in GMT, e.g.: 2019.05.31
[EndTime]	The end time of the conversation in GMT, e.g.: 16:56:46.848
[Duration]	The length of the conversation formatted as: days hours:minutes:seconds
[DurationInMinutes]	The length of the conversation in minutes
[MediaLength]	The length of the recorded media file in seconds
SMTP Generation	
[Year]	The current year in GMT
[Month]	The current month in GMT
[Day]	The current day in GMT
[Hour]	The current hour in GMT
[Minute]	The current minute in GMT
[Second]	The current second in GMT
[DateTime]	The current datetime in GMT, e.g.: 2019.05.27 14:26:46.396
[PolicyName]	The name of the export policy
Conversation Details	
[Modality]	The display name of the modality, e.g.: Voice, Video, Instant Messaging, Desktop Screen, Screen & Application Share
[ModalityId]	The ID of the modality, e.g.: voice, video, instant_messaging, desktop_screen, screen_and_applicaton_share
[RecordedParty]	The value of [From] or [To] or "Unknown" when unset

[Direction]	The direction of the conversation from the system point of view as text, e.g.: "Internal", "PSTN Incoming", "PSTN Outgoing", "Inter-tenant", "Dictation", "External", "Federated Incoming", "Federated Outgoing", "Contact Center Incoming", "Contact Center Outgoing", "Conference", "Undefined"
[DirectionUser]	The direction of the conversation from the recorded user point of view as text, e.g.: "Inbound", "Outbound" or "Unknown"
[RecordingServer]	The hostname of the recording server
[EndCause]	The conversation end cause as text, e.g.: "Normal", "Caller termination", "Callee termination", "Transfer", "Hold", etc.
[UserID]	The User ID obtained from the communication platform
Errors & Statistics	
[RecordingFailed]	If the recording failed, it shows "true" otherwise "false"
[MediaError]	The media error as text (it can contain any or none, space character separated list), e.g.: "No media", "Length mismatch", "RTP duplication", "RTP loss", "SRTP decryption", "Decoding error", "Media mixing", "One direction", "Missing file", "Corrupted file"
[SilenceRatio]	Silence to call length ratio in percent, e.g.: 68
[TalkoverRatio]	The length where both participants are talking to call length ratio in percent, e.g.: 32
[LongestSilence]	Longest silence in seconds
Instant Messaging Transcript (for more details please use the links)	
[IMTranscript]	Displays the IM transcript with the timezone of the Verba user who created this policy
[IMTranscript_InUserTimezone]	Displays the IM transcript in the recorded user's timezone
[IMTranscript_NoLeaveJoin]	Excludes the "Entered Conversation" and "Left Conversation" messages
[IMTranscript_NoLeaveJoin_InUserTimezone]	Excludes the "Entered Conversation" and "Left Conversation" messages in the recorded user's timezone
[IMTranscript_HTML]	Displays the messages using HTML formatting in GMT timezone
[IMTranscript_HTML_InUserTimezone]	Displays the messages using HTML formatting in the recorded user's timezone
[IMTranscript_HTML_NoLeaveJoin]	Displays the messages using HTML formatting and excludes the "Entered Conversation" and "Left Conversation" messages in GMT timezone
Transcript_HTML_NoLeaveJoin_InUserTimezone]	Displays the messages using HTML formatting and excludes the "Entered Conversation" and "Left Conversation" messages in the recorded user's timezone
[IMTranscript2]	Displays the IM transcript in plain text format in GMT timezone
[IMTranscript2_InUserTimezone]	Displays the IM transcript in plain text format in the recorded user's timezone
[IMTranscript2_HTML]	Displays the IM transcript using HTML formatting in GMT timezone
[IMTranscript2_HTML_InUserTimezone]	Displays the IM transcript using HTML formatting in the recorded user's timezone
[IMTranscript3]	Displays the advanced IM transcript in GMT timezone

[IMTranscript3_HTML]	Displays the advanced IM transcript in the recorded user's timezone
[IMTranscript4_HTML]	Displays the messages using HTML formatting in GMT timezone, formatted table
[IMTranscript4_HTML_InUserTimezone]	Displays the messages using HTML formatting in user timezone, formatted table
[NumberOfMessages]	The number of recorded IM messages
Voice Transcription	
[Transcription]	Voice transcription text
Metadata Templates	
[Meta-TemplateID-ColumnIndex-FriendlyName]	<p>The FriendlyName is an optional syntax element and is not used by the service. It is available to make the configuration more human-readable.</p> <p>For example: [Meta-14-3-BT_ITS_Line] where the TemplateID=14 is the BT-ITS metadata template, ColumnIndex=3 is the Line field.</p>
Expressions	
ISNULL([value1] , [value2] , [value3])	First not null (empty) value will be chosen
ISIM([value])	Text in the phranteses will be only displayed when the attachment is an IM file
ISNOTIM([value])	Text in the phranteses will be only displayed when the attachment is not an IM file
ISVOICE([value])	Text in the phranteses will be only displayed when the attachment is a Voice file
ISNOTVOICE([value])	Text in the phranteses will be only displayed when the attachment is not a Voice file
ISVIDEO([value])	Text in the phranteses will be only displayed when the attachment is a Video file
ISNOTVIDEO([value])	Text in the phranteses will be only displayed when the attachment is not a Video file
ISDESKTOP([value])	Text in the phranteses will be only displayed when the attachment is a Desktop Screen file
ISNOTDESKTOP([value])	Text in the phranteses will be only displayed when the attachment is not a Desktop Screen file
ISSHARE([value])	Text in the phranteses will be only displayed when the attachment is a Screen & Application Share file
ISNOTSHARE([value])	Text in the phranteses will be only displayed when the attachment is not a Screen & Application Share file
DATETIME([value], [date format])	<p>Format date time value, using %ddd as name of day, %MMM as name of month, %yyyy as year, %MM as month, %dd as day, %HH as hour, %mm as month, %ss as second. Example: DATETIME([EndDateTime]),%ddd, %dd %MMM %yyyy %HH:%mm:%ss)</p> <p>Note: if there is a leading space in the format string, then the result will also contain a leading space.</p> <p>Warning: Do not use DATETIME() in the Headers section in the Date field.</p>

If you leave blank fields then Verba will use the following default values:

- Header From = ISNULL([FromEmailAddress],[From],[FromName],[FromDeviceID],[FromIP],[FromLoginName],[FromUserCustomField0])
- Header To = ISNULL([ToEmailAddress],[To],[ToName],[ToDeviceID],[ToIP],[ToLoginName],[ToUserCustomField0])
- Header CC = [ConferenceParticipants]
- Title = Verba Technologies - Export action (<policy_name>) - [VerbaConversationID]

SFTP

Overview

Available in version 8.6 and later

This page provides a guide for configuring an SFTP service as a Storage Target in the Verba Recording System.

Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol.

SFTP was designed by the Internet Engineering Task Force (IETF) as an extended version of SSH 2.0, allowing file transfer over SSH and use with Transport Layer Security (TLS) and VPN applications. Both the commands and data are encrypted in order to prevent passwords and other sensitive information from being transferred over the network. The functionality of SFTP is similar to that of FTP. However, SFTP uses SSH to transfer files. SFTP requires that the client user must be authenticated by the server, and the data transfer must take place over a secure channel (SSH). It allows a wide range of operations to be performed on remote files, acting somewhat like a remote file system protocol. All data is encrypted before being sent across the network.

The SFTP Storage Targets support Username/Password and Public Key Authentication methods.

For a general description of storage targets, please refer to [Storage and export targets](#).

Creating an SFTP target

Follow the steps below to create a new Verba Storage target for SFTP:

Step 1 - Open the Verba Web interface, then select **Policies > Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select SFTP
Path	This is the path where you want to store the media files.
Host Name or IP Address	Name or address of the SFTP server.
Port	The access port of the SFTP server.
Username/Password Authentication	
Login Name	User name of the SFTP user configured for Verba access in SFTP server.
Password	Password of the SFTP user configured for Verba access in SFTP server.
Public Key Authentication	

SFTP Public Key	Specify the certificate file/certificate thumbprint (a certificate stored in the Windows Certificate Store or PEM/PFX certificate file path)
SFTP Private Key	Specify the certificate file/certificate thumbprint (a certificate stored in the Windows Certificate Store or PEM/PFX certificate file path)
SFTP Private Key Password	Specify the password for the file that contains the certificate key
Export Target	When enabled, the storage target is available as an export target for all or specific users

Step 4 - Click **Save** to save the settings

Storage Target Configuration

[Add New Storage Target](#)
[Back to Previous Storage Target List](#)

?

▼ Storage Target Data

Name*

Type*

Path

Host Name or IP Address

Port

Login Name

Password

SFTP Public Key Authentication

SFTP Public Key

SFTP Private Key

SFTP Private Key Password

▼ Export Target

Export Target

Everyone Selected Users/Groups

[Save](#)

i When you change the folder of a storage target, it is always your responsibility to move the files in the file system, otherwise the conversations cannot be played back from the web interface.

* Indicates required item.

After this point, the storage target is available for use by other Verba components (e.g., [Data management policies](#)).

Verint WFO

Available in version 9.2 and later

This page provides a guide for configuring a Verint Storage Target in the Verba system.

To have access control over the media files in the Verint system first, you have to create the employee profiles in Verint. In case the media cannot be assigned to a Verint employee, then only superusers will be able to search and playback the calls using the **search outside visibility** checkbox. The Verba Storage Manager service also sends out e-mail alerts when the media could not be assigned to an employee.

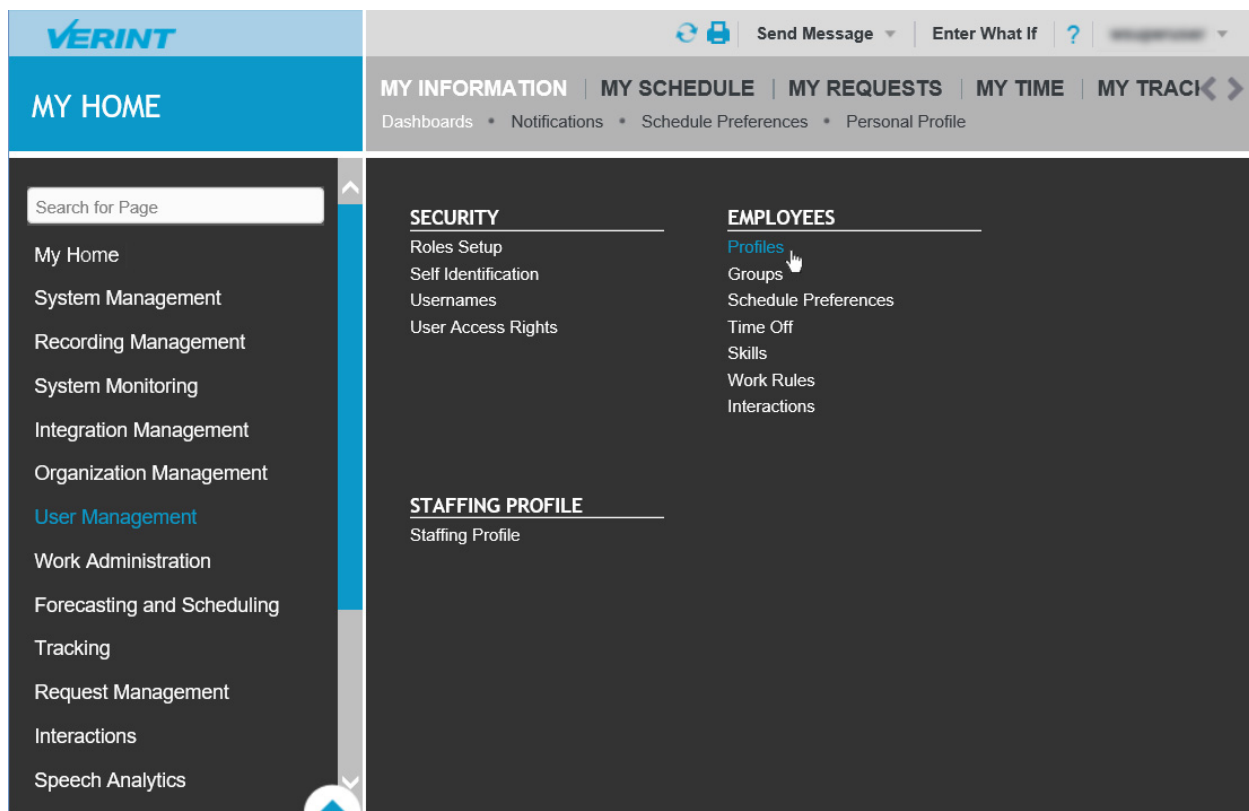
For a general description of storage targets, please refer to [Storage and export targets](#).

Creating an Employee in the Verint system

Follow the steps below to create a new Employee in the Verint system:

Step 1 - Open the Verint Web interface then click on the top left area to bring up the menu.

Step 2 - Select **User Management** then click on **Profiles**



Step 3 - Click on the **Create** button (

Create

)

Step 4 - The required fields are the **First Name**, **Last Name** and **Employee ID** for which you can enter multiple values (sip address, telephone number)

Step 4 - Click on the save button (

Save

).

Creating an API key in the Verint system

Follow the steps below to create a new API key in the Verint system:

Step 1 - Open the Verint Web interface then click on the top left area to bring up the menu.

Step 2 - Select **System Management** then click on **API Keys**

Step 3 - Click on the plus icon (




) on the top right edge of the view to add a new key.

Step 4 - In the popup window select **External** key type:

GENERATE KEY ? X

Key Type: Internal
 External

Description:

 A generated key is permanent. You cannot edit or delete the key.

Step 5 - Hit the generate button then copy the key to the clipboard by pressing the copy icon (



).

Creating a Verint storage target

Storage Target Configuration

[Add New Storage Target](#)
[Back to Previous Storage Target List](#)

?

▼ **Storage Target Data**

Name*

Type*

Verint application server url

Example url:
http(s)://verintappserver.contoso.com


Verint API key id

Verint API key secret

▼ **Export Target**

Export Target

Everyone Selected Users/Groups

 When you change the folder of a storage target, it is always your responsibility to move the files in the file system, otherwise the conversations cannot be played back from the web interface.

Creation Date: May 31, 2018 12:42:31 PM
Created By: Verba Administrator (Administrator)
Last Modification Date:
Last Modified By:
[View Change History](#)

* Indicates required item.

Follow the steps below to create a new Verba Storage target for Verint:

Step 1 - Open the Verba Web interface then select **Policies > Storage Targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name of the storage target. This name will identify this target across the system.
Type	Select Verint
Verint application server url	Address of the Verint application server in the following format: <i>http(s)://verintappserver.contoso.com</i>
Verint API key id	API key id for authentication.
Verint API key secret	API key value for authentication.

Step 4 - Click **Save** to save the settings

After this point, the storage target is available for use by other Verba components (e.g. [Data management policies](#)).

IBM Tivoli Storage Manager

This page provides a guide to configuring an IBM TSM storage as a Storage Target in Verba.

TSM is an alternative to the traditional optical "write once, read many" (WORM) data. The file retention policy can be managed on TSM side via Management Classes. TSM does not support direct CIFS/SMB access to the stored files, limiting some Verba functionalities, therefore we recommend to use it as a long term archive storage. The following features are not supported:

- Speech analytics
- Screen capture multiplexing
- In-place transcoding storage policies

For a general description of storage targets, please refer to [Storage and export targets](#).

Please refer to the official TSM guide to deploy and configure the TSM system.

Prerequisites

Verba uses the TSM Backup-Archive Client API and the related API runtime must be installed on all Verba servers accessing TSM (Media Repository/Combo, Recorder servers if media is directly to be uploaded to TSM). The latest client framework can be downloaded from here:

<ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/client/v7r1/Windows/x64/v713>

During installation, the x86 API component must be selected and installed

Configuring TSM client

Provision client node in TSM server

Via dsmadm you should create a new node for each Verba server that accesses the TSM server.

Use the following command: **register node [nodename] [password]**

Create a configuration file for TSM server

TSM client is configured via configuration files located under default path: c:\Program Files\Tivoli\TSM\config. When a TSM storage target is created in Verba then a configuration file must be referred based on which the server address, authentication credential.... is specified for the client.

Here is an example config file content:

file: dsm_sample_node.opt:

```
commmethod tcpip
TCPServeraddress 192.168.1.149
tcpport 1500
traceflags api
tracefile c:\tivoli.log
NODENAME SAMPLE
PASsword password
```

With this configuration Verba will connect to the 192.168.1.149:1500 server via TCP using the "SAMPLE" node with the "password" password (see client node provisioning section).

Creating a TSM target

Follow the steps below to create a new Verba Storage target for TSM:

Step 1 - Open the Verba Web interface then select **Policies > Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill in the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select Tivoli Storage Manager
File Space	Specify the filespace for the files. If filespace does not exists Verba tries to create it
Management class	Specify the Management Class to be applied to the files (determines retention time)
Configuration file path	Path of TSM client configuration related to current target
Retention Period	If Management Class forces data retention, then the number of days of the retention period***

*** Please note there is no possibility via the API to access management policy's retention config. To enforce proper retention management in Verba, the retention period configured with the management class must be explicitly configured.

Step 4 - Click **Save** to save the settings

▼ Storage Target Data

Name*	Tivoli
Type*	IBM Tivoli Storage Manager
File Space	VERBA
Management Class	STANDARD
Configuration File Path	c:\Program Files\Tivoli\TSM\config\tdsm_verba.opt
Retention Period (days)	

▼ Export Target

Export Target

Everyone Selected Users/Groups

iTernity iCAS

AVAILABLE IN VERSION 9.6.11 AND LATER

This page provides a guide for configuring an iTernity iCAS middleware as a Storage Target in the system.

iTernity Compliant Archive Software (iCAS) is an enterprise archive and data protection software that helps organizations store data flexibly and securely, and helps additionally to fulfill manifold regulatory requirements and internal corporate policies in information archiving. Built upon industry standards and Windows platforms and supporting various kinds of storage platforms (SAN, DAS, Object, Cloud), iCAS offers the adaptability today's IT departments need. iCAS is a flexible and cost-efficient Software-Defined Archiving solution for the long-term protection of critical enterprise data. iCAS acts as a middleware layer between data management applications (e.g. DMS /ECM systems, e-mail archiving, PACS, etc.) and hard disk-based or object storage systems. Archive data are protected from manipulation and deletion in Content Storage Containers (CSC) and can then be stored in an audit-proof manner on standard storage systems from any manufacturer. The patented CSC technology by iCAS facilitates enormous flexibility and integration into existing IT infrastructures. In doing so, iCAS facilitates WORM protection (Write Once Read Many) and the management of retention periods for the archive data. Additional options for data encryption and compression enable the highest security and efficient utilization of storage. iCAS operates as object-based storage software and creates content-based identifiers for the containers. The identifiers are created using SHA-512 hash values and make it possible to conduct an integrity check of the containers at any time.

For more information on iCAS, see <https://www.iternity.com/en/icas/>

The Verba system automatically applies the retention period on the files, using the iCAS file level retention feature, when the files are moved/uploaded to iCAS. The system uses the standard SMB protocol for file operations.

If you don't want to use the file level retention feature, you need to setup a standard network storage target pointing to iCAS, see [Network Storage](#).

For a general description of storage targets, please refer to [Storage and export targets](#).

Creating an iTernity iCAS target

Follow the steps below to create a new Verba storage target for iTernity iCAS:

Step 1 - Open the Verba Web interface then select **Data Management / Storage targets** from the top menu.

Step 2 - Click on **Add New Storage Target**

Step 3 - Fill out the configuration form according to the requirements in the following table.

Configuration item	Description
Name	Name your storage target. This name will identify this target across the system.
Type	Select iTernity iCAS
Path	Specify the path where the storage is accessible in the Windows file system (UNC path)

Step 4 - Click **Save** to save the settings

After this point, the Storage target is available for use by other Verba components (e.g. [Data retention policies](#)).

Using custom credentials for accessing file share

It is possible to use credentials other than the service user for each iTernity iCAS storage. If you want to use custom credentials, check the " **Use custom credentials for accessing the file share**" checkbox, then provide the credentials.

Data processors

Data processors represent integrations with external data processing solutions such as transcription engines/providers. In order to use a data processing policy which requires an external processor, a data processor entry has to be created. Data processing policies using the built-in functionality of the system (such as voice quality check, speech indexing, encryption, etc.) does not require data processor setup.

Available data processors:

Find and list data processors

Select the **Data / Data Processors** menu item. You can use the search form below the title to filter for data processors: just select your filter and click **Find**.

Creating a data processor

You can create a new data processor by clicking on the **Add Data Processor** link on the **Data / Data Processors** page.

Follow the data processor specific instructions to create a new data processor.

Modifying and deleting data processors

To edit a data processor entry, you have to click on the desired row of the list showing data processors. After clicking on the row, a new page opens automatically.

To make changes effective, press the **Save** button.

You can delete the data processor by clicking on the **Delete** button. Make sure there is no data processing policy using the processor.

Import sources

Import sources define the connection parameters and configuration of the data source for import. The system supports the following import sources:

- [Generic Import Source](#)
- [Verba Conversation Import](#)
- [Cloud9 Recording System API](#)
- [Cloud9 Call Data API](#)
- [Zoom Meeting and Phone](#)
- [IPC Data Exchange](#)
- [Symphony Instant Messages - Files - CDRs](#)
- [Cisco Webex Teams](#)
- [Bloomberg Instant Messages](#)
- [RingCentral](#)
- [Vodafone](#)
- [O2](#)
- [TeleMessage](#)
- [Verint](#)
- [Verba Import API](#)

- [Lync/SfB CDR](#)
- [Cisco IPT CDR](#)
- [Lync/SfB Archive](#)

Find and list import sources

In the Verba menu, navigate to the **Data > Import Sources** page. The search form below the title can be used to filter import sources.

Creating an import source

A new import source can be created by clicking on the **Add New Import Source** link at the top-right corner of the **Data > Import Sources** page.

The layout of the interface to create the new import source is determined by the technology that will be used. Please refer to the individual technology guides for instructions on how to configure them.

After completing the configuration, click on **Save**. After this point, the import source will be available for use by data management policies.

Modifying and deleting import sources

To edit an import source entry, click on the desired row of the list showing registered import sources. After clicking on the row, a new page opens automatically.

To apply the changes, press the **Save** button.

The import source can be deleted by clicking on the **Delete** button.

Import Source Configuration

[Add New Import Source](#)
[Back to Previous Page](#)

▼ Import Source

Name *

Type *

▼ Settings

Database Hostname

Database Name

Database QoE Name

Database Login

Database Password

Failover Partner

Database Multi-Subnet Failover

Windows Authentication

SSL Encryption

Import Not Established Conversations

Lync Version

Use QoE Metrics

Import Conference Participants

Generic Import Source

This page provides a guide to configuring a Generic Import Source in Verba.

Verba's capabilities are now further expanded by the Generic Import functionality: import any supported media - with CDR contained in .csv, .xml, or .json files - exported from your existing recordings directly to the Verba Platform. This feature enables you to import the files yourself or to significantly decrease handle time. The list of supported media formats can be found in the following article: [Storage requirements](#)


- [Creating a generic import source](#)
- [Import / Export](#)
- [Configuring CDR field mapping](#)
 - [Mandatory fields](#)
 - [Recommended fields](#)
 - [Expression types](#)
 - [Constant](#)
 - [Field](#)
 - [CSV](#)
 - [JSON](#)
 - [XML](#)
 - [Function](#)

For a general description of Verba Import sources, please refer to [Import sources](#).

For a general description of Data Import action, please refer to [Data Import policy](#).

The Generic Import function can import **240K records a day**.

 For non-real time import, the Enable Recording Rules option should be unchecked in the Data Import configuration.

 **Internal Article**
Previously created configurations
[Exported configurations for Generic Import](#)

Creating a generic import source

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
--------------------	-------------

Name	Name your import source. This name will identify this source across the system
Type	Select Generic
Source Files Type	CSV JSON XML
CSV Separator	the delimiter character
Source Files Folder	Path to the files. Local storage or NAS is supported.
Custom cred	Field for credentials if the NAS requires it.
On Completion	Select the action taken for the successfully imported files.
Timezone	Timezone of the conversations in the file
Stop words	The list of possible denotations of empty value

Source Files Types CSV JSON XML

CSV Separator

Source Files Folder *

Custom Credential

User Login Name

Password

On Completion Delete Files Move Files

Timezone

Greenwich Mean Time
12:34:03

Stop Words

These listed values will be handled as an empty value.

Step 4 - Click **Save** to save the settings

Import / Export


All settings can be imported from, or exported to a JSON format, except the custom credential information.

After pressing the export configuration button the current configuration's JSON file will be available to copy to the clipboard. This configuration can be pasted into a different Verba instance, using the import configuration button.

Export an import source configuration

 The export won't contains the custom credentials.

```
{
  "settings": {
    "setting_source_file_type": "csv",
    "setting_csv_separator": ";",
    "setting_folder": "\\10.4.0.10\\Folder\\",
    "setting_user_custom_credentials": "1",
    "setting_on_completion": "delete",
    "setting_timezone": "GMT",
    "setting_stop_words": "[]",
    "fieldMappings": [
      {
        "expression": null,
        "cdrFieldId": "start_time",
        "cdrParentFieldId": null,
        "childFieldMappings": [
          {
            "settings": {
              "time_format": "yyyy.MM.dd HH:mm."
            }
          }
        ]
      },
      {
        "expression": null,
        "cdrFieldId": "end_time",
        "cdrParentFieldId": null,
        "childFieldMappings": [
          {
            "settings": {
              "time_format": "yyyy.MM.dd HH:mm."
            }
          }
        ]
      },
      {
        "expression": null,
        "cdrFieldId": "duration",
        "cdrParentFieldId": null,
        "childFieldMappings": [
          {
            "settings": {}
          }
        ]
      }
    ]
  }
}
```

 Copy to clipboard

Close

Configuring CDR field mapping

Start Time *

Time format*

End Time *

Time format*

Duration Interval *

Mandatory fields

These three pre-defined CDR fields are **mandatory** in the Verba recording system. It is possible that one of the fields is not specified in the import source, the system will accept any of the two out of the three, and calculate the third one. The Start Time and End Time fields can be configured for the format in the source, for the required time format, please refer to [Generic Import Time/Date patterns](#). The Duration Interval is expected in seconds.

The full list of valid field can be found at [Generic Import CDR fields](#).

Recommended fields

There are two more fields that aren't mandatory, but are highly recommended that at least one of the is set properly for each entry: Recorded Extension or Recorded Party. These fields signal the import source that for each entry in the import files signals which participant should the record be associated to.

For example take a voice type entry with the following fields:

StartTime, EndTime, path, SourceID, DestinationID, Direction, Modality

and this example CSV, where both extension 422 and 433 are set up to be recorded:

2015.11.23.10:23:11.432,2015.11.23.10:25:23.665,"D:/some_path/media.file",422,433,1,"voice"

Will be saying to the Generic Import source that 422 is calling 433 and the entry has Direction 1 which is PSTN In, meaning that the recording was made from the perspective of 433. All well and good, but this entry will produce

2 CDR entries, because it can't tell that for this single line for which side should the entry be created for, thus it will fall back to creating a CDR record for both 422 and 433.

This is more than likely not what is intended as most systems would make a recording entry for both sides of the communication like so:

2015.11.23.10:23:11.432,2015.11.23.10:25:23.665,"D:/some_path/**media_for_433**.file",422,433,**1**,"voice" (Direction PSTN In)

2015.11.23.10:23:11.432,2015.11.23.10:25:23.665,"D:/some_path/**media_for_422**.file",422,433,**2**,"voice" (Direction PSTN Out)

In this scenario with the above configuration import source will fall back on making a CDR record for both entries in essence duplicating the number of entries. Making 4 instead of the expected 2.

This is why it is recommended to include the Recorded Extension or Recorded Party in each individual entry like so:

StartTime, EndTime, path, SourceID, DestinationID, Direction, Modality, Recorded Extension

2015.11.23.10:23:11.432,2015.11.23.10:25:23.665,"D:/some_path/media_for_433.file",422,433,1,"voice",433

2015.11.23.10:23:11.432,2015.11.23.10:25:23.665,"D:/some_path/media_for_422.file",422,433,2,"voice",422

This will produce the expected two records for the two entries, properly associating the unique recording file to the appropriate CDR entry.

Expression types

Constant

The constant expression type can be either a pre-defined value or an editable textbox depending on the Field.

Position of the expression Direction

Description for the CDR field The direction of the call

Expression Type Constant

Constant Value --Choose value--
--Choose value--
Internal
PSTN In

Position of the expression Location


Description for the CDR field The hostname of the server that recorded the conversation

Expression Type Constant ▼

Constant Value testserver1.verba.local

Field

The field expression type is a pointer for a value in the source file. As the supported source file types have different structures, the setup for them differs slightly.

 The import service is case sensitive for the fields.

CSV

Position of the expression Recorded Party

Expression Type Field ▼

Field Path Please, set the name of the column from the CSV file.

USRID

Delete expression

For a CSV source file, the name of the column needs to be specified. Using the Column and the number of the call in the list the value can unambiguously defined

JSON

Position of the expression Recorded Party

Expression Type

Field Path Please, set the absolute path of the field in your file structure from the root element.

Root element

Child element

Index in array
JSON array indices starts with 0.

Child element

Delete expression

For a JSON source file, the required property names and array indexes need to be chained together. ["Extensions"] [1] ["Office"]

The specification used is ECMA-404

XML

Position of the expression Recorded Party

Expression Type

Field Path Please, set the absolute path of the field in your file structure from the root element.

Root element

Child element

Index in array

Child element

Delete expression

For an XML source file, the required property names and array indexes need to be chained together. The Attribute values can be referred to as well.

```
//Extensions/List[1] /Office
```

The specification used is XML 1.0 3rd edition

Function

The function expression type is a collection of tools for transforming the source data if needed, and combining fields if one to one mapping is not possible.

The full list of valid Functions can be found at [Generic Import functions](#)

Generic Import CDR fields

This article describes the supported CDR fields in the [Generic Import Source](#).

CDR field	Description	Expected data
Meeting ID	Technical identifier for the conference	freetext
Meeting URI	Web link to join the meeting	freetext
End Cause	The end cause of the conversation	0 - Normal 1 - From Terminated 2 - To Terminated 3 - Hold 4 - Transfer 5 - Caller gave up 6 - Busy 7 - Unobtainable 8 - Error 13 - Conference 14 - Call park 15 - Join 28 - Direct Transfer 60 - Line change 80 - Timeout 81 - Forced termination 82 - Manual termination 83 - Program termination 84 - Video escalation 85 - Voice Inactivity 86 - Media Segmentation 87 - Team 90 - Blocked 500 - Unknown
Media Length	The length of the media file	Call length in seconds
Direction	The direction of the call	0 - Internal 1 - PSTN In 2 - PSTN Out 3 - Inter-Tenant 4 - Undefined 6 - External 10 - Federated In 11 - Federated Out 12 - Contact Center In 13 - Contact Center Out 14 - Conference
Modality	The type of conversation	voice - Voice im - Instant Messaging video - Video screen - Desktop Screen share - Screen & Application Share whiteboard - Whiteboard poll - Poll / Q&A file_share - File Share sms - SMS

Media File Location	The full path to the media file	freetext
Recorded Extension	The extension being recorded in the conversation	freetext
Recorded Party	The user being recorded in the conversation	freetext
Platform Call ID	Correlation ID based on which same call legs belonging to the same call flow can be correlated	freetext
Native Call ID	Unique Conversation ID assigned by the telephony platform	freetext
Secondary	primary or secondary (using 2N / duplicate recording)	0 - Primary 1 - Secondary 2 - Unset
Location	The hostname of the server that recorded the conversation	freetext
Codec	The codec used by the communication platform	1 - Nonstandard 2 - G.711 A-law 64k 3 - G.711 A-law 56k 4 - G.711 u-law 64k 5 - G.711 u-law 56k 6 - G.722 64k 7 - G.722 56k 8 - G.722 48k 9 - G.723.1 10 - G.728 11 - G.729 12 - G.729A 13 - IS11172AudioCap 14 - IS13818AudioCap 15 - G.729B 16 - G.729AwB 18 - GSM FR 19 - GSM HR 20 - GSM EFR 25 - Wideband 256k 32 - Data 64k 33 - Data 56k 80 - GSM 81 - ActiveVoice 82 - G.726 32k 83 - G.726 24k 84 - G.726 16k 90 - iLBC 20ms 91 - iLBC 30ms 92 - iSAC 93 - G.722.1(c) 94 - AAC - Low Complexity 95 - Microsoft RTAudio 96 - MPEG4-Generic 97 - MP4A-LATM 98 - Siren 99 - Speex 100 - L8 101 - G.726 40k 102 - Silk 103 - Celt 104 - DVI4 105 - VOX

		106 - OPUS 200 - H.261 201 - H.263 202 - H.263+ 203 - H.263++ 204 - H.264 AVC 205 - H.264 RCDO 206 - H.264 SVC 207 - Microsoft RT Video 208 - Microsoft RDP 209 - VP8 210 - VP9 299 - No Video 300 - TechSmith 301 - Windows Media 8 768 Kbps 302 - Windows Media 8 1024 Kbps 303 - Windows Media 8 1512 Kbps 304 - Windows Media 8 2048 Kbps 305 - Windows Media 9 768 Kbps 306 - Windows Media 9 1024 Kbps 307 - Windows Media 9 1512 Kbps 308 - Windows Media 9 2048 Kbps 309 - Windows Media Screen 768 Kbps 310 - Windows Media Screen 1024 Kbps 311 - Windows Media Screen 1512 Kbps 312 - Windows Media Screen 2048 Kb 313 - Verba Screen Codec Lossless 314 - Verba Screen Codec HQ 315 - Verba Screen Codec LQ 316 - Verba Screen Codec LQ - Monochrome 400 - No Screen 500 - Undefined
Source Caller ID	Extension for the caller party	freetext
Destination Caller ID	Extension for the called party	freetext
Source Caller Name	The display name of the caller party	freetext
Destination Caller Name	The display name of the called party	freetext
User ID	The User ID obtained from the communication platform as extra metadata	freetext

Generic Import functions

This article describes the supported functions fields in the [Generic Import Source](#).

Function Type	Function description	Return value	Value type
Absolute	Calculates the absolute value of the input number.	Absolute (A)= A	string
Add	Adds two numbers.	Add (A,B) = A+B	string
And	Returns TRUE if all of the arguments evaluate to TRUE.	AND(True,True)= True	boolean
Concat	Concatenates the argument values into one text and returns with it.	concat(A,B, C) = ABC	string
Divide	Returns with the divided value of two numbers (A / B).	Divide (A,B) = A/B	string
Equal	Checks equality between two values (A = B)). Returns with a boolean result.	1 if true, 0 if false	boolean
Exists	Checks if a field exists in the input metadata. Returns TRUE if the field can be found/resolved and the value is not empty. FALSE otherwise.	1 if true, 0 if false	boolean
Greater	Checks if the first parameter is greater than the second one (A > B). Returns with a boolean result.	1 if true, 0 if false	boolean
Greater or equal	Checks if the first parameter is greater or equal to the second one (A >= B). Returns with a boolean result.	1 if true, 0 if false	boolean
If	Based on the first logical parameter returns with the second or third parameter. If the logical value is TRUE then returns with the first parameter, otherwise with the second parameter.	if(condition, A, B) = A if true, B if false	string
Less	Checks if the first parameter is less than the second one (A < B). Returns with a boolean result.	1 if true, 0 if false	boolean
Less or equal	Checks if the first parameter is less or equal to the second one (A <= B). Returns with a boolean result.	1 if true, 0 if false	boolean
Mapping	Based on the first parameter value it finds a "Dictionary" key parameter in the given list and returns with its value.	Map(1, 1 ->odd, 2->even) = odd	string
Multiply	Returns with the multiplied value of two numbers (A * B).	Multiply (A,B) = A*B	string
Or	Returns TRUE if any argument evaluates to TRUE.	Or(True, False) = True	boolean
Regex	In the first parameter value run a regex search pattern from the second parameter. The first group match will be the output	regex(1234, \d{2}) = 12	string
Replace	In the first parameter, it searches a string from the second parameter and replaces it with the third parameter.	replace(input,in, out) = output	string
Substring	Returns the portion of the string from the first parameter specified by the start and length parameters from the second and the third parameter.	substring(input data, 2,3)= put	string
Subtract	Subtracts the second number from the first number.	Subtract(A,B)=A-B	string

Generic Import Time/Date patterns

This article describes the valid time/date patterns in the [Generic Import Source](#).

The time pattern must follow the required format of `%[primitive][separator]`

Examples

Source string	Time pattern
1999-12-31 23:12:01.118	<code>%yyyy-%MM-%dd %HH:%mm:%ss.%fff</code>
december 31 99	<code>%MMMM %dd %yy</code>
january 21 05 Saturday	<code>%MMMM %dd %yy %dddd</code>
11:12:31 PM	<code>%hh:%mm:%ss %tt</code>
1548236960	<code>%epochS</code>

Primitives

Primitive	Description	Examples
dddd	The full name of the day of the week	Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday
ddd	The abbreviated name of the day of the week	Sun,Mon,Tue,Wed,Thu,Fri,Sat
dd	The day of the month. Single-digit days will have a leading zero	
d	The day of the month. Single-digit days will not have a leading zero	
MMMM	The full name of the month	January,February,March,April,May,June,July,August,September,October,November,December
MMM	The abbreviated name of the month	Jan,Feb,Mar,Apr,May,Jun,Jul,Aug,Sep,Oct,Nov,Dec
MM	The numeric month. Single-digit months will have a leading zero	
M	The numeric month. Single-digit months will not have a leading zero	
yyyy	The year in four digits, including the century	
yy	The year without the century. The year is displayed with a leading zero	
y	The year without the century. The year is displayed without a leading zero	

hh	The hour in a 12-hour clock. Single-digit hours will have a leading zero	
h	The hour in a 12-hour clock. Single-digit hours will not have a leading zero	
HH	The hour in a 24-hour clock. Single-digit hours will have a leading zero	
H	The hour in a 24-hour clock. Single-digit hours will not have a leading zero	
mm	The minute. Single-digit minutes will have a leading zero	
m	The minute. Single-digit minutes will not have a leading zero	
ss	The second. Single-digit seconds will have a leading zero	
s	The second. Single-digit seconds will not have a leading zero	
fff	The fraction of a second in three-digit precision. The remaining digits are truncated.	
ff	The fraction of a second in double-digit precision. The remaining digits are truncated.	
f	The fraction of a second in single-digit precision. The remaining digits are truncated	
tt	The AM/PM designator	
t	The first character in the AM/PM designator	
zzz	The full time zone offset ("+" or "-" followed by the hour and minutes). Single-digit hours and minutes will have leading zeros.	Pacific Standard Time is "-08:00"
zz	The time zone offset ("+" or "-" followed by the hour only). Single-digit hours will have a leading zero. For example, Pacific Standard Time is "-08"	Pacific Standard Time is "-08:00"
epochS	Expects seconds counted from January 1, 1970 (midnight UTC /GMT), not counting leap seconds (in ISO 8601: 1970-01-01T00:00:00Z).	
epochMs	Expects milliseconds counted from January 1, 1970 (midnight UTC/GMT), not counting leap seconds (in ISO 8601: 1970-01-01T00:00:00Z).	

Verba Conversation Import

The Conversation Import scans a given **local or remote folder hierarchy** for formerly exported calls with a **valid Verba XML conversation detail record (CDR) file**. Conversations without valid XML CDR files are discarded.

Verba Conversation Import Sizing

The Verba conversation import policy can process **14 calls every second** on average. However, this is highly dependent on the file sizes and the network bandwidth.

If the network bandwidth is not holding back the import capacity, it takes up **0.2 CPU core** of the server where the Import service runs.

On the SQL server side, the policy takes up **0.3 CPU core**. It generates **75 IOPS with 0.7% R/W ratio**. If the recording rules setting is turned off, it takes up 0.25 CPU core.

Creating a Verba Import source

Follow the steps below to create a new Verba Import source for Verba conversation data:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select Verba
Source folder	Specify the network path to the shared folder where the Verba conversations are available for import. The original Year / Month / Day folder structure is required.

Step 4 - Click **Save** to save the settings

Import Source Configuration

[Add New Import Source](#)
[Back to Previous Page](#)


▼ Import Source

Name *

Type *

▼ Settings

Source Folder

 Please note that the content of the Source Folder will be deleted after the successful import. Therefore, the Source Folder cannot match any of the Verba storage targets or the media folders! It is highly recommended to create a temporary folder for the calls which has to be imported.

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**


Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

 Please note that the policy is executed by the **Verba Import Service**. To start the import, the activation and start of that service is required.

Enabling data import policy execution on servers

Step 1 - Login to the web interface with **System administrator** rights.

Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

Step 3 - Go to the **Service Activation** tab, then activate the **Verba Import Service** by clicking on the




icon.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 7 - Click on the **Service Control** tab.

Step 8 - Start the **Verba Import Service** by clicking on the



icon.

Cloud9 Recording System API

For general Cloud9 recording information see [Cloud9](#).


For a general description of Import sources, please refer to [Import sources](#).


Configuring Cloud9 Recording System API based recording and archiving

In order to archive the calls in the system, please make sure that **Local** or **Cloud and Local** is selected.

Set the **Voice Recording** to **Yes**, and provide the URI in "[http://verbaserver:port](#)" format.

User Settings

Product Type:  C9 Trader Enterprise

Voice Recording:  Yes No Not Answered

Recording Storage: Local

Enhanced Metadata:

URI:

Please make sure that the **Enhanced Metadata** checkbox is checked.

For more information, see https://cloud9technologies.desk.com/customer/en/portal/articles/2729473-onsite-call-archive-options?b_id=15792

Enabling the Verba Import Service

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Media Repository (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Import Service** by clicking on the



icon.

Step 3 - Click on the **Service Control** tab.

Step 4 - Start the **Verba Import Service** by clicking on the



icon.

Creating a Cloud9 import source

Follow the steps below to create a new Verba Import source for Cloud9:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system.
Type	Select Cloud9 Recording System API

HTTP Port	HTTP Port, where the Verba C9 import service is listening
HTTPS Port	HTTPS Port, where the Verba C9 import service is listening
TLS Certificate File / Thumbprint	Specify the certificatefile/certificatethumbprint that is being used for the Cloud9 connection. If left empty then the Verba default certificate will be used
TLS Key File	Specify the file where the certificate key is stored if not in the windows certificate store
TLS Key File Password	Specify the password for the file that contains the certificate keys
TLS Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: <ul style="list-style-type: none"> • .pem file with a list of certificates • comma separated certificate thumbprints • comma separated CA thumbprints

Step 4 - Click **Save** to save the settings

(Optional) Transcoding configuration

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Media Repository (or Single) Server > Click on the Change Configuration Settings** tab.

Step 2 - Expand the **Import \ Cloud9** node.

Step 3 - Select the codec at the **Audio Transcoder Profile** setting.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Extension configuration

To match the imported conversations to a Verba extension (and to a Verba User account) you need to add the Cloud9 login names to Verba as **extensions** with type "**User / Agent ID**".

Load balancer configuration

AVAILABLE SINCE 9.7.4

Load balancer health probe configuration must be HTTP GET with path = '/healthprobe'. The system will return a HTTP 200 OK when it is healthy and can receive new requests.

Cloud9 Call Data API

AVAILABLE IN VERSION 9.0 AND 9.5 OR LATER

For general Cloud9 recording information see [Cloud9](#).

For a general description of Import sources, please refer to [Import sources](#).


Configuring Cloud9 Call Data API based recording and archiving

Creating an API Key in the Cloud9 Portal

Step 1 - Login to the [Cloud9 Portal](#)

Step 2 - Navigate to the API Keys page (if not available then ask your Cloud9 contact to enable this feature)

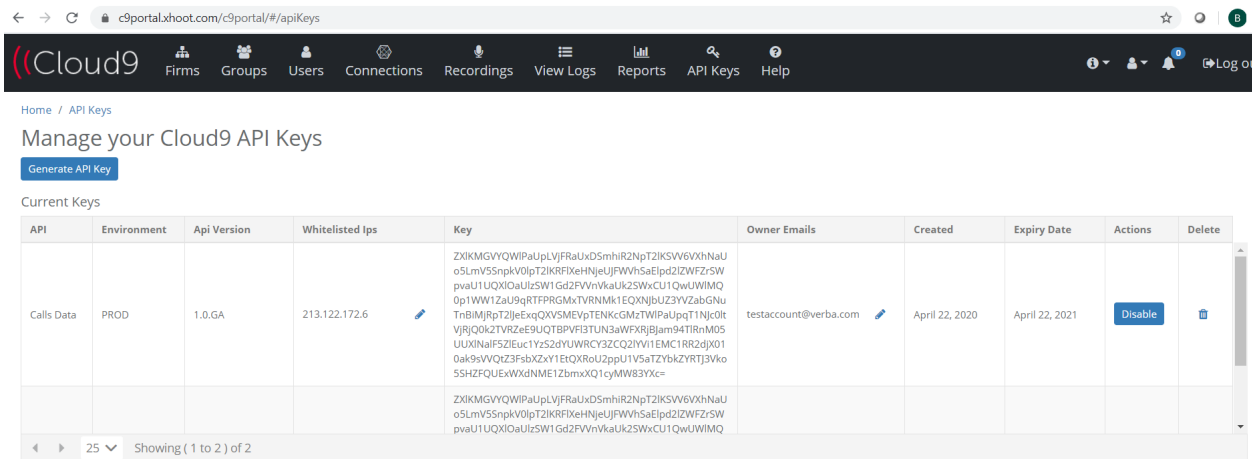
Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
API	Calls Data
Environment	Select your environment
Whitelisted IP(s)	A comma separated list of IP addresses of the Verba Recording Servers (public IP) where the Import Source will run <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> If the Recorder Server's public IP is not on this list then we will get 403 Unauthorized responses for our requests and we won't be able to record/archive calls</p></div>
Owner Email(s)	Comma separated list of emails

Generate New API Key ✕

API*	Environment*	Whitelisted IP(s)*	Owner Email(s)*
Calls Data ▾	PROD - 1.0... ▾	10.110.78.56	testaccount@verba.com
		Comma separated. CIDR notation accepted	Comma separated
			Cancel Generate Key & Secret

Step 4 - Please note your API Secret because later on you won't be able to copy it out.



Enabling the Verba Import Service

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server from the list where you want to enable the Import Service which will integrate with the Cloud9 API. The Import Service can be enabled on the following Server roles: Recording Server, Media Repository, Media Repository and Recording Server

Step 3 - Activate the **Verba Import Service** by clicking on the



icon.

Step 4 - Click on the **Service Control** tab.

Step 5 - Start the **Verba Import Service** by clicking on the



icon.

Creating a Cloud9 import source

Follow the steps below to create a new Verba Import source for Cloud9 Call Data API:

Step 1 - Open the Verba Web interface then select **Data \ Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system.
Type	Select Cloud9
API Key	The API Key you created on the Cloud9 Portal .
API Secret	The API Secret you created on the Cloud9 Portal .
TLS Certificate File / Thumbprint	Specify the certificate file / certificate thumbprint that is being used for the Cloud9 connection. If left empty then the Verba default certificate will be used.

TLS Key File	Specify the file where the certificate key is stored if not in the windows certificate store
TLS Key File Password	Specify the password for the file that contains the certificate keys
TLS Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: pem file with a list of certificates comma separated certificate thumbprints comma separated CA thumbprints
Forward Proxy Address	IP address or FQDN of the forward proxy. When defined, the system will connect through a forward proxy.
Forward Proxy Port	The port of the forward proxy
Forward Proxy Username	Username for basic authentication for the forward proxy server
Forward Proxy Password	Password for basic authentication for the forward proxy server

Step 4 - Click **Save** to save the settings

▼ Import Source

ID *

Name *

Type *

▼ Settings

API Key

API Secret

TLS Certificate File / Thumbprint

TLS Key File

TLS Key Password

TLS Trust List

Forward Proxy Address

Forward Proxy Port

Forward Proxy Username

Forward Proxy Password

Transcoder Configuration (Optional)

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server from the list where you have the Import Service enabled for the Cloud9 API.

Step 3 - Expand the **CDR and Archived Content Importer \ Cloud9 Call Data API** node.

Step 4 - Select the codec at the **Audio Transcoder Profile** setting.

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

⚠ There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please click here .

Other Configuration (Optional)

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server from the list where you have the Import Service enabled for the Cloud9 API.

Step 3 - Expand the **CDR and Archived Content Importer \ Cloud9 Call Data API** node.

<ul style="list-style-type: none"> ▾ CDR and Archived Content Importer <ul style="list-style-type: none"> ▶ General ▶ CDR Import ▶ Archive Import ▶ Cloud9 Recording System API ▾ Cloud9 Call Data API 	
Audio Transcoder Profile:	<input checked="" type="checkbox"/> Speex (CELP) in Ogg with silence suppression ▼
Maximum Query Page Size:	<input checked="" type="checkbox"/> 500
Query Interval [seconds]:	<input checked="" type="checkbox"/> 600
Database Cache Folder:	<input checked="" type="checkbox"/>
Cloud9 Call Data API URL:	<input checked="" type="checkbox"/> https://calldataapi.xhoot.com:443
Cloud9 Call Data API Metadata Endpoint:	<input checked="" type="checkbox"/> /v1/calls/metadata
Cloud9 Call Data API Recordings Endpoint:	<input checked="" type="checkbox"/> /v1/calls/recordings
Delete Metadata from Local Cache After [hours]:	<input checked="" type="checkbox"/> 72
Delete Media from Local Cache After [hours]:	<input checked="" type="checkbox"/> 72
Initial Query Look Back [days]:	<input checked="" type="checkbox"/> 14

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data \ Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Extension configuration

To match the imported conversations to a Verba extension (and to a Verba User account) you need to add the Cloud9 login names as **extensions** with type **User / Agent ID**.

Zoom Meeting and Phone

AVAILABLE IN VERSION 9.6.13 OR LATER

- [Configure Zoom compliance archiving](#)
 - [Enable and configure compliance recording for Zoom users](#)
 - [Create a Zoom application](#)
 - [JWT app \(to be deprecated by Zoom on June, 2023\)](#)
 - [Server-to-server OAuth 2.0 app](#)
- [Configure Zoom import](#)
 - [Enabling the Verba Import Service](#)
 - [Creating a Zoom Meeting or Zoom Phone import source](#)
 - [Creating an import policy](#)
 - [Adding users for archiving](#)
 - [Changing the Zoom import specific settings for the Import Service](#)

Zoom Meeting and Phone recordings can be archived into the system, using the import service framework.

For general information about Zoom recording and archiving, see [Zoom](#).

Configure Zoom compliance archiving

Enable and configure compliance recording for Zoom users

Refer to the Zoom documentation to enable and configure meeting and phone call archiving.

For more information on meeting archiving setup, see <https://support.zoom.us/hc/en-us/articles/4405656451213>

Create a Zoom application

In order to allow access to the Zoom APIs, an application has to be created on the Zoom portal. The system is integrated using either the JWT based or the Server-to-server OAuth 2.0 based authentication option which is suitable for the server-to-server type of integrations.

JWT app (to be deprecated by Zoom on June, 2023)

For information on creating a JWT application, refer to <https://marketplace.zoom.us/docs/guides/build/jwt-app>.

Make a note of the API Key and API Secret settings created during the process, because these will be required for the import source configuration.



Verint Financial Compliance

Intent to publish: No Account-level app JWT credentials

App credentials

Information

App credentials

Feature

Activation

API Key

[Redacted API Key] Copy

API Secret

[Redacted API Secret] Copy Regenerate

IM Chat History Token

[Redacted IM Chat History Token] Regenerate

View JWT Token ▾

< Back

Continue

Server-to-server OAuth 2.0 app

AVAILABLE IN VERSION 9.7.7 OR LATER

For information on creating a Server-to-server OAuth 2.0 app, refer to <https://marketplace.zoom.us/docs/guides/build/server-to-server-oauth-app/>

The created application should have the following roles:

- recording:read:admin
- dashboard_meetings:read:admin
- dashboard_webinars:read:admin
- phone:read:admin
- phone_call_log:read:admin
- phone_recording:read:admin

(As of October, 2022, a know bug in Zoom APIs invalidates every Server-to-server OAuth tokens upon requesting a new one, so a single OAuth app can ONLY be used by one server. If you plan to use multiple servers, create an app for each of them!)

Make a note of the Account ID, Client ID, Client secret of your app, because these will be required for the import source configuration.



Verba Server-to-Server OAuth

Intend to publish: No Account-level app Server-To-Server OAuth

App Credentials

- Information
- Feature
- Scopes
- Activation

App credentials

Below credential allows you to generate a token that is utilized by Zoom OAuth, providing you access to Zoom APIs.

Account ID

G2 [REDACTED] Copy

Client ID

I8 [REDACTED] Copy

Client secret

[REDACTED] Copy Regenerate

[Back](#)

✓ Saved

[Continue](#)

Configure Zoom import

The configuration includes the following steps:

- Enabling the Import Service on a server (if not enabled before)
- Creating a Zoom Meeting and/or Zoom Phone import source(s)
- Creating the corresponding import policies where CDR reconciliation can be optionally enabled
- Adding users and recorded extensions for Zoom users
- Optionally change the Zoom specific settings for the Import Service

The system includes 2 separate import sources for Zoom:

- Zoom Meeting: imports Zoom Meeting archives and optionally reconciles Zoom meeting logs with recordings
- Zoom Phone: imports Zoom Phone archives and optionally reconciles Zoom call logs with recordings

If you want to archive both Zoom Meeting and Zoom Phone, both import sources have to be configured separately.

It is not recommended to enable the import source on more than 1 server because the 2 servers will separately query the same data using the Zoom APIs. The system will eventually import only one copy of the same call and meeting, but the API usage will be doubled.

Enabling the Verba Import Service

Step 1 - In the Verba Web Interface go to **System \ Servers**

Step 2 - Select the server from the list where you want to enable the Import Service which will integrate with the Zoom APIs. The Import Service can be enabled on the following Server roles: Recording Server, Media Repository, Media Repository and Recording Server.

Step 3 - Activate the **Verba Import Service** by clicking on the



icon.

Step 4 - Click on the **Service Control** tab.

Step 5 - Start the **Verba Import Service** by clicking on the



icon.

Creating a Zoom Meeting or Zoom Phone import source

Follow the steps below to create a new Verba Import source for Zoom:

Step 1 - Open the Verba Web interface then select **Data / Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table:

Name	Description
API Key	The Zoom API key associated with the Zoom application registered earlier
API Secret	The Zoom API secret associated with your Zoom application registered earlier
Forward Proxy Address	IP of the forward proxy server. If left empty, no attempt is made for establishing a forward proxy connection.
Forward Proxy Port	Port for the forward proxy connection.
Forward Proxy User	Username for authenticating with the Forward Proxy. If left empty, authentication is omitted.
Forward Proxy Password	Password for authenticating with the Forward Proxy.
API Address	The base URL of the Zoom API
TLS Certificate File / Thumbprint	Specify the certificate file / certificate thumbprint that is being used for the Zoom API connection. If left empty then the Verba default certificate will be used.
TLS Key File	Specify the file where the certificate key is stored if not in the windows certificate store.
TLS Key Password	Specify the password for the file that contains the certificate keys.
TLS Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: <ul style="list-style-type: none">• .pem file with a list of certificates• comma separated certificate thumbprints• comma separated CA thumbprints

Step 4 - Click **Save** to save the settings

Creating an import policy

Once the import sources are created, a new import policy has to be created. For more information, refer to [Data Import policy](#).

Optionally, CDR reconciliation can be enabled in the policy. For more information, see [CDR reconciliation](#).

Adding users for archiving

In order to enable Zoom archiving create the [users](#) and the [extensions](#) on the Verba side. This can also be done via [Active Directory Synchronization](#).

- Zoom Phone: to control which user recordings have to be downloaded and archived, and to match the imported conversations to an extension (and to a user account) you need to add the Zoom user phone extension numbers (not the Zoom user ID) as **extensions** with type **User / Agent ID**.
- Zoom Meeting: to control which user recordings have to be downloaded and archived, and to match the imported conversations to an extension (and to a user account) you need to add the Zoom user ID as **extensions** with type **User / Agent ID**.

Changing the Zoom import specific settings for the Import Service

To change the server/service level settings from the Zoom integration, follow the steps below:

Step 1 - In the Verba Web Interface go to **System / Servers**

Step 2 - Select the server from the list where you have the Import Service enabled for the Zoom integration.

Step 3 - Expand the **Import / Zoom Phone** or **Import / Zoom Meeting** node.

Step 4 - Change the settings based on the description below:

Name	Description
Give Up Timeout In Minutes	The number of minutes before finally abandoning a repeatedly failing import. Default value: 10080 → a week
Maximum Number Of Entries To Import	The maximum number of meetings/phone calls to try and import from the Zoom API before throttling them in one import cycle. This will limit the maximal memory usage of the Import Source. This is not a hard limit, as sometimes to preserve the integrity of the imported data the application has to overstep it. If this has to happen it will be only done to the degree it is absolutely necessary.
Maximum Page Size	The page_size argument for the Zoom API requests. The value should be between 30-100. It defines how many results should be returned per API request. More should be desirable as it reduces the number of API calls that are to be made. Default value: 100.
Working Directory	The working directory where intermediate files will be stored. These describe where the files will be downloaded as well. The folders will be cleaned regularly, preventing their growth. Default value: [verba install directory]\work\cdrimport\zoom\phone
Worker Thread Count	How many worker threads should be used to concurrently download media and import them. An exceedingly big number can be given, but that will be overridden if the underlying machine does not support the necessary number of cores. This way an invalid config cannot starve the system of resources. Default value: 4

Step 5 - Save the changes by clicking on the



icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

⚠ There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please click here .

IPC Data Exchange

IPC Data Exchange is part of the IPC Unigy 360 cloud service. IPC Data Exchange is an archiving service for Unigy 360. IPC Data Exchange offers APIs to:

- archive external records into Unigy 360
- download recordings from Unigy 360 for on-premise archiving

The import source implements the IPC Data Exchange REST-based download API. Each Unigy 360 tenant has a unique URL. Verba can import from multiple tenants. Security:

- HTTPS using TLS 1.2
- OAuth2 based authentication
- Transmitted data is not encrypted

The records are imported as standard records because the Data Exchange API does not support the trader voice data model with separate CDR and Media records. It might result in bigger storage requirements compared to native recording where mixed recording channels are stored in an optimized format.

The Data Exchange service is offered in two options to the customer:

- Redundant archiving: Unigy 360 continues to archive a call that has been downloaded via the API for redundancy. These calls can continue to be accessed via the Unigy 360 Cloud Services Portal.
- Delete immediately: Unigy 360 purges the copy after confirmation of delivery of the call.

For a general description of Verba Import sources, please refer to [import sources](#).

 Supported file format for import:

- GSM-FR encoded audio in WAVE container

Recording is supported for the following modalities:

- Voice

Creating an IPC Data Exchange import source

Follow the steps below to create a new Verba Import source for IPC Data Exchange:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system.
Type	Select IPC Data Exchange

Service URL	A specific URL for each customer must be used to get the call list, retrieve a call and acknowledge the file has been processed
Authorization Provider URL	A specific URL must be used to be authenticated and authorized to use the Data Exchange API.
Client Id	OAuth client identifier
Client Secret	OAuth client secret
User Id	An ID used for identifying the tenant
Password	Password for the user defined above
TLS Certificate File / Thumbprint	Specify the certificate file/certificate thumbprint that is being used for the IPC Data Exchange connection. If left empty then the Verba default certificate will be used
TLS Key File	Specify the file where the certificate key is stored if not in the Windows certificate store
TLS Key File Password	Specify the password for the file that contains the certificate keys
TLS Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: <ul style="list-style-type: none"> • .pem file with a list of certificates • comma separated certificate thumbprints • comma separated CA thumbprints

Step 4 - Click **Save** to save the settings

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Extension configuration

To match the imported conversations to a Verba extension (and to a Verba User account) you need to add the IPC Data Exchange login names to Verba as **extensions** with type "**User / Agent ID**".

IPC Data Exchange metadata

The system captures the following metadata specific to IPC Data Exchange recordings. These fields are available through the standard and the IPC Data Exchange specific custom metadata template.

Metadata Field	Description	Template	Available
Start Date		Standard	Yes
Start Time		Standard	Yes
End Date		Standard	Yes
End Time		Standard	Yes
Duration		Standard	Yes
From	Phone number, Button name, User name	Standard	Yes
From Info	User / contact name	Standard	No
To	Phone number, Button name, User name	Standard	Yes
To Info	User / contact name	Standard	No
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Name of the Verba user associated with the calling party	Standard	Yes
To (Verba)	Name of the Verba user associated with the called party	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause		Standard	No
Audio Codec		Standard	No
Video codec		Standard	No
Platform Call ID		Standard	Yes
Silence Ratio		Standard	No
Talkover Ratio		Standard	No
Longest Silence		Standard	No
User ID / Agent ID	IPC Unigy Trader ID	Standard	Yes
From Device		Standard	Yes
To Device		Standard	Yes
Dialed Number		Standard	No
From IP		Standard	No
To IP		Standard	No
From Proxy IP		Standard	No
To Proxy IP		Standard	No
Source Platform	IPC Data Exchange	Standard	Yes

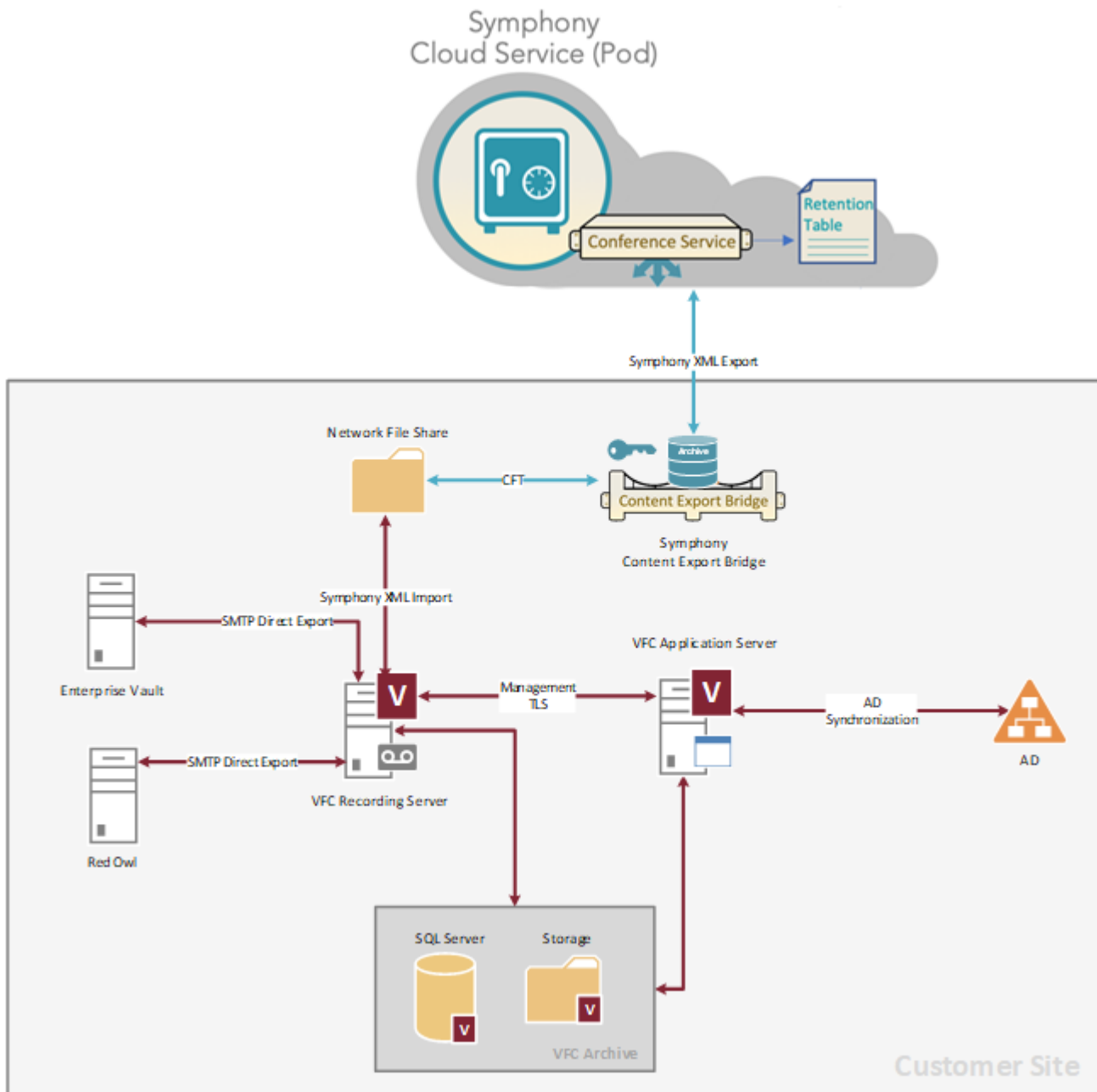
Conversation Type	Voice	Standard	Yes
Forward Reason		Standard	No
Recording failed		Standard	No
Media Length		Standard	No
Media Error		Standard	No
Voice Quality		Standard	Yes
Record Type	Standard	Standard	Yes
2N Source		Standard	No

Symphony Instant Messages - Files - CDRs

The secure, cloud-based communications platform that connects markets and individuals, Symphony promotes collaboration and increases workflow productivity while maintaining organizational compliance.

For more information on the solution, refer to the Symphony website at <https://symphony.com/>

Symphony can export the contents of conversations to shared folders. Verba then can import these files from this location and move them to the storage locations.



For a general description of import sources, please refer to [Import sources](#).

Supported import formats:

- XML (recommended)
- EML

Import is supported for the following features:

- Instant Messaging import
- File Transfer import
- CDR reconciliation for voice, video, screen recordings (Symphony XML format only)

Creating a Symphony import source

Follow the steps below to create a new Verba Import source for Symphony:

Step 1 - Open the Verba Web interface then select **Data / Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select Symphony XML (recommended) or Symphony EML
Source folder	Specify the network path to the shared folder where the Symphony conversations are available for import
Login Name	Login name for the network folder
Password	Password for the network folder

Step 4 - Click **Save** to save the settings

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data / Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, select the **Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information below:

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Step 6 - Set up how frequently the import should be run in the **Scheduling** section

Step 7 - Click on **Save**


Cisco Webex Teams

Cisco Webex Teams is an app-centric, cloud-based service that provides a complete collaboration suite for teams to create, meet, message, call, care, white board, and share, regardless of whether they're together or apart—in one continuous workstream before, during, and after meetings. It is built to help teams work seamlessly. It is simple, secure, complete, and open, and provides a space for people to work better. The core capabilities of Cisco Spark are Meetings, Messaging, and Calling. The Cisco Webex Teams platform, app-centric design, hybrid services, and architecture of Cisco Webex Teams create a unique and differentiated service.

For more information on the solution, refer to the Cisco Webex Teams website at https://www.cisco.com/c/en_uk/solutions/collaboration/webex-teams.html

Cisco Webex Teams provides an API that Verba is able to use to retrieve content from Webex Teams rooms.

For a general description of Verba Import sources, please refer to [Import sources](#).

 Recording is supported for the following modalities:

- Instant Messaging
- File Transfer

Creating the Integration on the Cisco Webex Teams side

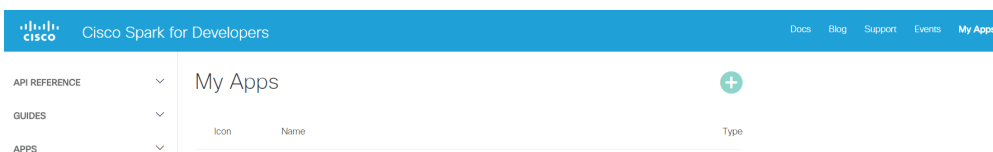
The integration needs to be set up in Cisco Webex Teams for it to allow connections for the Verba servers to the company's Webex Teams instance.

Follow the steps below to add Verba as a trusted source in Cisco Webex Teams.

Step 1 - Navigate to the Cisco Webex Teams developer page at <https://developer.webex.com/>

Step 2 - Click on the **My Apps** link at the top-right corner.

Step 3 - Click on the green **Add** button.



Step 4 - Click on the **Create an Integration** button

New App



Integration

Request permission (OAuth) to invoke Spark APIs on behalf of another user.
[Learn More](#)

[Create an Integration](#)



Bot

Build intelligent chatbots that post content and respond to commands.
[Learn More](#)

[Create a Bot](#)

Step 5 - Fill out the textboxes according to the table below.

Configuration item	Description
Name	Name the integration. This name will identify this integration in your Cisco Webex Teams environment
Contact Email	Set up a contact email. Certain messages may be sent as notifications to this email address
Icon	Select an icon
Description	Describe the integration
Redirect URI(S)	<p>Set up the Verba server's hostname or IP address and port number in the following format: https://verbaserver.company.com:4000</p> <p>The port that the service will listen on needs to be specified on the Verba side as well, as shown in the next section.</p> <p>This address and port is only used during authorization and needs to be accessible from the desktop computer used during the configuration. After successful authorization, this port is no longer used, the Verba servers will connect to Webex Teams directly.</p>
Scopes	<p>Select the following 3 scopes:</p> <ul style="list-style-type: none">• spark-compliance:events_read• spark-compliance:messages_read• spark-compliance:rooms_read• spark-compliance:people_read <p>The user who created the API Integration needs to be Compliance Officer on Webex Teams.</p>

New Integration

Name*

Name of your integration in 100 characters or less.

Verba Spark Integration

Contact Email*

Contact email for Cisco internal use only.

dummy@company.com

Icon*

Exact size 512 (W) x 512 (H) in jpg or png format.

Upload your own or select from our defaults.



[Edit](#)

Description*

Details of what your integration does, how it does, benefits, your business model and how an end user can get started in 1000 characters or less. Bullets and links markdown supported.

🔗 | ☰ | ☰ | 👁

[Supported markdown](#)

Redirect URI(s)*

One or more URIs that a user will be redirected to when completing an OAuth grant flow. [Learn more](#)

https://verbaserver.company.com:4000

[Add URI](#)

- spark-admin:roles_read Access to read roles available in your user's organization
- spark-admin:licenses_read Access to read licenses available in your user's organizations
- spark-compliance:events_read Access to read events in your user's organization
- spark-compliance:memberships_read Access to read memberships in your user's organization
- spark-compliance:memberships_write Access to create/update/delete memberships in your user's organization
- spark-compliance:messages_read Access to read messages in your user's organization
- spark-compliance:messages_write Post and delete messages in all spaces in your user's organization
- spark-compliance:rooms_read Access to read rooms in your user's organization
- spark-compliance:team_memberships_read Access to read team memberships in your user's organization
- spark-compliance:team_memberships_write Access to update team memberships in your user's organization
- spark-compliance:teams_read Access to read teams in your user's organization

Step 6 - Click on the **Create Integration** button.

At this point, the integration's page refreshes and at the bottom, you are presented with the automatically generated OAuth login parameters. The **Id** and the **Secret** shown here will need to be specified when configuring the integration on the Verba side.

Step 7 - Configure the Verba side integration as shown in the next section. This is important, as **Step 9** can only be performed if the Spark Import Source is already configured on the Verba side.

Step 8 - In the **OAuth Authorization URL** section, a URL is presented. Open this URL in the browser.

OAuth Settings

[Learn more about authentication in the Apps & OAuth Guide.](#)

Client ID

C96d609f881cdb08908d2dbe26a749cd1d2dc6d4cb399527487f403532d67c
Copy

Client Secret

fef26f569baa0bf57c25f3f493f3fa0f78fc3d122653cb0dee007385474f7083
Copy

The Client Secret will only be shown once so please copy and keep it safe! You can always regenerate it, but you will not see this one again.

OAuth Authorization URL

You can use the URL below to initiate an OAuth permission request for this app. It is configured with your redirect URI and app scopes. Be sure to update the state parameter.

```
https://api.ciscospark.com/v1/authorize?client_id=C96d609f881cdb08908d2dbe26a749cd1d2dc6d4cb399527487f403532d67cd2e&response_type=code&redirect_uri=https%3A%2FX2Fverbaserver.company.com%3A40808&scope=spark-compliance%3Aevents_read%26spark-compliance%3Arooms_read%20spark-compliance%3Amessages_read%20spark%3Aksms&state=set_state_here
```

Step 9 - At this point, you are presented with the prompt below to give access to the application. Click on the **Accept** button.



Verba Spark Integration
is requesting the following:

- Access to read events in your user's organization
 - Access to read rooms in your user's organization
 - Access to read messages in your user's organization
 - Allow decryption and encryption
- Only ask when requesting new permissions.

Accept

Decline

If the following page appears, then the integration is successful.

Verba Integration Successful

The Verba Importer Service has successfully received the Cisco Spark archiving access code.

Current token expire time: 89 days 23 hours 51 minutes 18 seconds

The Verba Import Service will automatically refresh the token.
You may close this window now.

If you receive an error here, please make sure that your Spark Import Source is correctly configured in Verba and try again.

Creating a Cisco Webex Teams import source

Follow the steps below to create a new Verba Import source for Cisco Webex Teams.

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select Cisco Spark
Spark Integration Client Id	Enter the Client Id that is shown in Step 7 of the previous section (Creating the Integration on the Cisco Spark side)

Spark Integration Client Secret	Enter the Client Secret that is shown in Step 7 of the previous section (Creating the Integration on the Cisco Spark side)
Redirect URI	Enter the hostname or IP address of the Verba server. The same address needs to be used as the setting that was configured in Step 5 of the previous section (Creating the Integration on the Cisco Spark side)
Listener Port	Enter the port where the Verba server is listening. The same a port needs to be used as the setting that was configured in Step 5 of the previous section (Creating the Integration on the Cisco Spark side)
TLS Certificate File / Thumbprint	Specify the certificate file / certificate thumbprint that is being used for the Cisco Webex Teams connection. If left empty then the Verba default certificate will be used
TLS Key File	Specify the file where the certificate key is stored if not in the windows certificate store
TLS Key Password	Specify the password for the file that contains the certificate keys
TLS Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: <ul style="list-style-type: none"> • .pem file with a list of certificates • comma separated certificate thumbprints • comma separated CA thumbprints

Step 4 - Click **Save** to save the settings

Import Source Configuration

[Add New Import Source](#)
[Back to Previous Page](#)

?

▼ Import Source

ID *

Name *

Type *

▼ Settings

Spark Integration Client Id

Spark Integration Client Secret

Redirect URI

Listener Port

TLS Certificate File / Thumbprint

TLS Key File

TLS Key Password

TLS Trust List

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Bloomberg Instant Messages

Bloomberg can export IM conversations to shared folders. Verba then can import these files from this location and move them to the Verba storage locations.

For a general description of Verba Import sources, please refer to [Import sources](#).

Creating a Bloomberg IM import source

Follow the steps below to create a new Verba Import source for Symphony:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select Bloomberg IM
Source folder	Specify the network path to the shared folder where the Bloomberg IM conversations are available for import

Step 4 - Click **Save** to save the settings

▼ Import Source

Name *

Type *

▼ Settings

Source Folder

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on Save

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy


RingCentral

RingCentral is an intuitive team messaging solution that will help your team reach their full potential with file and screen sharing, video, tasks, and more, all in one desktop and mobile app. Watch your business thrive thanks to more effective real-time communication and collaboration. In the digital age, it's an increasing challenge to connect teams due to the rich variety of resources. RingCentral provides a single, unified team workspace that empowers you to work, communicate, and collaborate faster and more effectively than ever before. Emails, scattered discussions, and disjointed resources are drastically reduced as teams share conversations, files, tasks, and calendars. Your teams, whether internal or external, can collaborate using their favorite devices anytime, anyplace.

For more information on the solution, refer to the RingCentral website at <https://www.ringcentral.com>

RingCentral can export the contents of conversations to shared folders. Verba then can import these files from this location and move them to the Verba storage locations.

For a general description of Verba Import sources, please refer to [Import sources](#).

 All RingCentral supported voice formats are supported by Verba as well.

Recording is supported for the following modalities:

- Voice

Creating a RingCentral import source

Follow the steps below to create a new Verba Import source for RingCentral:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select RingCentral
URL	The URL of the storage location where the RingCentral data is stored
User	Username of the service account that has access to the RingCentral storage
Password	Password of the service account that has access to the RingCentral storage
API Key	RingCentral Access API Key value. Visible in the RingCentral administration portal
API Secret	RingCentral Access API Secret value. Visible in the RingCentral administration portal

Step 4 - Click **Save** to save the settings

Import Source Configuration

[Add New Import Source](#)
[Back to Previous Page](#)

▼ Import Source

ID *

Name *

Type *

▼ Settings

URL

User

Password

API Key

API Secret

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Vodafone

Mobile Recording from Vodafone is a next generation mobile voice recording (MVR) solution that captures calls and text messages made and received on any mobile device regardless of operating system. For more information on the Vodafone solution, please refer to the Vodafone website at <https://www.vodafone.com/business/solutions/unified-communications/call-recording/network-mobile-recording>

Verba directly imports Vodafone calls via a secure and resilient connection. The system monitors when the last import occurred inside business hours, alerting and automatically failing over to an alternate connection if no calls are received. All available calls are imported as soon as they are available.

For a general description of Verba Import sources, please refer to [Import sources](#).

- Recording is supported for the following modalities**
- Voice

Creating a Vodafone import source

Follow the steps below to create a new Verba Import source for Vodafone:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration Item	Description
Primary Service URL	URL of the storage location where Vodafone recordings are stored
Secondary Service URL	URL of the storage location where Vodafone recordings are stored
User	Vodafone account user name
Password	Vodafone account password
TLS Certificate File / Thumbprint	Certificate file / certificate thumbprint used for the Vodafone connection.
TLS Key File	File system location where the certificate key is stored.
TLS Key Password	Specify the password for the file that contains the certificate keys.
TLS Key Trust List	Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options: pem file with a list of certificates comma separated certificate thumbprints comma separated CA thumbprints
Forward Proxy Address	IP address or FQDN of the forward proxy. When defined, the system will connect through a forward proxy.
Forward Proxy Port	The port of the forward proxy

Forward Proxy Username	Username for basic authentication for the forward proxy server
Forward Proxy Password	Password for basic authentication for the forward proxy server
Business Hours Timezone	Timezone applied to business hours for monitoring and failover purposes
Business Hours Start Time	Start of business hours
Business Hours End Time	End of business hours
Default Throttle Wait Time (Seconds)	Import back off time if Vodafone is busy
Recording Import Batch Size	Maximum number of Vodafone calls to request at once
On Completion Delete Files Stored In Vodafone	Must always selected during production. Allows flexibility during setup and testing.

Step 4 - Click **Save** to save the settings

ID *	<input type="text" value="12"/>
Name *	<input type="text" value="Vodafone Test Import Source"/>
Type *	<input type="text" value="Vodafone"/>

Primary Service Url	<input type="text" value="http://10.20.30.40/primary"/>
Secondary Service Url	<input type="text" value="http://50.60.70.80/secondary"/>
User	<input type="text" value="bank"/>
Password	<input type="password" value="*****"/>
TLS Certificate File / Thumbprint	<input type="text"/>
TLS Key File	<input type="text"/>
TLS Key Password	<input type="text"/>
TLS Trust List	<input type="text"/>
Forward Proxy Address	<input type="text"/>
Forward Proxy Port	<input type="text"/>
Forward Proxy Username	<input type="text"/>
Forward Proxy Password	<input type="text"/>
Business Hours Timezone	<input type="text" value="GMT-05:00 - SystemV/EST5EDT"/>
	<small>Greenwich Mean Time 8:55:29</small>
Business Hours Start Time	<input type="text" value="09 : 00"/> <input type="button" value="🕒"/>
Business Hours End Time	<input type="text" value="17 : 30"/> <input type="button" value="🕒"/>
Default Throttle Wait Time (Seconds)	<input type="text" value="60"/>
Recording Import Batch Size	<input type="text" value="10"/>
On Completion Delete Files Stored In Vodafone	<input type="checkbox"/>

Import Policy Configuration

Follow the steps below to configure the Data Import action:

- Step 1** - In the Verba web interface, navigate to **Data > Data Management Policies**
- Step 2** - Click on the **Add New Data Management Policy** button at the top-right corner of the page
- Step 3** - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Must be set as used to help determine call direction. If both source and destination numbers are unknown, i.e., not defined users/extensions, the call will still be recorded but only visible to superuser privilege.
Execute Only On Selected Servers	If enabled, a specific server can be chosen that will run this policy.

Vodafone metadata

The system captures the following metadata specific to Vodafone recordings. These fields are available through the standard and the Vodafone specific custom metadata template.

Metadata Field	Description	Template	Available
Start Date	Start date of the conversation	Standard	Yes
Start Time	Start time on the conversation	Standard	Yes
End Date	End date of the conversation	Standard	Yes
End Time	End time of the conversation	Standard	Yes
Duration	Length of the conversation	Standard	Yes
User	Name of the recorded user	Standard	Yes
From	Subscriber / Third Party Phone number	Standard	Yes
From Info	User / contact name	Standard	Yes
To	Subscriber / Third Party phone number	Standard	Yes
To Info	User / contact name	Standard	Yes
Direction	Direction of the call from the system perspective, requires configuring internal number/domain patterns	Standard	Yes
Direction (User)	Direction of the call from the recorded user perspective	Standard	Yes
From (Verba)	Verba user name associated with the From Number	Standard	Yes
To (Verba)	Verba user name associated with the To number	Standard	Yes
Location	Hostname of the recording server	Standard	Yes
End Cause	Normal, Hold, Transfer, Conference, Device Change, From Terminated, To Terminated	Standard	No
Audio Codec	Audio codec of the recorded streams	Standard	No
Video codec	Video codec of the recorded streams	Standard	No

Platform Call ID	Unique conversation identifier received from the recorded platform	Standard	Yes
Silence Ratio	Ratio of silence in the conversation	Standard	No
Talkover Ratio	Talkover ratio of the conversation	Standard	No
Longest Silence	Length of the longest silence present in the conversation	Standard	No
User ID / Agent ID	Vodafone user ID	Standard	Yes
From Device	Device ID of the calling party	Standard	No
To Device	Device ID of the called party	Standard	No
Dialed Number	Original dialed number	Standard	No
From IP	IP address associated with the calling party	Standard	No
To IP	IP address associated with the called party	Standard	No
From Proxy IP	IP address of the proxy server associated with the caller party	Standard	No
To Proxy IP	IP address of the proxy server associated with the called party	Standard	No
Source Platform	Vodafone	Standard	Yes
Conversation Type	Voice	Standard	Yes
Forward Reason	Forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)	Standard	No
Recording failed	Indicates if the recording has failed and the metadata was imported during CDR reconciliation	Standard	No
Media Length	Length of the media file related to the conversation in hhh:mm:ss format	Standard	No
Media Error	Shows the media processing errors during recording	Standard	No
Voice Quality	Overall voice quality check score for the conversation	Standard	No
Record Type	Standard	Standard	Yes
2N Source	In case of duplicate (2N) recording, records are marked as primary or secondary	Standard	No
Recording Id	Unique recording identifier	Vodafone	Yes
Archival Remarks	Vodafone archiver identifier and timestamp of call archive within Vodafone	Vodafone	Yes
Ingestion Time UTC	Timestamp of VFC recording ingestion	Vodafone	Yes
Route Id	Call route within Vodafone	Vodafone	Yes
Filename	Media filename within Vodafone, including IP of Vodafone archiver	Vodafone	Yes


O2

Mobile Recording from O2 is a next generation mobile voice recording (MVR) solution that captures calls and text messages made and received on any mobile device regardless of operating system.

O2 MVR can be delivered as a hosted on premise or hybrid solution. For more information on the O2 solution, please refer to the O2 website at <https://www.o2.co.uk/business/why-o2/customer-stories/mvr>

Verba directly imports O2 recordings via secure connection and depending on the value of the Polling Lag will run behind the current time a certain number of hours or minutes. This is to allow current calls to finish recording before import.

For a general description of Verba Import sources, please refer to [import sources](#).

 Recording is supported for the following modalities:

- Voice

Creating an O2 import source

Follow the steps below to create a new Verba Import source for O2:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration Item	Description
Name	Name your Import Source. This name will identify the source across the system.
Type	Select O2
Service URL	The URL of the storage location where O2 recordings are stored
Liquid Account Id	Id of the Liquid Account with access to O2 recordings
Solution Instance Id	Solution Instance Id of the Liquid Account with access to O2 recordings
User	Liquid Account Username
Password	Liquid Account Password
Polling Lag	Number of seconds import runs behind current time
End Timestamp	The earliest recording time to import from

Step 4 - Click **Save** to save the settings

ID *

Name *

Type *

Service Uri

Liquid Account Id

Solution Instance Id

User

Password

Polling lag (sec)

End Time

Import Policy Configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
------------------------------	-------------

Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

O2 metadata

The system captures the following metadata specific to O2 recordings. These fields are available through the standard metadata template only and only those fields listed are available.

Metadata Field	Description
Start Date	Recording Start Date
Start Time	Recording Start Time
End Date	Recording End Date
End Time	Recording End Time
Duration	Recording Duration
From	Subscriber / Third Party Phone number
From (Verba)	Verba user name associated with the From Number
To	Subscriber / Third Party phone number
To (Verba)	Verba user name associated with the To number
Direction	Call Direction
Direction (User)	Call Direction from user perspective
From (Verba)	Verba user name associated with calling party
To (Verba)	Verba user associated with called party
Source Platform	O2
Conversation Type	Voice
Record Type	Standard

TeleMessage

TeleMessage Recording is a next generation instant messaging solution that captures text messages and attachments sent and received on any mobile device via WhatsApp, WeChat/WeCom and TeleMessage Native Applications for iPhone and Android.

TeleMessage recording can be delivered as a hosted, on premise or hybrid solution. For more information on the TeleMessage solution, please refer to the TeleMessage website at [TeleMessage Mobile Archiver | Capture Mobile Text | Record Mobile Calls](#).

Verba directly imports TeleMessage recordings via secure connection in near real-time and includes support for plaintext, emotions, audio and video clips, location information, documents and contact cards exchanged during one on one conversations and group chat.

For a general description of Verba Import sources, please refer to [import sources](#).

Creating a TeleMessage import source

Follow the steps below to create a new Verba Import source for TeleMessage

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration Item	Description
IMAP Server	e-Mail account receiving TeleMessage data Server address format should be: <hostname or ip>:<port number> Note: The e-Mail account receiving TeleMessage data must have the TeleMessage e-Mail server IP addresses and sender account whitelisted
IMAP Username	e-Mail account username
IMAP Password	e-Mail account password
TLS Certificate File	Certificate file / certificate thumbprint used for the IMAP connection.
TLS Key File	File system location where the certificate key is stored.
TLS Key Password	Specify the password for the file that contains the certificate keys.
CA Certificate Chain File	Certificate chain (or Chain of Trust) is made up of a list of certificates that start from a server's certificate and terminate with the root certificate. If your server's certificate is to be trusted, its signature has to be traceable back to its root CA.
Use TLS	Tick to use TLS between the e-Mail account receiving TeleMessage data and Verba.

Step 4 - Click **Save** to save the settings

ID *	<input type="text" value="5"/>
Name *	<input type="text" value="TeleMessage Import Source"/>
Type *	<input type="text" value="Telemessage"/>

IMAP Server	<input type="text" value="outlook.office365.com:993"/>
	<small>Server address format should be: <hostname or ip>:<port number></small>
IMAP Username	<input type="text" value="vfcingest@outlook.com"/>
IMAP Password	<input type="password" value="*****"/>
TLS Certificate File	<input type="text"/>
TLS Key File	<input type="text"/>
TLS Key Password	<input type="password"/>
CA Certificate Chain File	<input type="text"/>
Use TLS	<input type="checkbox"/>

Map TeleMessage Users to Verba Users

Step 1 - Login to the web interface with **System administrator** rights.

Step 2 - Navigate to the **Users / Administration / Users** menu item.

Step 3 - Click the **Add New User** link and follow [User Configuration](#) instructions. The user name for WeChat users must match their WeChat user name.

Step 4 - Add new [Extension details](#) for recorded numbers, using either the TeleMessage number for WhatsApp and TeleMessage Native Application recording, or the Account Id for WeChat recording.

Step 5 - If the user is a WhatsApp or TeleMessage Native Application user, the **Extension Data Type** value should be set to Number /Address, otherwise set to User/Agent ID for WeChat.


Step 6 - While adding extension details for recorded numbers, each recorded user must have the following Recording Settings: Voice, Instant Messaging, Video and File Share.

Step 7 - Save the changes by clicking on the



icon.

Step 8 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Import Policy Configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Set up how frequently the Import should be run in the **Scheduling** section

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Specific Servers	If enabled, a specific server can be chosen that will run this policy

Enabling data import policy execution on servers

Step 1 - Login to the web interface with **System administrator** rights.

Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

Step 3 - Go to the **Service Activation** tab, then activate the **Verba Import Service** by clicking on the



icon.

Step 4 - Save the changes by clicking on the



icon.

Step 5 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

⚠ There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 7 - Click on the **Service Control** tab.

Step 8 - Start the **Verba Import Service** by clicking on the



icon.

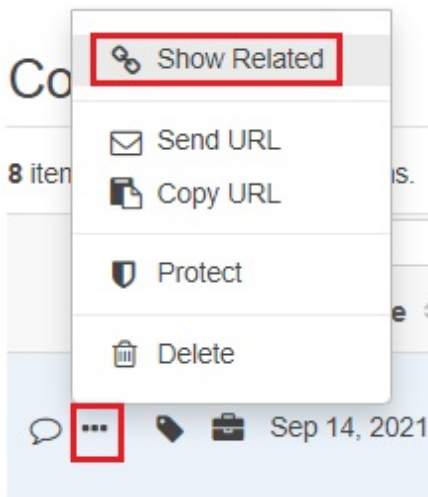
Conversation Search and Replay

[Searching conversations](#) works for all TeleMessage Source Platforms, e.g., TeleMessage WhatsApp or TeleMessage WeChat. Filtering using **Advanced Search Options** and adding Source Platform is possible.

A conversation record with "Instant Message" modality is created when a conversation first takes place, or, if the previous conversation has been idle for more than one hour. The instant message contains all conversation details and all participants are identified. During conversations, links to all attachments are created. These links allow download of audio, video, photos, documents, location and contact cards for review on the client computer.

Voice calls from WhatsApp, WeCom and TeleMessage native applications can be directly searched and replayed from their own voice conversation records in the web interface. File share conversation records are created for other types of attachments sent with individual messages.

It is possible to show all records created during a conversation by clicking on the elipsis (...) next to a record of interest and selecting **Show Related**.



When participants join or leave message groups, additional instant message type conversation records are created indicating the event. Instant Messages are also created when TeleMessage system administration events take place, for example, configuring a user for recording.

Conversation Archive

TeleMessage conversations may be archived using [Storage and export targets - VFC Capture \(Verba\) 9.6 - VFC Capture \(Verba\) Knowledge Base](#).

Normally, TeleMessage de-duplicates messages between users, however, for compliance purposes, messages are duplicated for every conversation participant. This allows different archive retention and ensures all recordings are found when searching using a specific user.

Maintenance of the IMAP Server mailbox is the responsibility of the customer. No incoming data from TeleMessage is deleted by VFC.

Fault Tolerance

If an error occurs during conversation import that requires it to be retried, this is possible during normal business hours.

The file *Program Files\Verba\work\cdrimport\telemesssage\<Import Source Id_Data Import Policy Id>\laststate\<Import Source Id_Data Import Policy Id_IMAP e-Mail UIDVALIDITY_.cursor>* contains an integer number which increases as conversations take place in the IMAP e-Mail inbox.

Conversation Import can be rewound by a certain number of messages according to the reduction in this value. Messages already ingested will be ignored, not duplicated.

If a message has been partially ingested, it is necessary to manually remove this message from the database before resuming just before this message number.

The number in the file is the next e-Mail message UID or Unique Identifier. The UIDVALIDITY is a single value together with the UID that ensures a unique key for every e-Mail in the IMAP mailbox.

Before rewinding conversation import, stop the Verba Import Service, then update the file before starting the Verba Import Service - [Service control and activation - VFC Capture \(Verba\) 9.6 - VFC Capture \(Verba\) Knowledge Base](#).

Microsoft Exchange IMAP configuration with OAuth 2.0

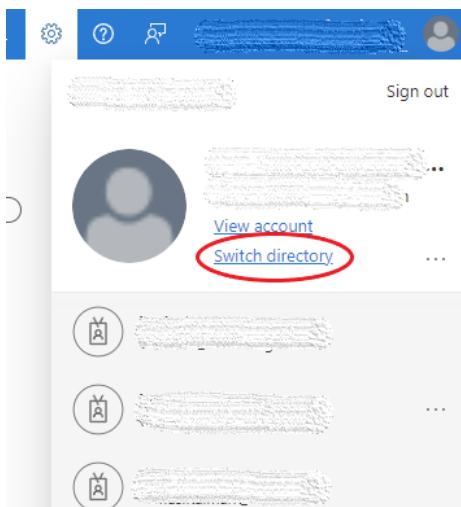
Effective October 1, 2022, Microsoft began disabling Basic authentication for Outlook, EWS, RPS, POP, IMAP, and EAS protocols in Exchange Online. This means that for TeleMessage import sources using Exchange will no longer work with simple username and password authentication, instead OAuth 2.0 authentication must be used.

Register application in Azure

For Import Service on a Media Repository server to use OAuth 2.0, an application needs to be registered in Azure.

Step 1 - Go to <https://portal.azure.com>

Step 2 - Select the directory (tenant) where the Exchange service is running. Click on *Switch directory* in the upper-right corner drop-down menu. Then select the appropriate directory from the list.



Step 3 - Go to *Azure Active Directory*. If it's not on the opening page, use the search or find it under *All services*.

All services

All

Favorites

Recents

Categories

- General
- Compute
- Networking
- Storage
- Web
- Mobile
- Containers
- Databases
- Analytics
- AI + machine learning

Azure Active Directory Virtual machines Resource groups

General (18)

- All resources
- Subscriptions
- Marketplace
- Templates
- Quickstart Center
- Reservations

Step 4 - Select *App registrations* on the left, and click on *New registration*.

Microsoft Azure Search results

All services > Verint Systems Kft.

Verint Systems Kft. | App registrations

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy

+ New registration Endpoints Troubleshooting

Starting June 30th, 2020 we will no longer add any new features that are not compatible with the Microsoft Authentication Library (MSAL) and Microsoft Identity Platform for Windows (MIPW).

All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter

2 applications found

Display name ↑↓

MT	Microsoft Teams Chat Recording
VI	Verba IMAP Oauth support test

Step 5 - Enter a name of your choice, then click *Register*.

Microsoft Azure Search resources, services, and docs (G+/)

All services > | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

OAuth service

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Verint Systems Kft. only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

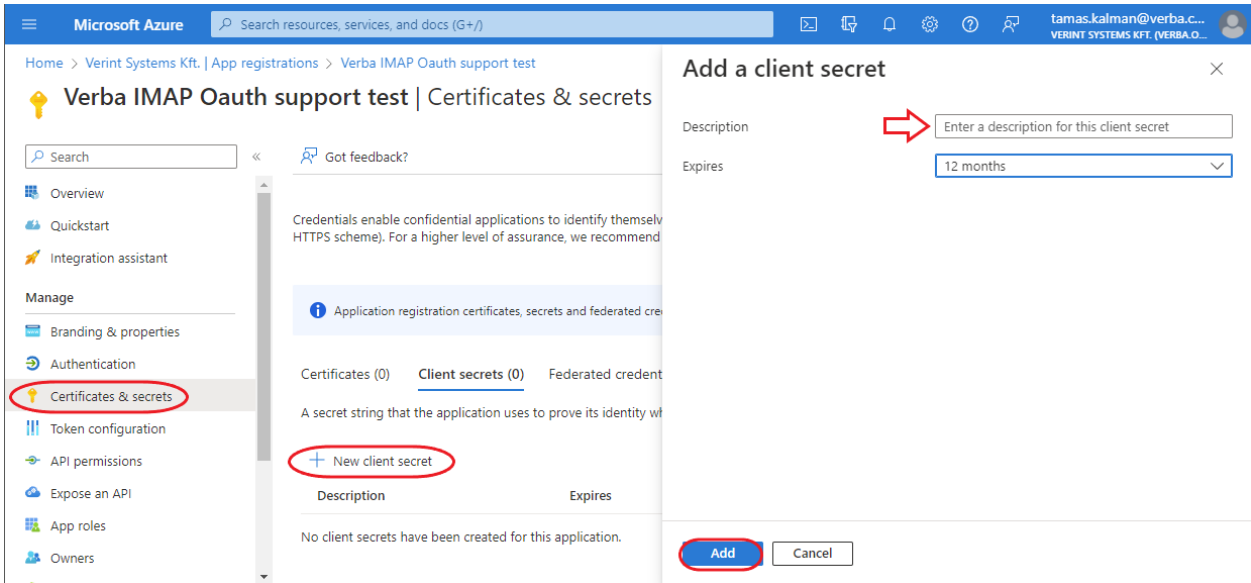
Select a platform e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

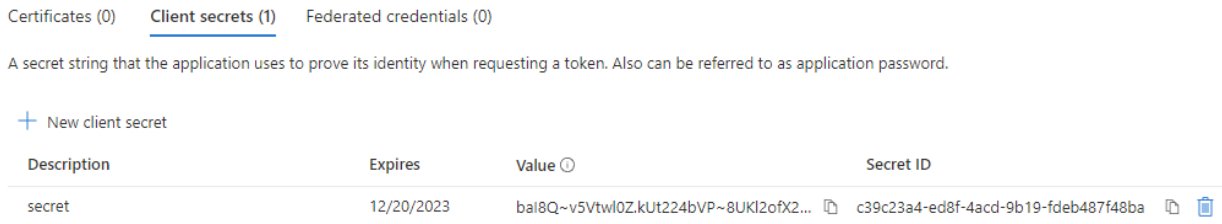
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

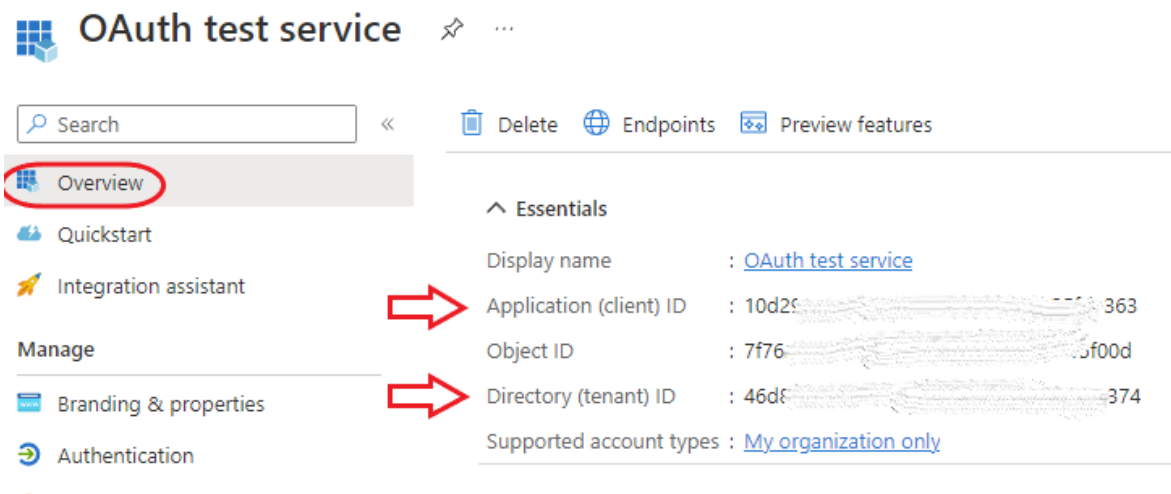
Step 6 - Create a new secret for the application.



Step 7 - Copy and save the secret's value. It is only shown for a short period after created. It cannot be viewed later.







Step 8 - The two other values we need from the application is the application (client) id and the directory (tenant) id. Both can be copied from Overview:



Configure TeleMessage import source

On the Import source configuration page, select OAuth 2.0 for Authentication Mode, and set Application (Client) ID, Application (Client) Secret, Directory (Tenant) ID to their respective values from the registered Azure application above.

IMAP Server	outlook.office365.com:993	
	Server address format should be: <hostname or ip>:<port number>	
IMAP Username		
Authentication Mode	OAuth 2.0	
Application (Client) ID	10d...363	
Application (Client) Secret	
Directory (Tenant) ID	46c...374	

Register service principals in Exchange

This whole section is quoted from here: [Authenticate an IMAP, POP or SMTP connection using OAuth](#)

Once your Azure AD application is consented to by a tenant admin, the tenant admin must register your AAD application's service principal in Exchange via Exchange Online PowerShell. This is enabled by the [New-ServicePrincipal cmdlet](#).

To use the New-ServicePrincipal cmdlet, install the ExchangeOnlineManagement and connect to your tenant as shown in the following snippet.

```
Install-Module -Name ExchangeOnlineManagement -allowprerelease
Import-Module ExchangeOnlineManagement
Connect-ExchangeOnline -Organization <tenantId>
```

If you still get an error running the New-ServicePrincipal Cmdlet after you perform these steps, it is likely due to the fact that the user doesn't have enough permissions in Exchange online to perform the operation.

The following is an example of registering an Azure AD application's service principal in Exchange:

```
New-ServicePrincipal -AppId <APPLICATION_ID> -ServiceId <OBJECT_ID> [-Organization <ORGANIZATION>]
```

The OBJECT_ID is the Object ID from the Overview page of the Enterprise Application node (Azure Portal) for the application registration. It is not the Object ID from the Overview of the App Registrations node. Using the incorrect Object ID will cause an authentication failure.

OAuth test service | Overview ...
Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups

OAuth test service ...

Search

Delete Endpoints Preview features

Properties

OT Name OAuth test service

Application ID 10d29dad-2404-412b-b4c5...

Object ID 3d30d86f-1999-44b8-a416-...

Getting Started

Essentials

Display name : OAuth test service

Application (client) ID : [REDACTED]

~~Object ID : 3d30d86f-1999-44b8-a416-...~~

Directory (tenant) ID : [REDACTED]

Supported account types : My organization only

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory that are not supported by Microsoft Authentication Library (MSAL) and Microsoft Graph.

Get Started Documentation

The tenant admin can find the service principal identifiers referenced above in your AAD application's enterprise application instance on the tenant. You can find the list of the enterprise application instances on the tenant in the Enterprise applications blade in the Azure Active Directory view in Azure Portal.

You can get your registered service principal's identifier using the [Get-ServicePrincipal cmdlet](#).

```
Get-ServicePrincipal | fl
```

The tenant admin can now add the specific mailboxes in the tenant that will be allowed to be access by your application. This is done with the [Add-MailboxPermission cmdlet](#).

The following is an example of how to give your application's service principal access to one mailbox:

```
Add-MailboxPermission -Identity "john.smith@contoso.com" -User <SERVICE_PRINCIPAL_ID> -AccessRights
```

VFC can now access the allowed mailboxes via the POP or IMAP protocols using the OAuth 2.0 client credentials grant flow. For more information, see the instructions in [Permissions and consent in the Microsoft identity platform](#).

Troubleshooting

If the import fails, do the following checks:

- Check if the client secret hasn't expired in Azure. Create a new one if needed and update on the import source configuration page.
- The default scope for the OAuth2 token is '<https://outlook.office365.com/.default>'. If this needs to be changed for some reason, the correct scope can be set/edited in the registry with the following entry:

HKEY_LOCAL_MACHINE\SOFTWARE\Verba\Archive Import\IMAP\OAuth2TokenScope

Verint

This page provides a guide to configuring a Verint Import Source in Verba.

Verba's capabilities are now further expanded by Verint Import functionality: Near real-time import of BT ITS (both TDM and IPSI) and Cisco Passive recording from WFO 15.2. The WFO and Verba systems are connected via an External Server within WFO and Data Import within VFC.

Please note for Cisco Passive Call Injection:

1. The VFC "from info" and "to info" fields are populated directly from WFO data.
2. The "Verba from" and "Verba to" fields are set by a trigger in the VFC database. Based on the recorded party flag, if the "to" or "from" extension is configured in Verba the system will find the user and assign the recording to that user.

Please note 2N and N+1 WFO systems are supported. If any WFO server fails, the Verba Import Source will continue with those WFO servers still working.

For a general description of Verba Import sources, please refer to [Import sources](#).

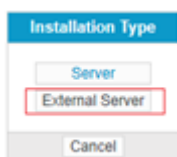
For a general description of Data Import action, please refer to [Data Import policy](#).

It is recommended to complete the WFO configuration steps before creation of the Verint Import Source.

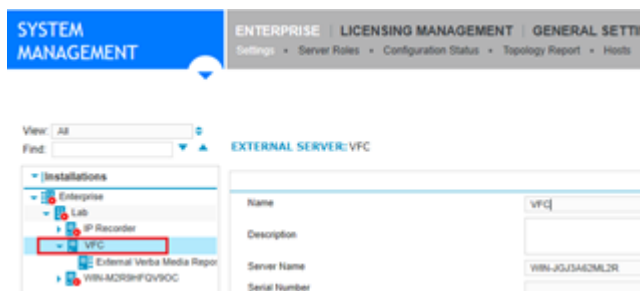
The minimum WFO patch levels are: Consolidator KB202257 and RecAncillary KB201776.

Configuration Steps - WFO

Step 1 - In WFO Enterprise Manager under System Management > Enterprise > Settings, press Create Installation and create an External Server.



Step 2 - Assign the External Server a Name and enter the Windows Server Name of the VFC Server.



Step 3 - Under System Management > Enterprise > Server Roles, add the External Verba Media Repository Role.

External Verba Media Repository

Step 4 - Select and configure the External Verba Media Repository Role. The Media Repository Name is identical to the Windows Server Name of the VFC Server used when adding the External Server. The Port number must be the same as the Port number used in the VFC Import Source configured shortly.



Creating a Verint import source

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system
Type	Select Verint
Verint Recorder Address	Newline separated Verint Recorder address(es). Each line must use the following syntax: Verint Recorder Serial Verint Recorder FQDN or IP For example: 329001 verintrecorder.contoso.com 329002 61.123.45.67
HTTP Port	Port number matching the Verba Media repository configured in WFO 15.2.
TLS Certificate File / Thumbprint	TLS Certificate Filename / Thumbprint (optional)
TLS Key File	TLS Key Filename (optional)
TLS Key Password	TLS Key Password (optional)

Step 4 - Create a Data Management Policy with Import Source Type Verint and Action Data Import.

Verba Import API

Enabling the Verba Import Service

Step 1 - In the Verba Web Interface go to **System > Servers > Select your Media Repository (or Single) Server > Click on the Service Activation** tab.

Step 2 - Activate the **Verba Import Service** by clicking on the



icon.

Step 3 - Click on the **Service Control** tab.

Step 4 - Start the **Verba Import Service** by clicking on the



icon.

Creating a Verba Import API import source

Follow the steps below to create a new Verba Import source for Cloud9:

Step 1 - Open the Verba Web interface then select **Data > Import Sources** from the top menu

Step 2 - Click on the **Add New Import Source** link on the top right

Step 3 - Complete the configuration according to the requirements in the following table

Configuration item	Description
Name	Name your import source. This name will identify this source across the system.
Type	Select Verba Rest API
HTTP Port	HTTP Port, where the Verba Rest API service will be listening for incoming HTTP requests. Any free port (aka not in use by other applications running on the Verba server) is good.
HTTPS Port	HTTPS Port, where the Verba Rest API service will be listening for incoming HTTPS requests. Any free port (aka not in use by other applications running on the Verba server) is good. Please, don't try to use the port 443 because the Verba web application is already using that.
TLS Certificate File / Thumbprint	Specify the certificatefile/certificatethumbprint that is being used for the connection. If left empty then the Verba default certificate will be used
TLS Key File	Specify the file where the certificate key is stored if not in the windows certificate store
TLS Key File Password	Specify the password for the file that contains the certificate keys

<p>TLS Trust List</p>	<p>Specify the list of certificates that Verba trusts from a 3rd-party connection. Available options:</p> <ul style="list-style-type: none"> • .pem file with a list of certificates • comma separated certificate thumbprints • comma separated CA thumbprints
<p>Connection Timeout [seconds]</p>	<p>Specify after how many seconds of communication inactivity should we consider an incoming HTTP or HTTPS request a failure.</p> <p>For bad network infrastructures you may want to increase this setting.</p>

Step 4 - Click **Save** to save the settings

Import policy configuration

Follow the steps below to configure the Data Import action:

Step 1 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 2 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 3 - For the action, select **Data Import**

Step 4 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 5 - Configure the policy details, based on the information that is shown in the **configuration items summary table** below

Step 6 - Scheduling must not be configured because this is an API where we must listen all the time for incoming requests

Step 7 - Click on **Save**

Configuration Parameter Name	Description
Enable Recording Rules	Specifies if all data should be processed in the imported data set or just the records of the recorded users as configured in Verba
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

HTTP, HTTPS request format

The requests have to be multipart ([rfc1341](#)).

The Verba Import API accepts the [Verba CDR XML](#) format alongside with a media file.

For SMS import you can place the text of the sms in the CDR XML's sms field and omit sending a media file.

For chat import you have to use our [IM XML](#) format to attach the chat messages (next to the CDR XML) as a .im 'media' file.

Load balancer configuration

AVAILABLE SINCE 9.7.4

Load balancer health probe configuration must be HTTP GET with path = '/healthprobe'.

Resilient storage and archiving

Resilient storage infrastructure

Storage resiliency is an important requirement in many deployments where the customers want to ensure that the data captured by the system is stored in a resilient and highly available fashion on the storage infrastructure. It is recommended to consult your storage administrator for best practices and available options. It is highly recommended to use the resiliency features of the storage infrastructure whenever it is available. The resiliency and high availability options may vary greatly depending on the underlying infrastructure, but most vendors offer sophisticated options. Here you can find some examples:


- On-premise solutions from Dell EMC, Netapp, Hitachi, etc. have mirroring or replication options
- Cloud storages have great variate of resiliency options with geo-redundant capabilities:
 - Azure Storage: <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>
 - AWS S3: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/disaster-recovery-resiliency.html>
- Windows DFS Namespaces have a replication option: <https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/dfs-overview>

These options seamlessly provide storage resiliency for the recording system. Depending on the capabilities, you can potentially achieve automatic failover as well.

Dual archiving

AVAILABLE IN 9.6.7 AND LATER

If for some reason, the storage platform cannot provide resiliency, the recording system has a feature called dual archiving which allows storing the recordings on 2 different storage targets.

 Do not use dual archiving if you can achieve storage resiliency with the built-in capabilities of the storage infrastructure. The storage platforms have more robust and advanced capabilities to provide resiliency with e.g. automatic synchronization across the instances, which are not supported by the dual archiving feature.

The system can upload/copy 2 copies of the same file to 2 different storage targets when this option is enabled. The system will not keep the storage targets in sync. If for some reason, there is a data loss on one of the storage targets, the system will not be able to detect that and will not attempt to synchronize the data between the 2 storage targets.

During playback, download, or export, the system will seamlessly attempt to access the files on the first storage target, and if for some reason that is not available, it will turn to the second storage target.

The following table summarizes the availability of the dual archiving feature in various storage-related capabilities:

Feature	Availability	Impact
Playback / Multi Playback	Supported	The process tries to access the media files on the first storage target. If it cannot access the media (storage target unavailable, media file unavailable), the process automatically tries the second storage target.

Download / Multi Download	Supported	The process tries to access the media files on the first storage target. If it cannot access the media (storage target unavailable, media file unavailable), the process automatically tries the second storage target.
Export (Advanced Export, Policy-based Export, Policy-based Direct Export)	Supported	The export process tries to access the media files on the first storage target. If it is able to access the media, it will move to the next call. If it cannot access the media (storage target unavailable, media file unavailable), the process automatically tries the second storage target.
Import	Supported	Once a call is imported, the system can upload/dual archive the call from the default media folder on the server.
Delete	Supported	The process only attempts to delete a copy only if the retention period has expired (if set). The system can delete one or both copies at one time. If only one copy is deleted, the CDR is updated accordingly. The audit log contains which copy was deleted during the transaction.
Upload	Supported	The upload process supports one or two storage targets. The upload action uploads the files as a single transaction to both locations. If one fails, it will continue trying to upload. Direct upload policies are also supported.
Move Media	Supported	The move policy is extended to allow dual archiving of existing records that are already uploaded (archived) to a storage target. Once a record is archived (uploaded to 2 storage targets), the policy only supports moving files from one of the locations. Both copies cannot be moved with a single move policy. The policy has a new filter option to define which copy to move (First, Second). If not set, the policy will automatically use the first copy only.
Copy	Supported	The copy policy is extended to allow dual archiving of existing records that are already uploaded (archived) to a storage target. Once a record is archived (uploaded to 2 storage targets), the policy only supports copying files from one of the locations. Both copies cannot be copied with a single copy policy. The policy has a filter option to define which copy to copy (First, Second). If not set, the policy will automatically use the first copy only.
Archive in DB	Supported	The database record is moved to the archive table. It has no impact on the files.
Archive in DB and Move Media	Supported	See Move and Archive in DB policies.
Increase Retention Period	Supported	The policy will increase the retention period of one or both copies. The policy has a filter option that defines which copy to increase (first, second, both). If not set, the policy will automatically apply the change on the first copy only.
Legal Hold	Supported	Legal hold works seamlessly across both copies. Only one of the copies cannot be under legal hold. If any of the copies are stored on a storage target that supports the legal hold flag on the storage, the system sets the flags accordingly.
Encryption, Signing	Supported	The system only supports encrypting and/or signing both copies with the same keys. There is no way to encrypt/sign only one of the copies. The system does not support post-upload signing/encryption (the policy automatically filters out dual archived records). The Verify Signature action on the web interface verifies only the first available copy.
Transcription	Supported	The transcription process tries to access the media files on the first storage target. If it fails, it will attempt to access the files from the second storage target. Currently, transcription is only supported for local and network shares (SMB/DFS). After successfully transcribing a call, the transcription files are uploaded to both storage targets.

Delete Phonetic Index	Not Applicable	-
Create Phonetic Index	Not Applicable	-
Voice Quality Check	Supported	<p>The process tries to access the media files on the first storage target. If it is able to access the media, it will move to the next call. If it cannot access the media (storage target unavailable, media file unavailable), the process automatically tries the second storage target.</p> <p>The system only uses one of the copies to calculate the score, because the 2 copies are identical (when both exist).</p>
Transcode	Supported	<p>The transcode process tries to access the media files on the “primary” location. If it cannot access the media (storage target unavailable, media file unavailable), the process automatically tries the “secondary” location. After successfully transcoding a call, the new media files are uploaded to both storage targets.</p>
Delete Communication Policy Events	Not Applicable	-
File Verification	Supported	<p>The file verification process runs on both copies. It will alert in case one or both copies are missing.</p>
Deduplicate Recordings	Supported	<p>Deduplication works on both copies seamlessly. The process will automatically remove duplicated records on both storage targets after the Primary/Secondary copy was selected. Primary/Secondary should not be confused with First/Second. Primary/Secondary designates the 2 copies created during 2N recording. These copies are initially stored on the same storage location. While First/Second is related to dual archiving. Without deduplication, someone can have 4 copies if dual archiving is enabled.</p>

Best practices for large databases

Using, operating, and maintaining large databases requires special considerations when configuring and using data management policies. This article provides best practices for large databases.

Use Direct Upload and Export

Direct upload and export minimize the impact on the database by relying on the files and system configuration available on the Recording Serves, instead of running expensive database queries.

Ensuring Data Retention Policy order

The policy processing acquires locks on each subject conversation to support parallel execution by default, and then each policy is tested for each conversation record to make sure the policy priority order is kept. This makes the policy configuration error-proof but can put a high load on the database if it contains many conversations. In that case, it is recommended that this type of locking be turned off in the server configuration by setting the **Storage Management / Data Retention / Check Policy Order on Call Basis** to **No**. But then the order of the policies should be ensured by some additional policy configuration:

- Conversations older than: for example, if the conversations should not be deleted until they got exported, then for the Delete policy, set Conversations older than to one week later than the export policy. This is not a 100% solution though, because if the export process stopped for more than a week then it will not be effective anymore.
- CDR fields
 - example 1: if the Export should not happen until the files are uploaded/moved to specific storage, set up a new filter so the Storage Target Equal to the desired storage
 - example 2: if a policy should be executed depending on if the Transcode policy already transcoded a conversation, then one can use the Elapsed Time Since Transcoding (UTC) field to filter
- Execute Only After Another Policy Executed / Execute Only After This Export Executed: if the previous options cannot work, then use these options to ensure the order of policy processing.

Note that setting Check Policy Order on Call Basis to “No” will result in bulk conversation locking and processing (1000 conversations per round) and that could prevent simultaneous transcoding on multiple servers.

Recent Than filter to save SQL Server processing

Policy filters can be complicated and so the SQL Server may perform unnecessary processing. In order to avoid that in case of large databases, it is recommended to set up a **Recent Than** filter for such types of policies. More specifically, if there are records for a long period of time (years), and the majority of the records cannot be ignored based on the nature of the policy (export policy for example), then a **Recent Than** filter can narrow down the processed records significantly. Obviously, if the processing is stopped for a longer period, then the conversations that moved out from the window will not be processed unless the **Recent Than** filter is broadened temporarily.

Data management policy monitoring

Available in version 8.1 and later

You can monitor the data management policy execution at the Background Task Monitor page at **System / Background Task**.

Each policy execution attempt has an item in the list. Tasks executed more frequently than daily have a single item for each day (e.g. upload policies).

Find and List Background Tasks Refresh										
Status:	All	Task Type:	All	2014.12.09 00:00	-	<input type="text"/>	<input type="button" value="Find"/>			
12 items found, displaying all items. Page(s): 1										
Name	Task Type	Current State	Processed	Total	Failed	Start Time	End Time	Status	Status Message	Server
Automatic Deletion	Delete	100% <div style="width: 100%;"></div>	2	2	0	Dec 09, 2014 19:14:01	Dec 09, 2014 20:14:01	Done	Task finished	MR
To Network Share	Upload	<div style="width: 0%;"></div>	2	0	0	Dec 09, 2014 19:09:50		Running	Processing	RS
Racstation Upload	Upload	<div style="width: 100%;"></div>	2	0	0	Dec 09, 2014 18:50:13	Dec 09, 2014 20:08:37	Done	Task finished	RS
NetApp Upload	Upload	<div style="width: 100%;"></div>	2	0	0	Dec 09, 2014 18:42:43	Dec 09, 2014 19:49:12	Done	Task finished	RS
Racstation Upload	Upload	<div style="width: 100%;"></div>	2	0	0	Dec 09, 2014 18:35:43	Dec 09, 2014 19:49:12	Done	Task finished	RS
Delete from NAS	Delete	100% <div style="width: 100%;"></div>	2	2	0	Dec 09, 2014 18:18:14	Dec 09, 2014 19:18:14	Done	Task finished	MR
Delete from NAS	Delete	100% <div style="width: 100%;"></div>	2	2	0	Dec 09, 2014 18:11:27	Dec 09, 2014 19:11:28	Done	Task finished	MR
Racstation Upload	Upload	<div style="width: 100%;"></div>	8	0	0	Dec 09, 2014 18:07:22	Dec 09, 2014 19:33:43	Done	Task finished	RS
Delete from MR	Delete	100% <div style="width: 100%;"></div>	1	1	0	Dec 09, 2014 18:02:30	Dec 09, 2014 19:02:30	Done	Task finished	MR
MR Storage Upload	Upload	<div style="width: 100%;"></div>	1	0	0	Dec 09, 2014 17:56:22	Dec 09, 2014 19:33:43	Done	Task finished	RS
No policy calls	Upload	<div style="width: 0%;"></div>	1	0	1	Dec 09, 2014 17:46:22	Dec 09, 2014 19:33:43	Error	Task finished with errors	RS
Default upload	Upload	<div style="width: 0%;"></div>	1	0	1	Dec 09, 2014 17:20:52	Dec 09, 2014 18:46:21	Error	Task finished with errors	RS
12 items found, displaying all items. Page(s): 1										
Export options: Excel RTF										

Data management policy audit log

The audit file is a standard CSV file where the values in each row are separated by semicolons. Each row represents a single conversation record in the audit log file. The name of the file contains all tasks executed by the Verba Storage Management and the Verba Import service produces an audit log stored on the given Verba server. The audit log files can be found under the standard "[LOG]\storage audit" where [LOG] is the standard log folder path.

- the type of the policy (e.g. delete, upload),
- the policy ID, and
- a timestamp representing the start date and time of the task execution.

The following table describes the available fields in the log file:

Column	Sample value	Description
ccdr_id	39896902-7fbf-11e4-8104-0050568b7c85	Unique conversation ID
native_id	3bb3a699-a3f3-40c6-8fae-f786dda2d5eb 1353 -1	Unique conversation ID derived from the signaling messages
n_files	3	Number of files effected by the action. The system stores multiple files for each conversation record such as metadata XML, waveform, etc.
src_folder_id	2	Source storage target ID
src_folder_name	MR Storage	Source storage target name
src_folder_type	mr	Source storage target type
src_folder_path	E:\media	Source storage target path
dst_folder	2	Destination storage target ID
dst_folder_id	MR Storage	Destination storage target name
dst_folder_type	mr	Destination storage target type
dst_folder_path	E:\media	Destination storage target path
policy_id	3	Data retention policy ID
policy_name	Delete from MR	Data retention policy name
action	delete	Data retention policy type
error_code	0	Error code
error_desc		Error description
ts	2014.12.09 17:02:30.253	Timestamp
retention_start		Data retention start date and time if configured
retention_period	0	Data retention period if configured
retention_auto_delete	false	Indicates if automatic deletion is configured for the record

Data management policy audit logs are never deleted.

Disposal audit log

The disposal log collects and maintains summary information when recordings are deleted (after the retention period has expired or after users manually delete a conversation).

The disposal log is disabled by default and has to be enabled in the server configuration (on all Media Respority servers) under **Storage Management / General / Disposal Log**.

The disposal log contains the following information:

- Reference data regarding the recording platform and jurisdiction for which the recording has been made
- The execution date of the disposal process
- The retention period for the recording
- Date of the recording
- The number of disposed recordings with the same date and retention period
- A separate line for each retention period disposed on the current date

The disposal log can be accessed through the following reports:


- [Disposal Log](#)
- [Disposal Log By User Location](#)

Export

, and you can also rename the headers

- [Overview](#)
- [User permissions for conversation export](#)
 - [User permissions](#)
 - [Administrator permissions](#)
- [Starting a conversation export](#)
- [Configuring advanced conversation exports](#)
 - [Conversation Export](#)
 - [Conversation Detail Fields](#)
 - [Media Files](#)
 - [Metadata Files](#)
 - [CDR File](#)
 - [Manifest File](#)
 - [Scheduling](#)
- [Checking export progress and status](#)
- [Failure behavior](#)
- [Disabling direct download](#)

Overview

 The system has 3 different export features:

- **Advanced export:** advanced export is designed to export data from the system on-demand or continuously with many configurable options.
The advanced export is described on this page in detail.
- **Export policy:** the export policy is designed to extract a large volume of data from the system on a continuous basis with only basic options.
The description of the export policy can be found here: [Export policy](#)
- **Direct export policy:** the direct export is designed to automatically extract all content directly from the Recording Servers, instead of querying the database. It is most suitable for exporting all data on a continuous basis from the system. The description of the export policy can be found here: [Export policy](#)

The following table describes the difference in the export features:

	Advanced Export	Export Policy	Advanced IM Export Policy	Direct Export Policy
Place of execution	Media Repository / Application Server	Media Repository / Application Server	Media Repository / Application Server	Recording Server
Suitable for Large Volumes	No	Yes	Yes	Yes, recommended
Data Types and Source Platforms	Any	Any	Microsoft Teams	Limited
Database Query / File Based	Database Query	Database Query	Database Query	File

Filters	Any	Any	Any	Limited
User Assignment	Yes (policy filter configuration)	Yes (policy filter configuration)	Yes (policy filter configuration)	Yes (user /extension configuration)
Available from Search	Yes	No	No	No
Custom CDR File	Yes	No	No	No
Manifest File	Yes	No	No	No
Audit Log	Yes	Yes	Yes	Yes
Configurable Schedule	Yes	Yes	Hourly or less frequent only	No
Supports imported records	Yes	Yes	No	No
Simultaneous Execution	A single advanced export job can only run on a single server.	A single export policy can run on multiple servers, data is split across the servers.	A single export policy can run on multiple servers, data is split across the servers.	No

Advanced conversation export allows exporting recordings from the system:

- The export feature is available for both users and administrators. Users can export recordings accessible for them, administrators can export any recordings.
- Access to the export features is controlled by permissions.
- Exports are executed by the storage service running on the Media Repository server(s). When users start a new export job, the system executes the job in the background and notify the users after completing the job in an email. Progress can be monitored on the export task list page.
- Storage targets are available specifically for export jobs. The system places exported files to these locations. Access to storage targets can be restricted for configured users/groups. The system also offers a direct download option, where exported files are hosted on the Media Repository server.
- The system is able to export media files for voice and video recordings, and IM transcript files if available (the system does not generate IM transcript files from the database if the file is missing).
- The process can export metadata files in two formats: CSV and XML. The columns in the CSV file are customizable and created during the export process. The XML metadata file is the original metadata file created by the recording services. If the XML file is not available, the export process will not create it.
- The export feature can create a Conversation Detail Records (CDR) file for each job in CSV/PDF format, listing all recordings.
- The system can create an export manifest file for each export job. It details how the search was run (query), the number of items exported, by who the search was run, the exceptions involved/encountered.
- Export jobs can be run based on a configured schedule.

User permissions for conversation export

User permissions

The table below summarizes user-level permissions controlling access to export features. Users are only allowed to access export features through the search/list page, providing access to recordings available for the specific user only.

Permission	Description
------------	-------------

Download a Conversation	Allows downloading a single conversation on the search/list page.
Conversation Export	Grants access to advanced conversation export on the search/list page: <ul style="list-style-type: none"> • Media Files Only • Metadata Files Only • Both Media and Metadata Files
Recurring Conversation Export	Grants access to scheduled/recurring export under advanced export.
Conversations List Export	Allows exporting conversation detail records to CSV/XLS/PDF on the search/list page.

Administrator permissions

The table below summarizes administrator-level permissions controlling access to export features. Administrator level permissions allow exporting all recordings under Administration -> Conversation Export.

Permission	Description
Conversation Export	Grants access to advanced conversation export under Administration -> Conversation Export: <ul style="list-style-type: none"> • Media Files Only • Metadata Files Only • Both Media and Metadata Files
Recurring Conversation Export	Grants access to scheduled/recurring export under advanced export.

Starting a conversation export

The system allows exporting and downloading conversations in various ways:

- Users can download voice/video recordings, media files on the search/list page by clicking on the download icon (disk), for more information see [Downloading a single media file](#).
- Users can export conversation detail records on the search/list page by clicking on one of the export options (Excel, CSV, PDF) under the export button in the top toolbar.
- Users can use the advanced export features on the search/list page by clicking on the **Advanced** option under the export button in the top toolbar.
- Administrators can use the advanced export features under **Data > Export**.

Configuring advanced conversation exports

Once you start an advanced conversation export, you can configure various settings for the export job.

Conversation Export

In this section, you can configure the general settings for the export job.

Configuration Item	Description
Name	Descriptive name of the export job.

Target Type	<p>Type of the storage destination, the process moves the files to this location.</p> <ul style="list-style-type: none"> Export to Storage Target A storage target can be defined in the Verba system by storage administrators. Access to storage targets, available for export, can be restricted to configured users or groups. For more information, see Storage and export targets. Access to exported files are not controlled by the Verba system, the system does not offer access to exported files. Export and Download as ZIP File Using this option, the system exports files to a configurable folder and offers a download option after completing the export job. The folder can be configured in the server configuration under Web Application \ Miscellaneous \ Conversation export direct download target folder setting. The download is available as a single non-compressed ZIP file containing all files exported during the job. The Direct Download feature can be completely disabled in the system, the feature is enabled by default. This option is only available for export jobs started from the search and list page. Once users download the ZIP file, the system offers the deletion of the ZIP file. No other mechanism is implemented to remove export files from the system, although these ZIP files can be removed administratively from the folder (manually).
Storage Target	Storage Target selected for the export job. This option is only available if the Target Type is set to Storage Target. For more information, see Storage and export targets .
Time zone	The event times in the conversation metadata will be shown based on the selected time zone.
Rename Files	Files exported using their original file name unless a specific pattern is defined to rename the files. All media and metadata files will be renamed using the configured pattern.
Do Not Create Subfolders	If turned on, the export job won't place the files into different folders based on the date of the recordings.
Do Not Create Log in the Database	<p>If turned on, then the system will not generate log in the database. This can be used to save space when no reporting is needed.</p> <p>Note that the system will not export a conversation multiple times for the same Export Task even if this option is turned on.</p>
Server	Sets which server(s) should run the export job. Servers can be added by clicking on the >> button, or removed by the << button. The server(s) on the same geographical location as where the user resides should be selected.
Query	Descriptive/friendly representation of the query used to select conversations for export. If a user starts the export from the search/list page, the query shows the criteria configured on the search page. If an administrator starts the advanced export job, this field reflects the query built on this page below.
Send Notification to Email Address(es)	Email address(es) for notifications, separated by line breaks. The system sends a notification to the configured email address(es) after completing the export job. If the recurring job is scheduled, the system sends the notification after each run.
Email Subject	The subject of the notification email.
Email Message	Body of the notification email.
Source Dataset	Administrators can limit the scope of exported conversations to online, archived or both.
Ignore CDR-Only Records Without Related Media	For trader voice conversations, the system can create CDR-Only records without a reference to any media. These records can be ignored during export.
Conversation Detail Fields	Administrators can define the criteria for selecting records for the export job.

Conversation Detail Fields

The table below summarizes the available conversation details fields which can be configured as a filter for the export.

Category	Field	Description
Participants	From	The number of the caller party in the conversation
	From Info	The number of the called party in the conversation
	From (digits)	The number of digits in the phone number of the initiator of the conversation
	From Device ID	The Device ID of the initiator of the conversation
	From IP	The IP address of the caller party in the conversation
	To	The name of the caller party in the conversation
	To Info	The name of the called party in the conversation
	To (digits)	The number of digits in the phone number of the target of the conversation
	To Device ID	The Device ID of the target of the conversation
	To IP	The IP address of the called party in the conversation
	Both To or From	The number of any party participating in the conversation
	Both To or From Info	The name of any party participating in the conversation
	Dialed Number	The original dialed number
	User	The user associated with the conversation based on the extension configuration
	User Location	The location of the user, defined in the user configuration
	Extension	The extension numbers in a conversation, a selection list of the configured extensions, otherwise similar to the 'Any party number' field below
	Group	The group where a conversation belongs to based on the users associated with the conversations
User ID	The User/Agent/Trader ID obtained from the recorded platform	
Details	Start Time (UTC)	The start time of the conversation in UTC timezone
	Recent Than	Only conversations selected where the start time is recent than the defined value. Make sure it is not used with a recurring schedule, otherwise conversations can be skipped if the defined value is close to the recurring period.
	Older Than	Only conversations selected where the start time is older than the defined value
	Direction	The direction of the conversation (e.g. internal, inbound, outbound, etc.)
	End Cause	The end cause of the conversation (e.g. normal, hold, transfer, etc.)
	Duration Interval	The length of the conversation

	Conversation Type	The type of conversation. Available options: <ul style="list-style-type: none"> • Voice • Video • Instant Messaging • SMS • Desktop Screen • Screen & Application Share (Lync/SfB) • Whiteboard (Lync/SfB) • Poll / Q&A (Lync/SfB) • File Share (Lync/SfB)
	Forward Reason	The forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)
	Protected	Defines whether the conversation is protected
	Label	The labels added to the conversation
	Case	The cases containing the conversation
	Encrypted with Certificate	The certificate used to encrypt the conversation
	Signed with Certificate	The certificate used to sign the conversation
	Quality Management Scorecard Exist	Checks if there is a Quality Management Scorecard assigned to the conversation
Analytics	Silence ratio	The silence ratio in a conversation
	Talkover ratio	The talkover ratio of the conversation
	Longest Silence	The longest silence present in a conversation
Technical	Recording Server	The hostname of the server that recorded the conversation
	Media file name	The name of the stored media file
	Storage target	The current storage location of the media file(s)
	Source Platform	Defines which telephony / unified communications system the conversation was recorded on (Cisco, Sfb, Avaya, etc.)
	Secondary	Defines whether the conversation is recorded on a server marked as secondary (using 2N / duplicate recording)
	CDR/Media Record	Defines whether the conversation is a Standard, CDR-Only or Media-Only record. CDR-Only and Media-Only records are used for trader voice recording.
	Elapsed Time Since Transcoding (UTC)	The time elapsed since transcoding in UTC timezone
	Time of Transcode (UTC)	The date and time of transcoding in UTC timezone
Metadata Fields	Custom Metadata Fields	Custom metadata fields configured in the system, the list of available fields might vary depending on the integration configured and the metadata templates added

Media Files

In this section, you can configure how you want to export media files (voice/video recordings and IM transcript files if available).

Configuration Item	Description
Export Media Files	Enables exporting media files.
Decrypt Encrypted Conversations	If a voice/video file is encrypted, the system can automatically decrypt the files before exporting. Original files remain encrypted.
Generate Media Files for CDR-Only Conversations	For trader voice recordings, the system can stitch related media files together for the CDR-Only records. If not enabled, the system will export the metadata file only for the CDR-Only records.
Voice Format	Voice recordings can be optionally transcoded to the selected format.
Video Format	Video recordings can be optionally transcoded to the selected format.
Desktop Recording and Screen /Application Sharing Format	Screen share recordings can be optionally transcoded to the selected format.

Metadata Files

In this section, you can configure how you want to export metadata files.

Configuration Item	Description
Export XML Metadata Files	Enables exporting original XML metadata files. Metadata XML files are generated by the recording services. If the file is missing, the system will not create it during the export process.
Create CSV Metadata Files	Enables creating customized CSV metadata files for each exported recording. By clicking on the Configure Columns button, you can select the fields and the order of the fields stored in the CSV file. The header names and the time format are configurable too.
CSV Delimiter	If CSV export is selected, the CSV delimiter can be configured here.

CDR File

In this section, you can configure how you want to create a conversation detail record file for the export job.

Configuration Item	Description
Create Conversation Detail Records (CDR) File	Enables creating a CDR file for the export job, listing all conversations. The system creates one CDR file for each export job. By clicking on the Configure Columns button, you can select the fields and the order of the fields displayed in the CDR file. The header names and the time format are configurable too.
Conversation Detail Records (CDR) File Format	The system supports CSV and PDF formats for CDR files.
CSV Delimiter	If CSV format is selected, the CSV delimiter can be configured here.

Manifest File

In this section, you can configure how you want to create a manifest file for the export job. The manifest file is an HTML formatted file with configurable content.

Configuration Item	Description
Create Manifest File	Enables creating a manifest file for the export job.
Include User Identification	Defines if user identification is included in the manifest file.
Include Query	Defines if the descriptive/friendly query (see above) included in the manifest file.
Include List of Exported Files	Defines if all files exported listed (with an indication of error) in the manifest file.
File Extension	Defines the file extension for the manifest file.

Scheduling

In this section, you can configure how you want to export conversation detail record files.

Configuration Item	Description
Schedule	<p>Scheduling setting for the export job.</p> <ul style="list-style-type: none"> • Recurring Allows periodic exports. The system keeps track of the periods and only exports recordings since the last run. • Once Immediately Run export now, once. • Once At... Run export at a configured date and time once.
Time of Next Export	Date and time of the next export run.
Period Settings	Scheduling settings for periodic/recurring exporting. By clicking on the ... button, the scheduling wizard opens.

Checking export progress and status

Advanced export jobs can be monitored in the following way:

- Advanced export jobs initiated by users can be checked under **Data > Export**. Users can only check their own export jobs.
- Advanced export jobs initiated by administrators under **Data > Export**. Administrators can check the status of any export job, regardless of the initiator of the export job.
- Advanced export jobs initiated by both users and administrators can be followed under **System > Background Tasks**. Access to this page is controlled by special permission.

Finished export tasks can be removed by opening the export task, then clicking on the **Delete** button at the bottom. When removing an export task, it's also possible to remove the exported files, by ticking the **Delete files on the export location** checkbox in the deletion confirmation popup.

Failure behavior

It is a rare occurrence, but recording export might fail, for example, unexpected permissions change or media unavailable. The behavior of export jobs in this scenario depends on job scheduling - Export jobs can be configured to run once and also to run continuously.

- If run once is selected, then failed records are never retried.
- If run continuously is selected, failed records are dealt with according to the scheduling:

- If no scheduling is set, or minute by minute scheduling is configured, the “end” of the export job is considered at the end of the day. At this point, background task and manifests are closed. During the day, failed exports will be retried and they will also be retried indefinitely on every following day. Exported recordings are placed in folders according to call start time date and not from export run time. Only the latest manifest contains details of exported recordings that failed on previous occasions but are now successful.
- If daily/weekly/monthly scheduling is set, failed records will be reported at the end of each export job and the manifest will contain them. As per the schedule, when the export runs again, failed recording exports will be retried. Exported recordings are placed in folders according to call start time date and not from export run time. Only the latest manifest contains details of exported recordings that failed on previous occasions but are now successful.

At present, it is not possible to configure a job that exports previously failed exports of recordings. In order to prevent the retry of failed exports, it is recommended to use the **Recent Than** condition to limit efforts. In general, this approach is recommended for reasons of performance.

Disabling direct download

You may want to completely disable the direct download option. By disabling the direct download option, users will only able to export recordings to specified storage targets.

In order to disable this option, follow the steps below:

Step 1 - In the Verba web interface click on **System > Servers** and select your Media Repository server, or select the appropriate Configuration Profile at **System > Configuration Profiles**.

Step 2 - Click on the **Change Configuration Settings** tab.

Step 3 - Expand **Web Application > Miscellaneous**.

Step 4 - Configure **Enable direct download folder field on the export page**.

Step 5 - Click on the **Save** icon to save your settings

Step 6 - The system will notify you that the changes need to be applied to the server by restarting the involved services. Execute the required tasks.

Server and service configuration

Server Configuration and Configuration Profiles

The Verba system enables administrators to centrally configure all Verba servers in a distributed recording system. The central configuration uses the concept of **configuration profiles**, that store common configuration settings of multiple servers, allowing simple configuration changes across many similar recording servers or desktop clients. Verba servers can be configured individually or through their configuration profiles in the Verba Web Application under **Administration / Verba Servers** or **Administration / Configuration Profiles**.

There are two types of configurations settings in the system:

- ones, which require service restart in order to take effect and
- ones, which can be modified on-the-fly without service restarts.

The system stores the affected service names and the type of the way of the configuration refresh for every configuration setting. So, after changing a configuration setting, the administrators will be notified, which service has to be restarted, which service has to reread the settings on-the-fly, etc. Administrators are also able to individually override the automatically generated tasks if certain conditions have to be met.

Every Verba server runs a service, called Verba Node Manager Agent, which is responsible for handling the central configuration actions and this service also provides server status information and service control and activation functionality.

After initial installation, every server is automatically registered into the central configuration database and the default server configuration profile is assigned also.

Configuration settings related to recorded phone numbers are also administered through this central configuration module.

- [Service control and activation](#)
- [Verba server administration](#)
- [Verba server configuration](#)
- [Verba server configuration profiles](#)
- [Shared servers](#)
- [Server Certificates](#)

Service control and activation






In order to access service control and activation for a given Verba server follow these steps:

- Step 1** - Select **Administration / Verba Servers** menu item (requires System Administrator rights for your user)
- Step 2** - **Click on the row of the server** you want to manage (in your system there might be only one server)
- Step 3** - On the server configuration page you will find the **Service Control** and the **Service Activation** tabs

Service Activation




Under the Service Activation tab, the startup type of the Verba services can be set. The configuration of the not activated (disabled startup type) services won't be shown under the Change Configuration Settings tab.

The following table describes the available features for the services:

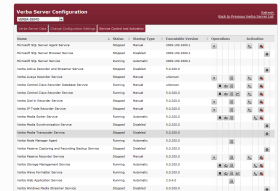
Icon	Feature	Description
	Automatic service startup	Sets the startup type of the service to automatic.
	Manual service startup	Sets the startup type of the service to manual.
	Delayed service startup	Sets the startup type of the service to delayed.
	Disable service	Disables the service. Disabling a service will turn off the corresponding configuration settings as well.
	Enable service	Enables the service and sets the startup type to automatic. Enabling a service will turn on the corresponding configuration settings.







Service Control

The following table describes the available features:

Icon	Feature	Description
	Start service	Starts the service.
	Stop service	Stops the service.
	Restart service	Restarts the service.

i The Service Control and Activation tabs might be on one tab instead of two in your installation (as seen on the above screenshot).







	View service log	Loads the most current part of the service log into the log viewer pane.
	Download service log	Downloads the last 100000 lines of the service log
	View service statistics	Displays the service statistics in a new browser window.
	Trigger failover recovery	Triggers the failover recovery if the service failed over to another node previously. Available only in the case of BT ITS and IPC Unigy recording.
	Stop maintenance mode	Stops the maintenance mode. For more information, see: Maintenance mode
	Start maintenance mode	Starts the maintenance mode. For more information, see: Maintenance mode

Using the log viewer

After selecting the **View Service Log** button for a service, the system loads the most recent lines from the service log.

```
Loaded Service Log: Verba Cisco Compliance Service
INFO 2019-07-15 10:04:42.202 StandbyHelper - Standby mode read from registry: false
INFO 2019-07-15 10:04:42.202 StandbyHelper - Standby state not changed.
INFO 2019-07-25 14:11:33.406 Options - About to reread access lists and persistent room list.
INFO 2019-07-25 14:11:33.611 Options - Number of extensions in blacklist: 0
INFO 2019-07-25 14:11:33.611 Options - New blacklist:
INFO 2019-07-25 14:11:33.611 Options - Number of extensions in accesslist: 0
INFO 2019-07-25 14:11:33.611 Options - New accesslist:
On-demand: 00001010
On-demand: 00001999
On-demand: 00001096
WARN 2019-07-25 14:11:33.611 Options - Number of extensions in blacklist is zero!
WARN 2019-07-25 14:11:33.611 Options - Number of extensions in accesslist is zero!
INFO 2019-07-25 14:11:33.611 StandbyHelper - Reading Standby mode from Registry...
INFO 2019-07-25 14:11:33.612 StandbyHelper - Standby mode read from registry: false
INFO 2019-07-25 14:11:33.612 StandbyHelper - Standby state not changed.
INFO 2019-07-25 14:11:33.948 Options - About to reread access lists and persistent room list.
INFO 2019-07-25 14:11:33.952 Options - Number of extensions in blacklist: 0
INFO 2019-07-25 14:11:33.952 Options - New blacklist:
INFO 2019-07-25 14:11:33.952 Options - Number of extensions in accesslist: 0
INFO 2019-07-25 14:11:33.952 Options - New accesslist:
On-demand: 00001010
On-demand: 00001999
On-demand: 00001096
WARN 2019-07-25 14:11:33.952 Options - Number of extensions in blacklist is zero!
WARN 2019-07-25 14:11:33.952 Options - Number of extensions in accesslist is zero!
INFO 2019-07-25 14:11:33.952 StandbyHelper - Reading Standby mode from Registry...
INFO 2019-07-25 14:11:33.955 StandbyHelper - Standby mode read from registry: false
INFO 2019-07-25 14:11:33.955 StandbyHelper - Standby state not changed.
INFO 2019-08-19 13:32:24.161 Options - About to reread access lists and persistent room list.
INFO 2019-08-19 13:32:24.163 Options - Number of extensions in blacklist: 0
```

The following table describes the available features:

Icon	Feature	Description
	Toggle log tail follow	If this option is enabled, the system automatically refreshes the log panel with the latest service log file content and scrolls the panel to the end.
	Toggle line wrapping	If this option is enabled the log lines are wrapped to fit into the log window.
	Toggle log filter	Enables log filtering using the expression entered into the input box.
	Clear log buffer	Clears the log buffer on the screen.

Verba server administration


If a Verba system is installed at different locations in a multi-site environment and may need to use multiple recording servers to scale up, there are more than one Verba Recording Servers. Verba stores server information (the hostname of the Recording Server, which has recorded the call) in every call record and provides searching capabilities based on this field.

Moreover, the system provides central configuration capabilities through Verba server administration.

In order to define Verba servers, the administrator or the system administrators have to select **Administration / Verba Servers** menu item.

Find and List Verba Servers

[Add New Verba Server](#)
[Discover Verba Servers](#)
[View Last Calls by Verba Servers](#)
[Refresh List](#)

 There are tasks to be executed regarding the configuration of some of the Verba Servers.
If you would like to execute these tasks now, please [click here](#).

Hostname begins with

No active query. Please enter your search criteria using the options above.

5 items found, displaying all items. Page(s): **1**

Hostname	Role	Configuration Profile
BOSTON-RECORDER	Local Recorder	Default Local Recorder Configuration Profile
LOSANGELES-RECORDER	Local Recorder	Default Local Recorder Configuration Profile
NEWYORK-RECORDER	Local Recorder	Default Local Recorder Configuration Profile
PRINCETON-MR	Central Controller	Default Central Controller Configuration Profile
VERBA-TEST	Central Controller & Local Recorder	Default Central Controller and Local Recorder Configuration Profile

5 items found, displaying all items. Page(s): **1**

Export options: [Excel](#) | [PDF](#) | [RTF](#)

Creating a Verba Server

You can add servers by clicking on the **Add New Verba Server** link on the **Administration / Verba Servers** page. The system automatically registers the servers after installation. After pushing the button the following page opens.

Verba Server Configuration

[Refresh](#)
[Add New Verba Server](#)
[Back to Previous Verba Server List](#)

VERBA-TEST

[Verba Server Data](#) | [Change Configuration Settings](#) | [Service Control and Activation](#)

Verba Server Data

Hostname*

Role*

Configuration Profile

Record non-configured extensions

Description

Creation Date: Jun 17, 2010 9:57:27 AM
 Created By: Verba Administrator (Administrator)
 Last Modification Date:
 Last Modified By:
[View Change History](#)

* Indicates required item.

Server Status

Operating System Windows 7 (6.1.7600)

CPU Intel(R) Core(TM)2 Duo CPU P8700 @ 2.53GHz

Memory Usage

Category	Value [Mbyte]
Free Memory	1346.44
Used Memory	2189.46

Media Folder Drive Usage

Category	Value [Mbyte]
Used Storage Space	221793.76
Free Storage Space	15600.23

The following table describes the available fields:

Field Name	Description	Requirements
Hostname	FQDN of the server	Required field. Minimum length: 1 Maximum length: 255 Must be unique in the system.

Role	Select the desired role for this server	-
Configuration Profile	Select the desired configuration profile to use for this server. All settings configured in the configuration profile will be available for the server. In this way the configuration can be easily centralized and multiple servers with the same configuration (or with almost the same configuration) can be easily and quickly configured through the configuration profile.	-
Description	Customizable description field.	Maximum length: 256

After filling out the form, press the **Save** button to save server data into the database.

Modifying and deleting Verba servers

To edit a Verba Server entry, you have to click on the desired row of the list showing previously defined servers. After clicking on the row, a new page opens automatically.

To make changes effective, push the **Save** button. All conditions, which are described in the previous part, have to be met.

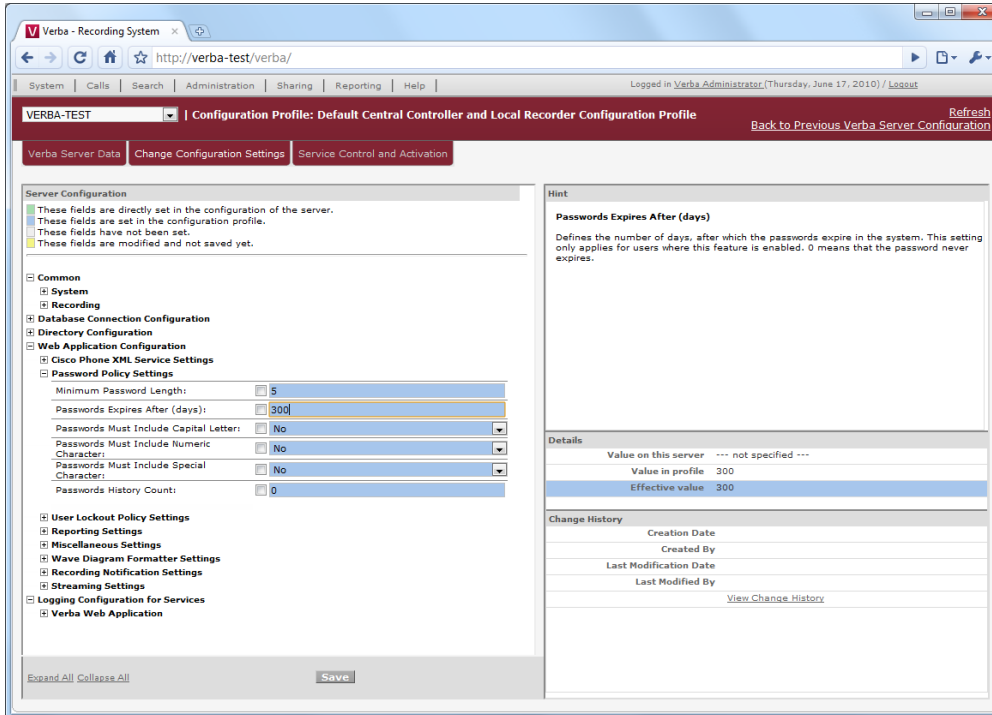
You can delete a server by clicking the **Delete** button. Only those servers which have not recorded any calls can be deleted.

Discover Verba servers

The system can help to determine servers, which have not been added to the system database, but there is at least one call that was recorded on those servers. On the **Find and List Verba Servers** page, choose **Discover Verba Servers** link. The system automatically lists servers, which are have not been added yet. The system automatically registers the servers after installation.

Verba server configuration

In order to access Verba servers configuration, the administrator or the system administrators have to select **Administration / Verba Servers** menu item and select the desired server. When the server configuration page is loaded, select the **Change Configuration Settings** tab.



Configuration settings

- [Network settings](#)
- [Directory settings](#)
- [Cisco Central Silent Monitoring Configuration settings](#)
- [Cisco JTAPI Configuration settings](#)
- [Unified Call Recorder service configuration reference for Cisco network based recording](#)
- [Web application settings](#)
- [CDR and Archived Content Importer settings](#)

Verba server configuration profiles

Verba server configuration profiles help administrators to easily configure and maintain Verba servers. The configuration profiles hold common configuration settings for a group of Verba servers. After changing a configuration setting in the profile, the change can be easily populated to the effected server by a single button click.

During system installation every server is assigned to a default configuration profile based on the server role.

Find and list configuration profiles

Select **System / Configuration Profiles** menu item. You can use the quick filter above the title, to apply the query and press enter.

Find and List Configuration Profiles [Add New Configuration Profile](#)

4 items found, displaying all items. ?

Name	Type	Default	Creation Date	ID
Default Media Collector & Lync Filter Configuration Profile	Media Collector & Lync Filter	Yes	Aug 14, 2020, 11:22:14 AM	5
Default Media Collector & Proxy Server Configuration Profile	Media Collector & Proxy Server	Yes	Aug 14, 2020, 11:22:15 AM	7
Default Media Repository and Recording Server Configuration Profile	Media Repository & Recording Server	Yes	Aug 14, 2020, 11:22:13 AM	2
Default Media Repository Configuration Profile	Media Repository	Yes	Aug 14, 2020, 11:22:14 AM	6

4 items found, displaying all items.


Export options: [Excel](#) | [CSV](#) | [PDF](#)

Creating a configuration profile

You can create a new configuration profile by clicking on the **Add New Configuration Profile** link on the **System / Configuration Profiles** page. After selecting the link, the following page is opened.

Configuration Profile Configuration [Add New Configuration Profile](#)
[Back to Previous Configuration Profile List](#)

[Configuration Profile Data](#)

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

Configuration Profile Data

Name*

Type*

Default

Copy Settings from Profile

[Save](#)

* Indicates required item.

The following table describes the available fields:

Field Name	Description	Requirements
Name	The name of the configuration profile.	Required field. Minimum length: 3 Maximum length: 128
Type	Choose the server role for the configuration profile. Only servers with selected role can be assigned to the configuration profile.	Required field.

Default	Indicates whether this profile is the default one or not.	-
Copy Settings from Profile	Copy settings from a preexisting profile	-

After filling out the form, press the **Save** button to save the configuration profile data into the database.

Modifying and deleting configuration profiles

To edit a configuration profile entry, you have to click on the desired row of the list showing registered configuration profiles. After clicking on the row, a new page opens automatically.

To make changes effective, press the **Save** button. All conditions, which are described in the previous part, have to be met.

You can delete the configuration profile by clicking on the **Delete** button. Only those profiles can be deleted, which does not have any server linked to it.

Profile level and server level configuration

The system highlights the configuration items that are different from the profile value, both in the profile and server configuration. In the server configuration the checkbox notes that the local configuration should overwrite the central value.

Profile configuration:

- These fields are being used on all servers.
- These fields are being overridden by at least one server.
- These fields are modified and not saved yet.

▲ Upload

Uploading Enabled:	Yes
Number of Upload Threads:	4
Policy Based Uploading Enabled:	No

Server configuration:

- These fields are directly set in the configuration of the server.
- These fields are set in the Configuration Profile.
- These fields are modified and not saved yet.

▲ Upload

Uploading Enabled:	<input type="checkbox"/>
Number of Upload Threads:	<input checked="" type="checkbox"/> 6
Policy Based Uploading Enabled:	<input checked="" type="checkbox"/>

Shared servers

- [Overview](#)
- [Configuring a Verba cluster](#)
- [Configuring shared servers](#)
- [Firewall requirements](#)

Overview

Due to strict regulatory requirements in certain countries, recordings and metadata containing Client Identifying Data (CID) need to be stored and accessed only from within a certain country or jurisdiction. Recording may be done outside of the jurisdiction, if all data associated with the recording is immediately moved to the final storage location, and no data containing CID is kept at the place of recording. Microsoft SfB/Lync systems can be deployed in a shared fashion, where other parts of the system can use certain components of the system. For instance, Edge pools can be shared by multiple Front-End pools. Due to this design, calls belonging to users from different countries/jurisdictions will be handled by the same shared component in certain cases. In order to record calls handled by the shared components such as Edge Servers, various Verba components need to be deployed and made aware of all recorded users regardless of their location.

In order to meet these requirements, the Verba system supports shared components/servers. It allows deploying multiple Verba systems to properly segregate both media and metadata, and support shared SfB/Lync deployments. Key features include:

- Multiple Verba systems, called Verba clusters, can be deployed to segregate media files and recorded metadata.
- Specific servers in a Verba cluster can be shared with other clusters to allow the recording of users initially belonging to the other cluster(s). These calls are called external calls.
- Server roles available for sharing: Verba Recording Server, Verba SfB/Lync Call Filter, Verba Media Collector & Proxy Server
- Supported integrations:
 - Microsoft SfB/Lync voice/video/screen share recording
 - Microsoft Teams voice/video/screen share recording
 - BT IPTrade, IPC Unigy and Speakerbus trader voice recording (BT ITS recording is not supported)
 - Cisco voice/video/screen share recording
 - Any active SIP/SIPREC based voice/video recording integration
 - Any network port mirroring based voice/video recording integration
- Only voice/video/screen share recording is supported
- External calls recorded by the shared Recording Servers are automatically moved to the corresponding Verba cluster using an internal API running on the Verba Media Repository servers. No metadata or media file is kept on the shared servers for these types of calls.

Limitations:

- Silent monitoring is not supported for external calls recorded by shared servers
- On-demand recording is not supported for external calls recorded by shared servers

Configuring a Verba cluster

In order to allow using shared servers in a Verba system, a Verba cluster needs to be configured.

Follow the steps below to configure the cluster:

Step 1 - In the Verba web interface click on **Administration > Verba Servers** and select your **Media Repository** server.

Step 2 - Click on the **Change Configuration Settings** tab.

Step 3 - Expand **Network**.

Step 4 - Configure your **Verba Cluster ID** and add your **Media Repository servers** belonging to this cluster.

Step 5 - After making your changes click on the **Save** button on top right corner of the configuration tree.

Step 6 - Follow the instruction in the yellow stripe above the configuration tree to **apply changes** to Verba services.

The screenshot shows the Verba configuration interface. On the left, the 'Server Configuration' panel is expanded to the 'Network' section. It includes fields for 'Server IP Address' (192.168.1.13), 'Verba Cluster ID' (Cluster1), and a list of 'Media Repositories' with entries like 'MR1_in_Cluster1:20111|1' and 'MR2_in_Cluster1:20111|1'. On the right, the 'Media Repositories' panel shows fields for 'Host' (MR1_in_Cluster1), 'Port' (20111), and 'Priority' (1). A 'Save' button is visible at the bottom right of the Media Repositories panel.

Step 5 - Repeat step1 - step4 on each Media Repository servers.

Configuring shared servers

Follow the steps below to add a shared server:

Step 1 - In the Verba web interface click on **Administration > Verba Servers**.

Step 2 - On the top right edge of the view, select **Add New Verba Server**.

Step 3 - Enter the **Hostname** and select the **Role** of your server.

Step 4 - Check the **Shared** checkbox. Optionally enter a Description.

Step 5 - Click on the **Save** button then follow the instruction in the yellow stripe above the configuration tree to **apply changes** to Verba services.

The screenshot shows the 'Verba Server Data' configuration form. It includes fields for 'Hostname*' (RS_in_Cluster1), 'Role*' (Recording Server), a checked 'Shared' checkbox, a 'Configuration Profile' dropdown, and a 'Description' text area containing 'This Recording Server is located (and can be configured) in Cluster1 and is running in shared mode in Cluster2.'. At the bottom, there are 'Save' and 'Delete' buttons. A footnote at the bottom left states '* Indicates required item.'

Firewall requirements

The same firewall rules apply for shared Verba servers as for normal Verba servers. On the Verba Media Repository servers, the port needs to be opened for the Verba Storage Management Service.

Please visit the integration-specific firewall configuration page for more information.

Server Certificates

The Verba system uses a public key cryptography based encryption for the communication between the Verba services. The system uses the Windows Certificate Store (WCS) for the key management and relies on industry standards such as RSA, AES, SHA.

Choosing the Certificate Authority

Besides using the domain's own CA or a 3rd-party CA, Verba provides the option for configuring the first Media Repository (or Single) server as a CA. It simplifies the installation process and the certificate management. For the installation guides see: [Install the Verba software](#)

If the Verba CA is being used, then the server certificates going to be requested by the Verba installer from the first Media Repository (or Single) server through HTTPS connection. The certificates generated by the Verba CA is a KSP certificate, and uses SHA512 for the signature algorithm, and RSA2048 for the public key.

If the domain's own CA or a 3rd-party CA has to be used, then the server certificates and the CA certificate have to be placed into the server's certificate store in advance.

Server Certificate Requirements

- Certificates must have RSA keys (2048 recommended)
- All server certificates must be signed by the same CA
- Certificates must be valid, not expired or revoked
- Certificates must have a private and a public key
- Strong private key protection must be disabled
- The private key must be exportable
- The Verba service account (LocalSystem, service user account) must have access to the CA and server certificates
- Both CSP (Crypto Service Provider) and the new generation KSP (Key Storage Provider) type certificates are supported

Server Configuration

Every Verba server and component has its own **Server Certificate** configuration. The configuration can be reached by going to the **System \ Servers** menu, selecting the server, then going to the **Change Configuration Settings** tab.

Server Certificate

Enable Advanced API Security:	<input type="checkbox"/>	Yes
Certificate Trust List:	<input type="checkbox"/>	own_ca
Server Certificate:	<input checked="" type="checkbox"/>	B263714E264CB62A6F2657712A5B68C45FF1CF2B
Verba Certificate Authority:	<input checked="" type="checkbox"/>	9D1DA643F4F4534E05A2087B39F1B5B32F94A011
Key File:	<input type="checkbox"/>	
Key File Password:	<input type="checkbox"/>	*****
Verify Trust of HTTP API Connection:	<input type="checkbox"/>	Yes
Verify Hostname of HTTP API Connection:	<input type="checkbox"/>	Yes

Setting Name	Description
--------------	-------------

Enable Advanced API Security	Sets whether the advanced API security is being used, or the legacy mode. If disabled then API ports going to use unauthenticated TCP and maintain compatibility with earlier Verba versions.
Certificate Trust List	<p>Sets the method of the verification of the server certificate of the remote peers. Accepts the following values:</p> <ul style="list-style-type: none"> • empty - No verification, all certificates going to be trusted. • "*" - All certificates going to be trusted whose CA certificate can be found in the Trusted Root Certificate Authorities folder of the WCS. • "own_ca" - All certificates going to be trusted, whose CA certificate is the same as the server's own server certificate's CA. (default setting) • list of thumbprints - All certificates going to be trusted, whose thumbprint or whose CA certificate's thumbprint is provided. <p>Alternatively, instead of using the WCS, a path to a .crt file can be also provided. In this case, all certificates going to be trusted, whose CA certificate is the same as the provided file.*</p>
Server Certificate	<p>The thumbprint of the server certificate.</p> <p>Alternatively, instead of using the WCS, a path to a .crt file can be also provided.*</p>
Verba Certificate Authority	The thumbprint of the CA certificate. Required only if the server is a CA.
Key File	If a path is provided to the Server Certificate setting, then here a path has to be provided to the corresponding .key file.* If the WCS is being used, then this setting is empty.
Key File Password	If a path is provided to the Key File setting, then the password of the key file has to be provided here.*
Verify Trust of HTTP API Connection	Set if the CA of remote peer's server certificate has to be verified in case of HTTP API connections.
Verify Hostname of HTTP API Connection	Set if the Subject (and SANs) of remote peer's server certificate has to be verified in case of HTTP API connections.

**Not recommended scenario.*

Downloading Server Certificate from the Verba CA

If Verba CA is being used, then the server certificates can be generated and downloaded using the Verba Web interface.

Step 1 - Log into the **Verba Web Interface**, and go to the **System \ Request Server Certificate** menu.

Step 2 - Provide the properties of the certificate. The subject should be the FQDN of the server which going to use the certificate.

Certificate Generation

Organization	<input type="text"/>
Organizational Unit	<input type="text"/>
Country/Region	<input type="text"/>
State/Province	<input type="text"/>
City/Locality	<input type="text"/>
Subject*	TESTRS1.VERBATEST.LOCAL
Subject Alternative Name	<input type="text"/>
Password	*****
Validity (Days)*	18250

[Generate](#)

Step 3 - Click **Generate**. The new certificate will be downloaded.

Changing the Server Certificate if Verba CA is being used

The following steps describe the procedure of changing the server certificates. This usually required, when a certificate becomes expired, or corrupted. The certificate can be downloaded from the Verba Web Interface.

Step 1 - Log into the server and go to the Start menu. Type "mmc.exe", then press enter.

Step 2 - Go to the **File / Add/Remove Snap-in...** menu.

Step 3 - From the list on the left side select **Certificates** and click on the **Add** button.

Step 4 - Select **Computer Account** then click **Next**. On the next page, select **Local Computer** then click **Finish**. In the MMC windows press **OK**.

Step 5 - Import the new .pfx file downloaded from the Verba Web Interface to the **Personal** folder.

Step 6 - Log in to the **Verba Web Interface**, and go to the **System \ Servers** menu.



Changing certificate when the server certificate is expired already

If the server certificate is expired already, then the configuration the Verba server cannot be reached through the web interface. In this case, the settings have to be updated in the registry. Update the following registry value in order to change the server certificate:

HKEY_LOCAL_MACHINE\SOFTWARE\Verba\ApiCert

For changing the CA certificate, update the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Verba\ApiCaCert

Finally, restart the Verba services.

Step 7 - Select the server from the list, then go to the **Change Configuration Settings** menu.


Step 8 - Expand the **Server Certificate** node, and update the **Server Certificate** setting.

Step 9 - Click on the



icon.

Step 10 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 **There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please click here .**

Step 11 - Changing the Server Certificate configuration also requires the **manual restart of the Verba Node Manager Agent service**. Log into the servers where required, and restart the service.

Changing the Server Certificate if the Domain or 3rd-party CA is being used

The following steps describe the procedure of changing the server certificates. This usually required, when a certificate becomes expired, corrupted, or the CA is changed.

Step 1 - Log into the server and go to the Start menu. Type "mmc.exe", then press enter.

Step 2 - Go to the **File / Add/Remove Snap-in...** menu.

Step 3 - From the list on the left side select **Certificates** and click on the **Add** button.

Step 4 - Select **Computer Account** then click **Next**. On the next page, select **Local Computer** then click **Finish**. In the MMC windows press **OK**.

Step 5 - Place the new server certificate to the **Personal \ Certificates** folder. This can be done either by importing the new .pfx file, requesting a new certificate directly from the domain's CA, or by creating a new certificate request then importing the signed .crt file.

Step 6 - If the CA also changes, then make sure that the new CA certificate can be found under the **Trusted Root Certificate Authorities** folder. If list of thumbprints or "own_ca" value is provided in the server's Certificate Trust List setting (in Verba), then the CA certificate can be also under the **Personal** folder.

Step 7 - Log in to the **Verba Web Interface**, and go to the **System \ Servers** menu.

Changing certificate when the server certificate is expired already

If the server certificate is expired already, then the configuration the Verba server cannot be reached through the web interface. In this case, the settings have to be updated in the registry. Update the following registry value in order to change the server certificate:

HKEY_LOCAL_MACHINE\SOFTWARE\Verba\ApiCert

For changing the CA certificate, update the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Verba\ApiCaCert

Finally, restart the Verba services.

Step 8 - Select the server from the list, then go to the **Change Configuration Settings** menu.

Step 9 - Expand the **Server Certificate** node, and update the **Server Certificate** setting.

Step 10 - If the CA also changes, then the **Certificate Trust List** setting has be updated on all servers if not "*" value is being used. Then new value should contain the thumbprint of the old and the new CA certificate also. After the change, the old thumbprint can be removed, or the setting can be changed to "own_ca".

Step 11 - Click on the



icon.

Step 12 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



There are tasks to be executed regarding the configuration of this Verba Server.
If you would like to execute these tasks now, please [click here](#) .

Step 13 - Changing the Server Certificate configuration also requires the **manual restart of the Verba Node Manager Agent service**. Log into the servers where required, and restart the service.

Log and Configuration Collector

The Log and Configuration Collector tool makes it possible to collect all of the log files and configuration settings in the system with a click of a button.

The tool can be accessed by navigating to the **System -> Collect Configuration and Logs** page.

The table below shows the information that can be exported from the system and from each server.

Extent	Information to be exported
System-Wide	<ul style="list-style-type: none">• License Information - Exports the information shown on the License page• System Alerts - Exports the system alerts that have been generated• Active Directory Profiles - Exports the Active Directory connection information and synchronization rules• Active Directory Synchronization Logs - Exports the logs of Active Directory Synchronizations that have been run before
Server specific settings (All)	<ul style="list-style-type: none">• Central Recording Rules (database) - Exports the recording rules (which extensions are to be recorded, recording mode, etc.)• Central Configuration (database) - Exports the configuration of the services running on the server, as stored in the database• Local Configuration (registry) - Exports the configuration of the services running on the server, as stored in the local registry of the machine• Service Status - Exports the current status of all of the installed Verba services on the server• Log Files (/log) - Exports the contents of the /log folder• Configuration Files, Recording Rules (/settings) - Exports the contents of the /settings folder• Resource Files (/resources) - Exports the contents of the /resources folder• Dump Files (/bin) - Exports the contents of the /bin folder
Server Specific settings (Media Repository)	<ul style="list-style-type: none">• Central Recording Rules (database) - Exports the recording rules (which extensions are to be recorded, recording mode, etc.)• Central Configuration (database) - Exports the configuration of the services running on the server, as stored in the database• Local Configuration (registry) - Exports the configuration of the services running on the server, as stored in the local registry of the machine• Service Status - Exports the current status of all of the installed Verba services on the server• Log Files (/log) - Exports the contents of the /log folder• Configuration Files, Recording Rules (/settings) - Exports the contents of the /settings folder• Resource Files (/resources) - Exports the contents of the /resources folder• Dump Files (/bin) - Exports the contents of the /bin folder• Web Application Version - Web Application version• Tomcat Configuration Files (/tomcat/conf) - Exports the contents of the /tomcat/conf folder• Tomcat Log Files (/tomcat/log) - Exports the contents of the /tomcat/log folder

After selecting the data that should be exported, click on the **Start** button at the top-left corner of the page.

The Web Application collects the necessary information and shows an **In Progress** sign until it finishes.

Once all the required data is available, it can be **downloaded** as a compressed (zip) file as shown in the screenshot below. A **ZIP File Password** can be entered which will make the compressed file inaccessible to non-authorized parties.

Collect Configuration and Logs

Collection finished in 0 minute(s) (started by Verba Administrator (Administrator)). 3 / 3 server(s) completed successfully.
The files are available on TESTMR4

ZIP File Password [Download \(24.57 MB\)](#) [Delete Files](#)

▼ System-Wide **Done**

License Information	Done
System Alerts	Done
Active Directory Profiles	Done
Active Directory Synchronization Logs	Done

▼ TESTMR4 (Media Repository) **Done**

Central Recording Rules (database)	Done	
Central Configuration (database)	Done	
Local Configuration (registry)	Done	
Service Status	Done	
Log Files (/log)	Done	(20655.75 KB)
Configuration Files, Recording Rules (/settings)	Done	(2.01 KB)
Resource Files (/resources)	Done	(1054.97 KB)
Dump Files (/bin)	Done	(1372.19 KB)
Web Application Version	Done	(3.04 KB)
Tomcat Configuration Files (/tomcat/conf)	Done	(28.73 KB)
Tomcat Log Files (/tomcat/log)	Done	(13.49 KB)

▶ TESTRS1 (Recording Server) **Done**

ZIP File Password [Download \(24.57 MB\)](#) [Delete Files](#)

- ✔ To run a new collection task that contains the latest information, the current files need to be deleted with the **Delete Files** button. A new collection task can be started after.

Metadata templates

Verba metadata templates are powerful tools for attaching text-based comments to recorded calls. A metadata template consists of metadata template fields. Each metadata template field defines the appearance of a given metadata field (e.g. a selection list type field contains predefined items, which can be selected by a user).

The system contains multiple built-in templates which are used by specific integrations automatically.



The built-in templates should not be removed or changed (other than appearance settings), because it will break the related integrations.

The metadata templates are accessible only when the template is associated with the users' group. Each group has a metadata template and every user is associated with at least one group. This way ensures that each user is able to use at least one metadata template.

There is a default metadata template to provide basic functions for the system:

- Private field: enables users to flag a call as private and prevent other users, who were not part of the call, from listening to the call or downloading the media file
- Important field: enables users to flag a call as important and list it from a dedicated menu.
- IP Phone Service XML List: provides a selection list type comment field to use in the Verba XML Service for call Tagging. e.g. "For Review", "Threat", "Customer Dispute" etc.

The default metadata template fields cannot be deleted and are automatically added to each new metadata template.

A default metadata template exists to provide a metadata template for the primary group.

- [Find and list metadata templates](#)
- [Metadata template details](#)
- [Metadata template fields](#)

Find and list metadata templates

Metadata templates are available under **System | Metadata Templates**.

Find and List Metadata Templates

[Add New Metadata Template](#)
[Refresh List](#)



15 items found, displaying all items.

Id ↕	Name ↕	Type ↕	Groups ↕
16	Verint Template	Verint	Default
15	Scribe	Scribe	Default
14	BT ITS/PSI Template	BT ITS/PSI	Default
13	Voice Quality Template	Voice Quality	Default
12	IPTrade Template	IPTrade	Default
11	Lync (ComputerTalk ICE) Template	Lync (ComputerTalk ICE)	Default
10	Genesys Template	Genesys	
9	IPC Unigy Template	IPC Unigy	Default
8	Cloud9 Template	Cloud9	Default

Metadata template details

Creating a metadata template

You can create a new metadata template by clicking on the **Add New Metadata Template** link on the **System / MetadataTemplates** page. After selecting the link, the following page is opened.

Metadata Template Configuration

[Add New Metadata Template Field](#)
[Add New Metadata Template](#)
[Back to Previous Metadata Template List](#)

Metadata Template Data Metadata Template Fields ?

Metadata Template Data

Id

Name*

Type*

Group Association

Default


Scribe Group

>>

<<

Save

The following table describes the available fields:

Field Name	Description	Requirements
Name	The name of the metadata template.	Required field. Minimum length: 3 Maximum length: 32 Must be unique in the system. Reserved name: Default
Type	The type of the template. The system has several built-in template types for various integrations. For custom fields, select Standard.	Required field.
Groups Association	Users can only access the template if the template is associated with one or more groups related to the users. You can select one or more groups from the left column and by clicking on the  button, the group can be associated with the template.	-

After filling out the form, press the **Save** button to save metadata template data into the database.

Modifying and deleting metadata templates

To edit a metadata template entry, you have to click on the desired row of the list showing registered metadata templates. After clicking on the row, a new page opens automatically.

To make changes effective, press the **Save** button. All requirements, which are described in the previous part, have to be met.

You can delete the metadata template by clicking on the **Delete** button. Metadata templates can only be deleted if they do not belong to a group and nobody has attached a comment to a recorded conversation.

Metadata template fields

Metadata template fields are essential components of the metadata templates. The list of metadata template fields for a given metadata template can be listed by clicking on the **Metadata Template Fields** tab on the **Metadata Template Configuration** page.

Metadata Template Configuration

[Add New Metadata Template Field](#)
[Add New Metadata Template](#)
[Back to Previous Metadata Template List](#)

Metadata Template: Scribe

Metadata Template Data	Metadata Template Fields
------------------------	--------------------------

4 items found, displaying all items.

Display Name	Enable API Access	Editable	Private	Type
Quotes	Yes	No	No	Text
Product Classes	Yes	No	No	Text
Key Phrases	Yes	No	No	Text
Key Terms	Yes	No	No	Text

4 items found, displaying all items.

Export options: [Excel](#) | [CSV](#) | [PDF](#)

Creating a metadata template field

You can create a new metadata template field by clicking on the **Add New Metadata Template Field** link on the **Metadata Template Configuration** page. After selecting the link, the following page is opened.

Metadata Template Field Configuration

[Add New Metadata Template Field](#)
[Back to Previous Metadata Template Field List](#)

Metadata Template: Scribe

Metadata Template Field Data

Id

Display Name*

Field Identifier

Property Id

Enable API Access

Editable

Private

Type*

Appearance*

Maximum Number of Characters on the Search Screen

Display in New Row(s) Instead of in a Column

[Save](#)

The following table describes the available fields:

Field	Description	Requirements
Display Name	The displayed name of the custom field variable. It is displayed on the web interface for the users.	Required field Minimum length: 3 Maximum length: 128
Field Identifier	Unique identifier of the field used by external applications to refer to the field through the API.	Required field Minimum length: 3 Maximum length: 128 Must be unique in the system The field cannot contain special characters and spaces, only alphanumeric characters including underscore (_) or dash (-) can be used.
Property Id	Unique identifier of the property mapped to the metadata field. The built-in templates for the various integration use this identifier to map the source data to a metadata field.	-
Enable API Access	Indicates whether external applications can access/write this field or not. If you want to insert information into this field by an external application, this option has to be enabled.	-
Editable	If enabled, users can edit/modify the content of the field on the web interface.	-
Private	By default, all custom fields are public, which means that the content of the field is available for anyone in the system, who has access to the call itself. If the private flag is enabled on the custom field, then only the user, which filled in the data in the field can edit the content of the field. API driven fields cannot be private.	-
Type	Type of the custom field variable. The following valid values apply: <ul style="list-style-type: none"> • Text • Numeric • Date • Boolean <p>Note: all values are stored as string variables in the database to avoid discrepancies and incompatibility, however in order to provide sophisticated search controls and operators, the system has to know the type of the data inserted into the custom field variable. E.g. for numerical fields, users can use "Greater Then" or "Less Then" operators.</p>	-
Appearance	Defines the way how the custom field is displayed on the user interface. The following valid values apply: <ul style="list-style-type: none"> • Single-line Input Box • Multi-line Input Box • Selection List • CheckBox. <p>The type of the custom field defines the available appearance options.</p> <ul style="list-style-type: none"> • Numeric: Single-line Input Box, Selection List • Text: Single-line Input Box, Multi-line Input Box, Selection List • Date: Single-line Input Box • Boolean: CheckBox 	-

Maximum Number of Characters on the Search Screen	Defines the maximum number of characters displayed on the search screen. If the value is longer than this value, the system will display '...' at the end of the text.	
Display in New Row (s) Instead of in a Column	By default, the field is displayed as a new column on the search screen (when the field is added to the conversation list layout). By enabling this option, the field will be displayed as a new line instead of a column. This is especially useful when the field can contain long text.	
Display Values in One Row	When enabled, the multiple values in the field are displayed as a single line separated with ',' (comma) instead of displaying the values in new lines.	
Mapped ID /Name Values	Defines if the items for Selection List type fields should be displayed based on a matching ID.	
Items	<p>If the appearance is set to Selection List, the list of pre-configured items can be defined, which are automatically offered for the user. The items have to be added separated by ';' (semicolon).</p> <p>If the Mapped ID/Name Values setting is enabled, both the ID and the Name have to be defined. When a value is added to the field as an ID, the system will look for the matching Name attribute, which will be used for displaying the value.</p>	

After filling out the form, press the **Save** button to save metadata template field data in the database.

Modifying and deleting metadata template fields

To edit a metadata template field entry, you have to click on the desired row of the table showing registered metadata templates. After clicking on the row, a new page opens automatically.

To make changes effective, push the **Save** button. All conditions, which are described in the previous part, have to be met.

You can delete the metadata template field by clicking on the **Delete** button. Metadata Template Fields can only be deleted if they have not been attached to a recorded call and are not part of a default template field.

Labels

The Labeling system allows users with sufficient rights to create labels that can be applied to conversations to distinguish and group them together in a highly customizable manner.

Once created, labels can be applied to conversations to tag them in the search result list, thus making it considerably easier to search for them.

Multiple labels can be applied to the same conversation. Labeling is deeply integrated with user access control and can be used to manage the accessibility of the tagged conversations for specific users and groups.

Labels can be applied to conversations manually from the conversation search page or automatically based on configurable criteria.

The system also includes the option to place tagged calls under Legal Hold to make sure the selected conversations cannot be deleted.

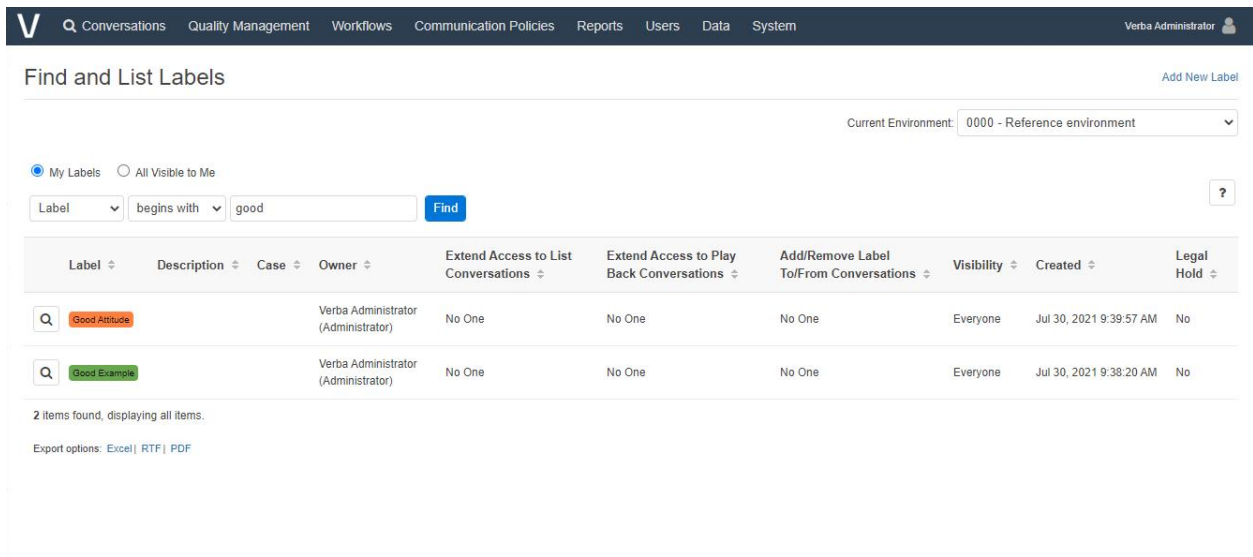
The following articles contain the guides to setting up and using the labeling system.

- [Managing Labels](#)
- [Automatic labeling](#)
- [Legal Hold](#)

Managing Labels

This article provides a guide for managing labels.

To access label management open the Verba Web interface and select **Data > Labels > Manage Labels**.



A list is displayed showing the labels that were previously configured. Clicking the **magnifying glass icon** next to a label takes you to the Search page with an automatically applied filter that lets you **search for conversations that have been tagged with that label**.

On the top of the page, there is an option to display labels created by your user or labels visible to your user. There is also a 'Find' interface to allow you to find the label you would like to manage faster.

Creating new labels

On the Find and List Labels page click the **Add New Label** button. On the Label configuration page you have the following options.

Verba Administrator

Conversations Quality Management Workflows Communication Policies Reports Users Data System

Label Configuration

Good Example

Add New Label
Back to Previous Label List


?

▼ Label

Environment* 0000 - Reference environment

ID* 120

Label* Good Example


Color* 

Description

Owner* Verba Administrator (Administrator)

Show Number of Conversations

▼ Access / Share

Access / Share Expires  Never Expires

Override "Unable to Access Conversations Older than" Permission

Extend Access to List Conversations No One Select Users Everyone

Extend Access to Play Back Conversations No One Select Users Everyone

Add/Remove Label To/From Conversations Owner Select Users Everyone

Visibility Owner Select Users Everyone

▼ Legal Hold

Legal Hold Details [Enable Legal Hold](#)

Release from Legal Hold needs the approval of a user who has Approve Release from Legal Hold permission.

Configuration option	Description
Label	The name of the label. This will appear on the tag showing next to each conversation the label is applied to. This is a mandatory field.
Color	Select a color for the label. This will be the background color of the tag showing next to each conversation the label is applied to. This is a mandatory field.
Description	Provide an optional description for the label that appears in the label list.
Access/Share Expires	This setting relates to the access extension settings configurable below. If a date is set, then the access extension will only be in effect for the selected users till this date.
Override "Unable to Access Conversations Older than" Permission	Enable this checkbox if the access extension settings should override the Unable to Access Conversations Older than setting that is configured in the user roles for the affected users.
Extend Access to List Conversations	This option allows you to extend access to list conversations tagged with the label. <ul style="list-style-type: none"> No One: Access to the conversations tagged with this label does not change, meaning everyone who had access to the conversation before will retain it, but no additional users are given access. Select Users: selecting this option will allow you to extend access to the conversation tagged with this label to additional users and/or groups. Everyone: selecting this option will grant access to the conversations tagged with this label to every Verba in the system.

Extend Access to Play Back Conversations	<p>This option allows you to extend access to conversations tagged with the label.</p> <ul style="list-style-type: none"> • No One: Access to the conversations tagged with this label does not change, meaning everyone who had access to the conversation before will retain it, but no additional users are given access. • Select Users: selecting this option will allow you to extend access to the conversation tagged with this label to additional users and/or groups. • Everyone: selecting this option will grant access to the conversations tagged with this label to every Verba in the system.
Add/Remove Label to/From Conversations	<p>This option controls which users can add and remove the label to/from conversations</p> <ul style="list-style-type: none"> • Owner: only the creator of the label can apply or remove this label to/from conversations • Select users: the selected users and the members of the selected groups will be able to apply or remove this label to/from conversations • Everyone: every user in the system will be able to apply and remove this label to/from conversations
Visibility	<p>This option allows you to control which users have visibility of a specific label.</p> <ul style="list-style-type: none"> • Owner: only the creator of the label has visibility of this label within Conversation Search and other application functionality that use Labels • Select Users: selecting this grant visibility of this specific label within Conversation Search and other application functionality that use Labels. Visibility of this label is extended to additional users and/or groups. • Everyone: selecting this grant visibility of this specific label within Conversation Search and other application functionality that use Labels. Visibility of this label is extended to every user in the system.
Legal Hold	<p>This option allows you to enable Legal Hold for conversations tagged with the label. For more information on Legal Hold, see the corresponding article.</p>

Click **Save** to save the label. After the label has been created the users who were granted access to it can apply or remove it to/from conversations they have access to.

Existing Label modification

To edit a label's settings, select it from the Label list. In addition to the adjustable settings covered above, the owner of the label is displayed, along with a button to query the database for the number of conversations the label is currently applied to ('Show number of Conversations').

If the label is not marked as Legal Hold, the **Delete** button can be used to delete the label. When a label is deleted, it will be **removed from every conversation**, but the conversations themselves will not be deleted.

You can use the **Search using this label** button to open the Search interface and automatically apply a filter to search for conversations with this label.

At the bottom of the screen you can find some additional properties for the label (creation and modification dates) and you can also view a detailed change history by clicking the **View Change History** link.

The **Authorization Requests** section shows all events when access was requested for this specific label.

Click the **Save** button to save any changes you made.

Label Visibility

AVAILABLE IN 9.6.12 AND LATER

It is possible to control, and restrict which users have visibility of a specific label. As an example, this can be used to control whether all users, or selected users can see a specific label within the application, an example would be to restrict visibility to a Label that identifies 'non-compliance' or 'legal hold' to a subset of users.

Automatic labeling

This article provides a guide to set up and manage automatic labeling.

Automatic labeling allows you to create labeling rules that apply and / or remove a configurable set of layers to calls selected by the specified criteria.

Creating labeling rules

To set up and manage automatic labeling rules open the Verba Web interface and select Labels > Automatic Labeling.

A list of labeling rules is displayed showing the previously created rules.

Find and List Label Rules

[Add New Label Rule](#)
[Show Disabled Rules](#)

My Labeling Rules All Labeling Rules

Name begins with

?

Enabled	Name	Special Filter	Created By	ID
Yes	Add Compliance Review Label		Verba Administrator (Administrator)	14
Yes	Adding Participants		Verba Administrator (Administrator)	11
Yes	Domain Terms for Gifts		Verba Administrator (Administrator)	10
Yes	TEST Transcription Auto Label		Verba Administrator (Administrator)	9
Yes	label_for_luke		Verba Demo Account (demo)	8
Yes	Darkside		Verba Administrator (Administrator)	7
Yes	Problem_text		Verba Demo Account (demo)	6
Yes	Customer Call Quality Issue		Verba Administrator (Administrator)	3
Yes	Compliance risk	Speech	Verba Administrator (Administrator)	2
Yes	20min+ calls in the contact center		Verba Administrator (Administrator)	1

10 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

To create a new rule, click the 'Add New Label Rule' button. On the rule configuration page, you have the following options:

Label Rule Configuration

[Add New Label Rule](#)
[Back to Previous Page](#)

Label Rule Data
SQL Query
?

Label Rule Data

Name*

Enabled*

Add Labels

- PC - FX Options
- PC - Gas Options
- PC - Gilts
- PC - Interest Rate Swaps
- PC - Middle Distillates
- PC - Sugar
- PC - Swaptions

>>

<<

Remove Labels

- PC - Core Equities, Research and Earnings
- PC - Corporate Bonds
- PC - Crude Options
- PC - European Government Bonds
- PC - Fuel Oil
- PC - FX Forwards

>>

<<

Notifications

Send to recorded user

Send to all participating users

Send to all participating email addresses

Send email to

Filtering Criteria

Conversation Detail Fields

+

[Save](#)

* Indicates required item.


Configuration option	Description
Name	The name of the rule. This is a mandatory field.
Enabled	The rule is only in operation if this field is set to 'Yes'
Add Labels	Choose the labels you want the rule to apply by selecting them in the list on the left then moving them to the list on the right using the '>>' button.
Remove labels	Choose the labels you want the rule to remove by selecting them in the list on the left then moving them to the list on the right using the '>>' button.
Send to recorded user	Enable this to send an email notification to the recorded user of the conversations when the rule is executed on them
Send to all participating users	Enable this to send an email notification to all of the participating users of the conversations when the rule is executed on them
Send to all participating email addresses	
Send email to	Sends an email to the given email addresses in the list.


Conversation Detail Fields	<p>Use this interface to specify filters for selecting calls to apply the rule to. Click the '+' button to add a new filter, select the call detail record field you wish to base it on, then add your criteria. You can add more filters by repeating the previous step.</p> <p>To delete a filter, click the trash icon next to it.</p>
----------------------------	---

Filtering Criteria

The table below summarizes the available conversation details fields which can be configured as a filter for the Automatic Label Rule.

Category	Field	Description
Participants	From	The number of the caller party in the conversation
	From Info	The number of the called party in the conversation
	From (digits)	The number of digits in the phone number of the initiator of the conversation
	From Device ID	The Device ID of the initiator of the conversation
	From IP	The IP address of the caller party in the conversation
	To	The name of the caller party in the conversation
	To Info	The name of the called party in the conversation
	To (digits)	The number of digits in the phone number of the target of the conversation
	To Device ID	The Device ID of the target of the conversation
	To IP	The IP address of the called party in the conversation
	Both To or From	The number of any party participating in the conversation
	Both To or From Info	The name of any party participating in the conversation
	Dialed Number	The original dialed number
	User	The user associated with the conversation based on the extension configuration
	User Location	The location of the user, defined in the user configuration
	Extension	The extension numbers in a conversation, a selection list of the configured extensions, otherwise similar to the 'Any party number' field below
Group	The group where a conversation belongs to based on the users associated with the conversations	
User ID	The User/Agent/Trader ID obtained from the recorded platform	
Details	Start Time (UTC)	The start time of the conversation in UTC timezone
	Recent Than	<p>Only conversations selected where the start time is recent than the defined value.</p> <p>Make sure it is not used with a recurring schedule, otherwise conversations can be skipped if the defined value is close to the recurring period.</p>
	Direction	The direction of the conversation (e.g. internal, inbound, outbound, etc.)
	End Cause	The end cause of the conversation (e.g. normal, hold, transfer, etc.)

Duration Interval	The length of the conversation
Conversation Type	The type of conversation. Available options: <ul style="list-style-type: none"> • Voice • Video • Instant Messaging • SMS • Desktop Screen • Screen & Application Share (Lync/SfB) • Whiteboard (Lync/SfB) • Poll / Q&A (Lync/SfB) • File Share (Lync/SfB)
Forward Reason	The forward reason for the conversation (e.g. forwarded, transferred, team call, delegated, etc.)
On-demand	Defines whether a call was recorded as on-demand
Marked for recording	Defines whether an on-demand conversation was marked for recording
Protected	Defines whether the conversation is protected
Case	The cases containing the conversation
Encrypted with Certificate	The certificate used to encrypt the conversation
Signed with Certificate	The certificate used to sign the conversation
Quality Management Scorecard exits	Checks if there is a Quality Management Scorecard assigned to the conversation
Analytics	<p>Text Search</p> <p>Full-text search in instant messages, SMS and voice transcriptions:</p> <ul style="list-style-type: none"> • All of these phrases: the search will return conversations where all phrases are matched • Any of these phrases: the search will return conversations where at least one phrase is matched • None of these phrases: the search will return conversations where none of the phrases are matched <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Integrations using the advanced data model for instant messages (e.g. Microsoft Teams) do not support automatic labeling.</p> </div>

	Word Hit Count	Count occurrences of words using full-text search in instant messages, SMS and voice transcriptions, where: <ul style="list-style-type: none"> • Word(s) (Comma-Separated): comma-separated lists of words used for counting • Occurrences: minimum and maximum occurrence of the word defined <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Integrations using the advanced data model for instant messages (e.g. Microsoft Teams) do not support automatic labeling. </div>
	Marker	Full-text search in comments added to markers: <ul style="list-style-type: none"> • Marked as all of these: the search will return conversations where all phrases are matched • Marked as any of these: the search will return conversations where at least one phrase is matched • Not marked as any of these: the search will return conversations where none of the phrases are matched
	Silence ratio	The silence ratio in a conversation
	Talkover ratio	The talkover ratio of the conversation
	Longest Silence	The longest silence present in a conversation
Technical	Recording Server	The hostname of the server that recorded the conversation
	Media file name	The name of the stored media file
	Storage target	The current storage location of the media file(s)
	Source Platform	Defines which telephony / unified communications system the conversation was recorded on (Cisco, Sfb, Avaya, etc.)
	Secondary	Defines whether the conversation is recorded on a server marked as secondary (using 2N / duplicate recording)
	CDR/Media Record	Defines whether the conversation is a Standard, CDR-Only or Media-Only record. CDR-Only and Media-Only records are used for trader voice recording.
	Elapsed Time Since Transcoding (UTC)	The time elapsed since transcoding in UTC timezone
	Time of Transcode (UTC)	The date and time of transcoding in UTC timezone
Metadata Fields	Custom Metadata Fields	Custom metadata fields configured in the system, the list of available fields might vary depending on the integration configured and the metadata templates added

Editing existing labeling rules

To edit an existing rule, select it from the rule list then modify any of the options described in the previous section. To apply the changes, click Save.

You can use the 'Delete' button to delete the rule.

At the bottom of the screen you can find some additional properties for the rule (creation and modification dates) and you can also view a detailed change history by clicking the 'View Change History' link.

Customizing notification emails

The email notification template can be configured in the Verba Labeling Processor service configuration. It can be found in the server configuration under the **Label Processing** node.

The available variables are the following:

Variable	Description
\${RULE_NAME}	Name of the labeling rule
\${LABELS}	List of the labels added / removed
\${LINK}	Link to the recording
\${DISPLAY_NAME}	Notification target name
\${EMAIL_ADDRESS}	Notification target email address
\${FROM_ADDRESS}	The line number / sip address of the caller participant
\${FROM_NAME}	The name of the caller participant
\${TO_ADDRESS}	The line number / sip address of the called participant
\${TO_NAME}	The name of the called participant
\${START_DATETIME}	The start time of the call
\${END_DATETIME}	The end time of the call

Audit logs

The system creates audit logs for the following aspects of the system:

	Events / Content	Format / Access	Location
User actions on web interface	All user actions are logged with related metadata such as login, playback, search, configuration change and 100+ other events. Audit log for user related events Searching a call playback event	<ul style="list-style-type: none">• Search interface at System / Audit Log page• Reports• Dashboard widget	Verba SQL Server
Data retention policies	All storage policy actions are logged where each row represents a single conversation record in the audit log file with related information on the action. Customer Identification Data (CID) is not logged. Data management policy audit log	<ul style="list-style-type: none">• CSV Files	Verba server which executed the policy
Data retention policies	All storage policy actions are logged for each conversation record affected by the policy. Conversation audit log	<ul style="list-style-type: none">• View interface at Conversation Details / View Conversations Audit Log page	Verba SQL Server
Disposal log	Summarized information of deletions Disposal audit log	<ul style="list-style-type: none">• Reports	Verba SQL Server
Communication policies	All communication policy actions are logged with information about disclaimers were sent, when session and content blocking rules were used, notifications sent, etc. Communication Policy Audit Log	<ul style="list-style-type: none">• Search interface at Communication Policies / Audit Log page• Reports	Verba SQL Server

Audit log for user related events

This audit log contains all events related to user actions including login, logout, playback, configuration change, etc. The log is stored in the SQL database. The log cannot be altered or deleted through the user interface.

The administrator and the system administrators can access the event log by clicking on the **System / Audit Log** menu item. An event log search page appears, where the user can define event log searching criteria.

You can define as many search criteria as you want. The search fields are connected with logical AND connections. Therefore only those calls that meet all of the search criteria will be listed.

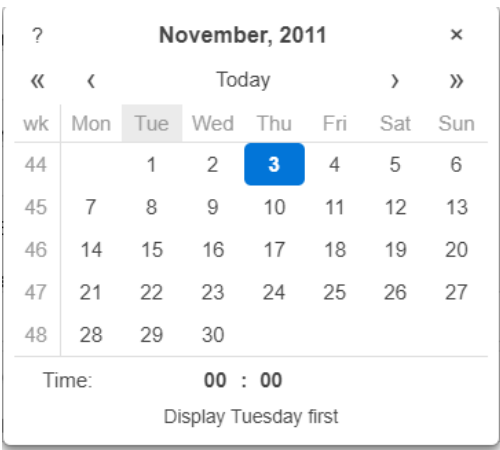
Step 1 Select the desired field into the input box on the left side of the field control.

Step 2 Press the >> button to add the criteria to the search query.

Step 3 Repeat the steps between 2 and 3 to add more criteria.

(Optional) You can remove a previously added criteria by selecting the desired criteria on the right pane of the field control and pressing the << button.


The following table describes search fields:

Name	Description
Query Interval	<p>The date and time of the event.</p>  <p>Selecting a date and time value is easy with this tool:</p> <p>Date selection:</p> <ul style="list-style-type: none">• Use the <<, >> buttons to select the year• Use the <, > buttons to select the month• Click and hold the mouse button on any of the above buttons for faster selection <p>Time selection:</p> <ul style="list-style-type: none">• Click on any of the time parts to increase the value• or Shift-click to decrease the value• or click and drag for faster selection
Event	The list contains all available events, which had happened.

User

The list contains all configured users in the Verba database.

Find and List Audit Log

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

Timestamp: Event Type:

User(s):

User Name (Login) ⌵	Event ⌵	Timestamp ⌵
▼ Verba Administrator (Administrator)	Insert Group	Oct 16, 2017 12:05:02 PM

Log ID: 500806

Metadata Templates:

Added: Default

Group Name:

Test

1 item found.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Searching a call playback event

In order to use the Verba event log to find out detailed information about a user event, just perform the following steps:

- Step 1** Login to the Verba user interface.
- Step 2** Select the System / Event log menu item.
- Step 3** Select the date/time interval for the event.
- Step 4** Select the desired event type (e.g. Playback in this case).
- Step 5** Select the desired user.
- Step 6** Click the Search button. The event log list will be displayed.
- Step 7** Select the displayed log entry and the call detail page will appear.
- Step 8** Click on the display row and the given call detail page is loaded.

Conversation audit log

The conversation audit log contains all events related to a specific conversation including both user actions (playback, download, etc.) and data management policy actions (upload, archive, export, etc.).

The administrator and/or the system administrators can access the **Conversation Audit Logs** upon initiating a Search on a conversation and opening the **Conversation Details** screen.

Conversation Details

View Conversation Audit Log
Share/Publish the conversation
Close

▼ Conversation Participants

Phone Number	Name	User	Role	Start Time	End Time	Duration	End Cause
2026		Verba Administrator (Administrator)	Caller	2017 Sep 26 14:22:07	2017 Sep 26 14:22:50	00:00:43	Normal
12013			Called	2017 Sep 26 14:22:07	2017 Sep 26 14:22:50	00:00:43	Normal

▼ Conversation Details Data

Start Time	Sep 26, 2017 2:22:07 PM	End Time	Sep 26, 2017 2:22:50 PM
Duration	00:00:43	Direction	Undefined
From	2026	To	12013
From Info		To Info	
Verba From Party Name	Verba Administrator	Verba To Party Name	
Conversation Identifier	4f5976c5-a2b5-11e7-80e0-00155d001c29	Recording Server	TESTMR1.VERBATEST.LOCAL
From IP	10.4.1.20	To IP	
From Proxy IP		To Proxy IP	
Audio codec	G.711 u-law 8kHz	Video Codec	
Archived	Yes	Import Source	
Source Platform	Cisco Network Based	Forward Reason	
Conversation Type	Voice	File format	WAVE XML
End Cause	Normal	Data Management Events	Calculate
Storage Target		Delete after End of Retention	No
End of Retention		Technical Identifier	17113950
Platform Conversation ID	2017092612-17113950	Talkover Ratio	
Silence Ratio			

Click on the **View Conversation Audit Logs** link on the top right corner of the **Conversation Details** window. The following picture shows a sample audit log:

Conversation Audit Log Close

4f5976c5-a2b5-11e7-80e0-00155d001c29

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

Event Date	Event	User / Policy	Details
Sep 29, 2017 10:33:23 AM	Archive in DB	archive-one-call (5)	
Sep 29, 2017 10:29:50 AM	Download	Verba Administrator (Administrator)	

2 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

The log can be exported into Excel, RTF and PDF formats for further use.

Multitenancy

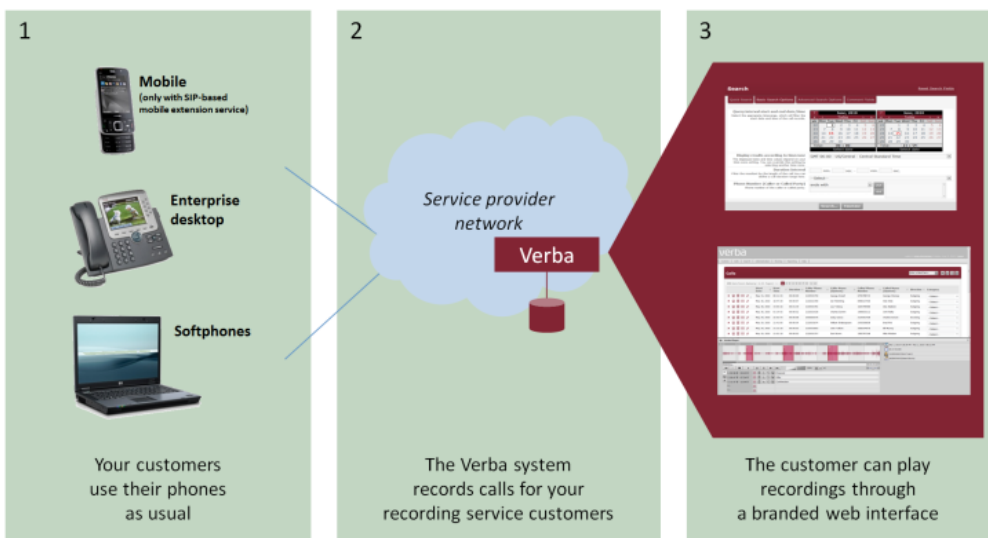
Call Recording as a Service

With the Verba Recording System Service Provider edition you can start providing your hosted Unified Communications customers call recording solutions from the "cloud".

Depending on the network scenario you can offer recording without placing recording equipment at customer sites.

This solution is simple which enables the following:

1. Your customers can make regular phone calls in the usual manner
2. The Verba Recording System Service Provider edition servers are recording calls in your data center
3. Your customers access recordings through a secure web interface



Multi-tenancy and user administration

The Verba Recording System Service Provider edition provides support for multiple "tenants" within the same recording system.

Using this, multiple organizations can be hosted on a single system and all organizations can view a complete solution customized for their needs:

- Multi-tenancy separates customers, while providing with a full feature set
- Every customer sees "their own call recording system"
- Saves servers, which drives operational costs down

This guide covers:

- [Configuring Verba for Multitenancy](#)
- [Creating a new Environment](#)
- [Adding a user to an Environment](#)
- [Adding an extension to an Environment](#)
- [Environment login](#)
- [Searching calls in different Environments](#)
- [Managing Data Retention in Environments](#)
- [Multi-tenant License Allocation](#)

Further service provider features

The Service Provider edition provides advanced capabilities designed for telecom companies:

- **User Interface Branding** – see [Branding and customization](#)
- **Single Sign-On API** - see [HTTP Single Sign-On API](#)
- **SNMP Alerts** - see [SNMP Trap OIDs](#)
- **SAN/NAS storage management** - see [Data management](#)
- **SOAP Provisioning API** - see [Provisioning API \(8v5 old\)](#)

Configuring Verba for Multitenancy

Enabling the Multi-tenanted mode will allow creating multiple isolated logical environments while using a single Verba instance and its' supporting infrastructure.

Configuring Multitenancy

Step 1 - In the Verba Web Interface, go to **System > Servers > Select your Verba Server**. (Alternatively, if you have multiple servers with the same role, the **System > Configuration Profiles** option also can be used)

Step 2 - Click on the **Change Configuration Settings** tab.

Step 3 - Expand the **System** node

Step 4 - Set the Cisco **Multi-Tenant Mode** to **Yes**.

System


API Connection

Server IPv4 Address:	<input checked="" type="checkbox"/>	10.0.16.6
Server S-NAT/Public IPv4 Address:	<input type="checkbox"/>	
Server IPv6 Address:	<input type="checkbox"/>	
Server S-NAT/Public IPv6 Address:	<input type="checkbox"/>	
Verba Cluster ID:	<input type="checkbox"/>	
Media Repositories:	<input type="checkbox"/>	+
Multi-Tenant Mode:	<input checked="" type="checkbox"/>	Yes
Tenant-Based License Allocation:	<input type="checkbox"/>	No

Step 5 - Click **Save**.

Step 6 - Repeat the steps for all the Verba servers or all active configuration profiles.

Step 7 - A notification banner will appear on the top. Select the **click here** link so that you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#) .

Creating a new Environment

To create a new environment in your Verba multi-tenant system, you have to login the '0000' default environment. This tenant is the main configuration part of a multi-tenant system.

The environment management page is under the '**System\Environments**', here you can create and manage the environments.

Find and List Environments

[Add New Environment](#)

Environment ID (EID) begins with

Environment ID (EID) ⇅	Environment Name (Short) ⇅	Environment Name ⇅
0000	Ref.	Reference environment
0001	Contoso	Contoso
0002	VFC	Verint Financial Compliance

3 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

On the top right corner of this page you will find the '**Add new environment**' link. Click on this and you will see the following form, where you can compile a new environment:

Environment Configuration

Verint Financial Compliance (0002)

[Add New Environment](#)
[Back to Previous Environment List](#)

[Environment Data](#)
[Assigned Extension Ranges](#)
[Assigned IP Ranges](#)
[Teams](#)

Environment Data

Environment ID (EID)

Environment Name

Environment Name (Short)

Valid From

Valid Until

CUCM Partitions

HelpDesk URL

User Count Limit

Group Count Limit

Extension Count Limit

Always On Recording Mode Limit

On Demand (Full) Recording Mode Limit

Controlled Recording Mode Limit

Permit XMLApp Access

Permit "Click2Dial"

Web Session Count Limit

Page Size (Row Count)

Send Emails From

Enable SMTP Authentication

SMTP Password

SMTP Server

Maximum Number of Rows per User in the Ondemand Conversations Buffer

Maximum Age of a Conversation in the Ondemand Conversations Buffer (hours)

[Save](#)

The following table describes the available fields:

Field Name	Description	Requirements
Environment ID (EID)	This ID represents the environment in Verba. This is a unique ID which required at administration.	Required field Unique 4 digit alphanumerical string Max length: 4 characters
Environment Name	Full name of the environment	Required field
Environment Name (short)	Short name of the environment	Required field

Logo to display	<p>Optional logo image can be attached to an environment. The logo image will be displayed in the header of Verba Web Application for every user in the environment. The logo will be also displayed in report headers generated by environment members.</p> <p>In order to select a logo image, press the Choose Logo button. In the open window, you can see the uploaded logo images. Simply click on the name of the file in the first column to select an image.</p>	-
Valid From	<p>Start date of the validation for the environment. 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 an environment. If a call with a phone number, which is mapped to an environment is recorded, but the Valid From date is later than the start date of the call, the call will not be associated to the environment.</p>	Required field
Valid Until	<p>End date of the validation for the environment. 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 an environment. If a call with a phone number, which is mapped to an environment is recorded, but the Valid Until date is earlier than the start date of the call, the call will not be associated to the environment.</p> <p>If the field is blank the environment will not expire.</p>	Required field
CUCM Partitions	<p>A list of CUCM partitions which enables the system to assign calls to configured tenants, and support non-unique recorded numbers across the tenants / partitions.</p>	-
User Count Limit	<p>The number of maximum users of the environment.</p>	-
Group Count Limit	<p>The number of maximum groups of the environment.</p>	-
Extension Count Limit	<p>The number of maximum extensions of the environment.</p>	-
Always on Recording Mode Limit	<p>The number of maximum Always on Recording Mode users of the environment.</p>	-
On Demand Recording Mode limit	<p>The number of maximum On Demand Recording Mode users of the environment.</p>	-
Controlled Recording Mode Limit	<p>The number of maximum Controlled Recording Mode users of the environment.</p>	-
Web Session Count Limit	<p>The number of simultaneous connections to the web interface.</p>	-
SMTP options	<p>You can add your own SMTP service to send system alert, report to the environment users. (Verba has a default built-in SMTP service)</p>	-

Adding a user to an Environment

Creating a new user account in Verba multi-tenant environment has two possibilities:

- Create a user in the default environment to the relevant environment
- Login to the desired extension with a user with full user rights and create the user account 'inside' the environment

The **first option** is a global solution of adding users to Verba multi-tenant system.

To create the user in default environment, login the default, '0000', environment with the administrator user.

Under '**Administration/Users**' you can find on the top right corner a drop down menu, the '**Current Environment**' menu. Here you can select the relevant environment and click the '**Add New User**' link above.

Find and List Users [Add New User](#)

Current Environment: 0000 - Reference environment

Display Name begins with

No active query. Please enter your search criteria using the options above.

11 items found, displaying all items. Page(s): 1

Display Name	Login ID	Extensions	Groups	Valid From	Valid To	Type	Admin	Superv
Betty Collins	bcollins	1345	Default Customer Services Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Carter Hall	chall	1113	Default Administration Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
David Miller	dmiller	3487	Default Customer Services Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Gordon Sullivan	gsullivan		Default Administration Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Jeff Parker	jparker		Default Administration Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Jennifer Green	jgreen	8768	Default Administration Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
John Adams	jadams	3243 4006	Default Tech Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Maria Gonzalez	mgonzalez	6575	Default Tech Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Thomas Young	tyoung	2734	Default Tech Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No
Verba Administrator	Administrator		Default	Apr 15, 2012		Standard	Yes	Yes
Walter White	wwhite	4002 9875	Default Customer Services Group	Jan 1, 1970	Jan 1, 2099	Standard	No	No

11 items found, displaying all items. Page(s): 1

Export options: [Excel](#) | [RTF](#) | [CSV \(valid users only\)](#)

* Indicates expired user.

The user form is the same as the standard Verba system's user form.

Here you can find out details regarding the form: [User Configuration](#)

The **second option** is that you can create the user in the environment's administration page.

Login to the relevant environment with a user account and follow the instructions set out in the [User Configuration](#) article.

Adding an extension to an Environment

Adding a new extension in Verba multi-tenant environment has two possibilities:

- Add an extension in the default environment to the relevant environment
- Login to the desired extension with a user with full user rights and add the extension 'inside' the environment

The **first option** is a global solution of adding users to Verba multi-tenant system.

To create the user in the default environment, log in to the default, '0000', environment with the administrator user.

Under '**Administration/Extensions**' you can locate on the top right corner, a drop down menu, the '**Current Environment**' menu. Here you can select the desired environment and click the '**Add New Extension**' link above.

Find and List Extensions [Add New Extension](#)
[View Last Calls by Extensions](#)

Current Environment: 0000 - Reference environment

Extension begins with

No active query. Please enter your search criteria using the options above.

10 items found, displaying all items. Page(s): 1

Extension	User name (login)	Description	Recording Mode	Apply IP Filter	Record only on specified Verba Server(s)	Screen Capture Enabled
1113	Carter Hall (chall)		Full	Yes	No	No
1345	Betty Collins (bcollins)		Full	Yes	No	No
2734	Thomas Young (tyoung)		Full	Yes	No	No
3243	John Adams (jadams)		Full	Yes	No	No
3487	David Miller (dmiller)		Full	Yes	No	No
4002	Walter White (wwhite)		Full	No	No	No
4006	John Adams (jadams)		Full	No	No	No
6575	Maria Gonzalez (mgonzalez)		Full	Yes	No	No
8768	Jennifer Green (jgreen)		Full	Yes	No	No
9875	Walter White (wwhite)		Full	Yes	No	No

10 items found, displaying all items. Page(s): 1

Export options: [Excel](#) | [RTF](#)

The extension form is the same as the standard Verba system's extension form.

You can find out details about the form and how to add an extension: [Extension Details](#)

The **second option** is that you can add the extension in the desired environment's administration page.

Login to the relevant environment with a user account from that account and follow the instructions set out in the [Extension Details](#) article.

Environment login

If the multi-tenant feature is enabled, the Verba login screen contains a new field, the environment ID.



The screenshot shows the Verba login interface. At the top left is the 'verba' logo. Below it are the following fields and controls:

- Environment ID:** A text input field with a checked checkbox and the label 'change' next to it.
- Environment Name:** A text input field.
- Login ID:** A text input field.
- Password:** A text input field with a checked checkbox and an asterisk '*' next to it.
- A **Login** button below the password field.

Below the login fields, there is a note: '* Click the check box to enable four eyes login!'

Further down, the license information is displayed: 'The software is licensed to: **Verba**
Version: **7.0.4361.0**'

At the bottom, there is a copyright notice: '(c) Copyright Verba Technologies, LLC. 2000-2013. All rights reserved.'

A detailed license agreement text follows, stating that the software is furnished under a license agreement and may be used or copied only in accordance with the terms of the license agreement. It is against the law to copy the software on any other medium except as specifically allowed in the license agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without the prior written permission of Verba Technologies, LLC. This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Verba represents the environments with a 4 digit number/character ID, during the environment creation you can assign this specified ID to the new environment.

The default (reference environment) is the '0000'. From this default environment you are able to manage the other environments directly ([add environment](#), [add users to environments](#), [add extensions](#) and data retention targets).

In the Environment ID field type the relevant environment's EID.

In a selected environment you are able to login just with an environment user. A newly created environment doesn't contain any user by default, it is important to create at least one user to able to login to the environment.

The login screen remembers the previous choice of environment. If you want to change the EID, you have to click on the 'change' check box.

Searching calls in different Environments

In a multi-tenant system, you are able to apply search filters from the default tenant to other tenants or you can log in the relevant environment and apply filter only on the logged in tenant.

Search from the default environment

If you are logged in to the '0000' default environment you will find an additional field under the Search page's Advanced Search Option segment of Criteria panel, this is the 'Environment' drop down field.

Here you can select the environment you would like to apply your search filter to.

The screenshot shows two panels: 'Search' and 'Calls'.

Search Panel:

- Search bar: Enter a label here...
- Basic Search Options: Two calendar pickers for July 2005 and July 2013. Time: 00:00.
- Advanced Search Options: Environment dropdown set to '0000 - Reference environment'. Call detail record fields: Call Type (Voice), Equal to.
- Metadata Fields: Instant Messaging.
- Buttons: Search..., Timeline.

Calls Panel:

- 1000 items found, displaying 1 to 20. Page(s): 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | > | Results per page: 20

Start Date	Start Time	Duration	Caller Phone Number	Caller Name (Verba)	Called Phone Number	Called Name (Verba)	Direction	Video Thumbnail
Dec 30, 2012	7:23:48 PM	00:01:35	101865855		2734	Thomas Young	Incoming	
Dec 30, 2012	6:08:25 AM	00:01:17	9875	Walter White	121301583		Outgoing	
Dec 30, 2012	4:09:09 AM	00:03:28	159759009		3487	David Miller	Incoming	
Dec 29, 2012	12:17:00 AM	00:00:58	3243	John Adams	197298736		Outgoing	
Dec 28, 2012	11:19:01 AM	00:04:08	1345	Betty Collins	116530276		Outgoing	
Dec 28, 2012	3:02:12 AM	00:01:57	2734	Thomas Young	109295955		Outgoing	
Dec 28, 2012	2:39:27 AM	00:01:54	188034488		1113	Carter Hall	Incoming	
Dec 27, 2012	6:54:16 PM	00:00:38	1345	Betty Collins	123728873		Outgoing	
Dec 27, 2012	3:13:43 PM	00:01:01	3243	John Adams	109352325		Outgoing	
Dec 26, 2012	11:36:48 AM	00:04:59	8768	Jennifer Green	184366138		Outgoing	
Dec 25, 2012	9:39:08 PM	00:01:35	3487	David Miller	116121047		Outgoing	
Dec 25, 2012	1:44:43 AM	00:03:33	1113	Carter Hall	102152682		Outgoing	
Dec 24, 2012	11:42:01 AM	00:03:55	126881183		9875	Walter White	Incoming	
Dec 23, 2012	5:48:12 PM	00:03:26	145048518		6575	Maria Gonzalez	Incoming	
Dec 23, 2012	2:30:06 PM	00:02:13	178733511		6575	Maria Gonzalez	Incoming	
Dec 23, 2012	11:23:59 AM	00:00:52	6575	Maria Gonzalez	107605421		Outgoing	
Dec 22, 2012	9:12:33 AM	00:02:21	109356873		3243	John Adams	Incoming	
Dec 22, 2012	7:38:30 AM	00:01:17	8768	Jennifer Green	187400873		Outgoing	
Dec 22, 2012	12:11:32 AM	00:00:33	100630920		3487	David Miller	Incoming	
Dec 21, 2012	9:53:29 PM	00:01:13	1113	Carter Hall	191075152		Outgoing	

- 1000 items found, displaying 1 to 20. Page(s): 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | > | Results per page: 20
- Export options: Excel | CSV | PDF | Download all

You can find out further information regarding using the Search panel in [Searching conversations](#) article.

Search in the desired environment

If you are logged in to the relevant environment, you also use the standard guide of [Searching conversations](#).

Managing Data Retention in Environments

In the multi-tenant environment if you want to apply data retention policies you have to first create [target folders](#).

Only the '0000' default environment provides an opportunity to create the target folders.

The default environment created folder can be used for data retention policies in separate environments.

Create a new storage target folder

The storage target folder provides the destination path of the archiving process. If you want to archive an environment's calls you have to create a storage target folder for the relevant environment.

To create the folder you have to log in the '0000' default environment and go to the '**Administration/Storage Target Folders**' page.

Find and List Storage Target Folders [Add New Storage Target Folder](#)

Current Environment: 0001 - Test environment

ID begins with

No active query. Please enter your search criteria using the options above.

1 item found. Page(s): 1

Name	Path
0001 archive	D:\0001

1 item found. Page(s): 1

Export options: [Excel](#) | [RTF](#)

Here you can select the relevant environment in the top right corner drop down menu ('**Current Environment**') and add a new target folder by clicking on the link ('**Add New Storage Target Folder**') above the drop down field.

To create the folder please read the [Storage Target Folder details](#) article. All options can be applied in a multi-tenant environment.

Create a data retention policy

When you have the storage target folder you can make data retention policies for archiving or deleting calls.

To create data retention policies for an environment log in '0000' default or in the desired environment.

Go to the '**Administrator/Data Retention Policies**' page.

Find and List Data Retention Policies

[Add New Data Retention Policy](#)

Current Environment: 0001 - Test environment

Name begins with

No active query. Please enter your search criteria using the options above.

1 item found. Page(s): 1


Name	Enabled	Priority	Action	Calls older than
delete calls older than 1 year	Yes	10	Delete	16 year(s)

1 item found. Page(s): 1

Export options: [Excel](#) | [RTF](#)

Here you can select the relevant environment in the top right corner's drop down menu ('**Current Environment**') and add a new target folder by clicking on the link ('**Add New data Retention Policy**') above the drop down field.

To create the folder please read the [Data Retention Policy details](#) article. All options can be applied in a multi-tenant environment.

 The data retention policies can be applied from the desired environment as well but the target folders can be created only in the administration environment ('0000')

Multi-tenant License Allocation

Multi-tenant license allocation enables assigning specified kind of and number of licenses to tenants. This provides the separated tracking of the license usage and the feature allowance between the different tenants. Administrators within the tenants can track their own usage, and they can be alerted in the case of license violation.

Enabling Multi-tenant License Allocation

Step 1 - Go to the **System \ Servers** menu.

Step 2 - Select the Media Repository (or Single Server) from the list.

Step 3 - Go to the **Change Configuration Settings** tab.

Step 4 - Set the **Network \ System \ Tenant-Based License Allocation** setting to **Yes**.

Network


- System
 - API Connection

Server IPv4 Address:	<input checked="" type="checkbox"/>	52.17.20.12
Server S-NAT/Public IPv4 Address:	<input type="checkbox"/>	
Server IPv6 Address:	<input checked="" type="checkbox"/>	fe80::98ce:9eb2:b99c:5dbf%12
Server S-NAT/Public IPv6 Address:	<input type="checkbox"/>	
Verba Cluster ID:	<input checked="" type="checkbox"/>	
Media Repositories:	<input checked="" type="checkbox"/>	<input data-bbox="726 1137 762 1182" type="button" value="+"/>
Multi-Tenant Mode:	<input checked="" type="checkbox"/>	Yes <input type="button" value="v"/>
Tenant-Based License Allocation:	<input checked="" type="checkbox"/>	Yes <input type="button" value="v"/>

Step 5 - Click **Save**.

Step 6 - Repeat the steps for all the Media Repository (or Single) servers.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

 There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please [click here](#).

Using the Tenant-Based License Allocation

Once the Tenant-Based License Allocation is enabled, the feature can be accessed by going to the **System \ License** menu, then clicking on the **Assign Licenses** link in the upper right corner.

Assign Licenses

Environment: 0001 - Contoso

Name	Code	Quantity	Adjust	Allocated
Verba Platform Standard	V4-PL-S-L	<input type="text" value="1"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba User Ethical Wall	V4-E-W1-L	<input type="text" value="99900"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="100"/>	
Verba User CompliancePlus	V4-R-CP1-L	<input type="text" value="99900"/>	<input type="button" value="-"/> <input type="text" value="100"/> <input type="button" value="+"/> <input type="text" value="100"/>	
Verba Add-on Desktop Screen	V4-A-SC1-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba Add-on Video	V4-A-VD1-L	<input type="text" value="99900"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="100"/>	
Verba Add-on Turret	V4-A-TR1-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba Add-on Advanced Compliance	V4-A-AC1-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba Add-on QM	V4-A-QM1-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba Recorded Radio Voice Channel	V4-C-RAD-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba Transcription License	V4-A-STR-L	<input type="text" value="100"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	
Verba User Add-On Speech Analytics (1-100) License	VR3-UAO-SP1-L	<input type="text" value="100000"/>	<input type="button" value="-"/> <input type="text" value=""/> <input type="button" value="+"/> <input type="text" value="0"/>	

Save

For allocating licenses to specific tenants, first, select the tenant on the top, at the **Environment** setting.

In the **Quantity** column, the available license quantities are shown from the total license pool. The **Allocated** column shows the assigned licenses in the selected tenant.

Once the tenant is selected, provide the license quantities to assign or unassign in the **Adjust** column. The specified license quantity can be assigned to the tenant by clicking on the



icon. With the



icon, the specified quantity can be removed from the tenant, and added back to the pool. Once the licenses are assigned / unassigned, the changes can be saved by clicking on the **Save** button.

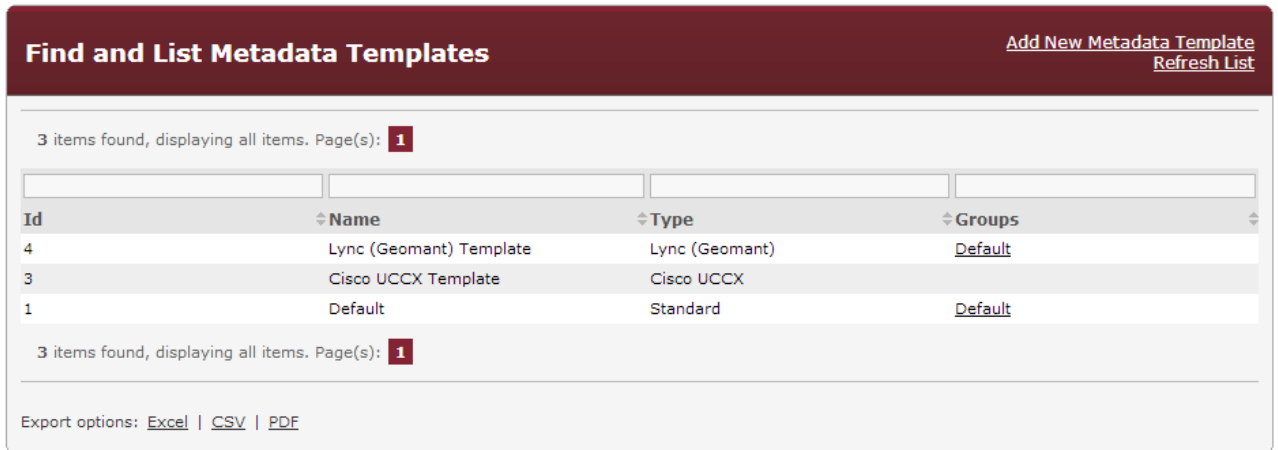
Configuring metadata for contact center integrations

Setting the contact center metadata to specific user groups

To set the contact center metadata to a specific user group please follow the instructions below:

Step 1 Select 'Administration/Metadata Templates'

Step 2 Select the desired metadata template



Find and List Metadata Templates [Add New Metadata Template](#) [Refresh List](#)

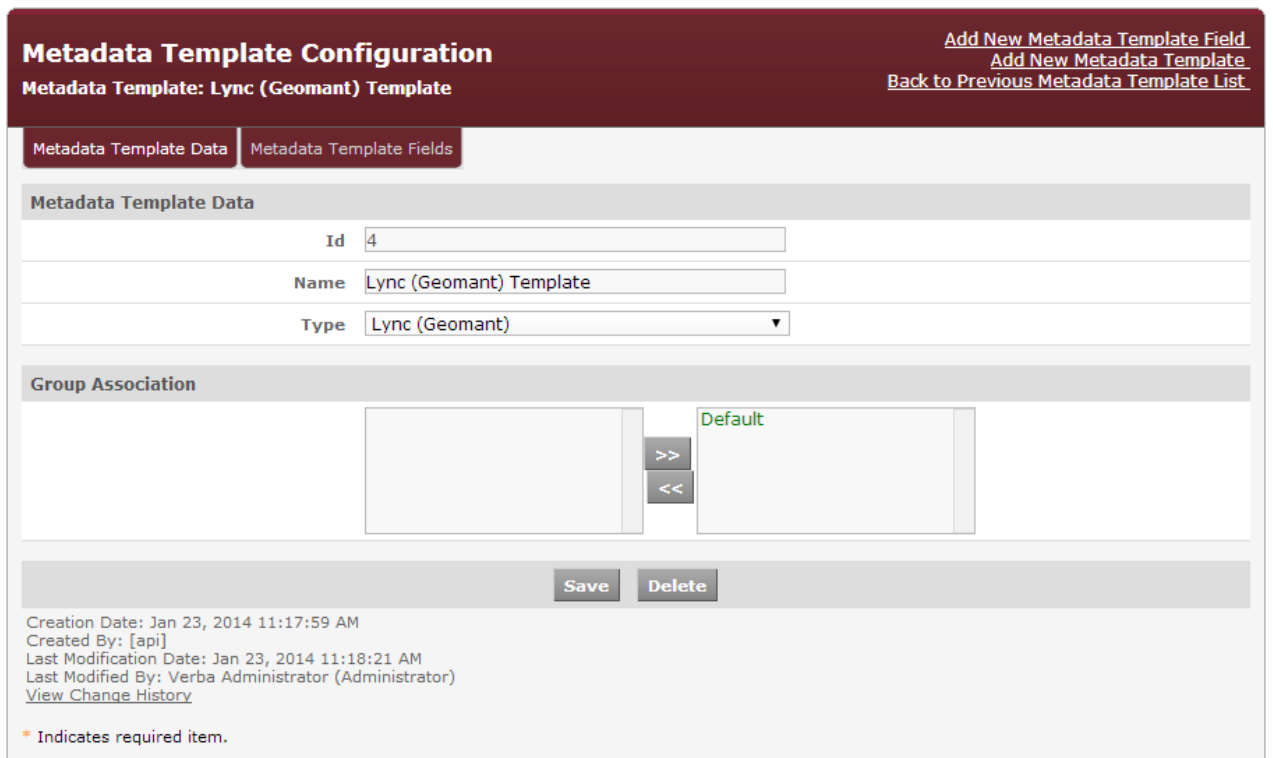
3 items found, displaying all items. Page(s): **1**

Id	Name	Type	Groups
4	Lync (Geomant) Template	Lync (Geomant)	Default
3	Cisco UCCX Template	Cisco UCCX	
1	Default	Standard	Default

3 items found, displaying all items. Page(s): **1**

Export options: [Excel](#) | [CSV](#) | [PDF](#)

Step 3 At the Group Association add the desired groups to the right column and the selected group member will be able to use the metadata fields.



Metadata Template Configuration [Add New Metadata Template Field](#) [Add New Metadata Template](#) [Back to Previous Metadata Template List](#)

Metadata Template: Lync (Geomant) Template

Metadata Template Data | Metadata Template Fields

Metadata Template Data

Id: 4
Name: Lync (Geomant) Template
Type: Lync (Geomant)

Group Association

Default

[Save](#) [Delete](#)

Creation Date: Jan 23, 2014 11:17:59 AM
Created By: [api]
Last Modification Date: Jan 23, 2014 11:18:21 AM
Last Modified By: Verba Administrator (Administrator)
[View Change History](#)

* Indicates required item.

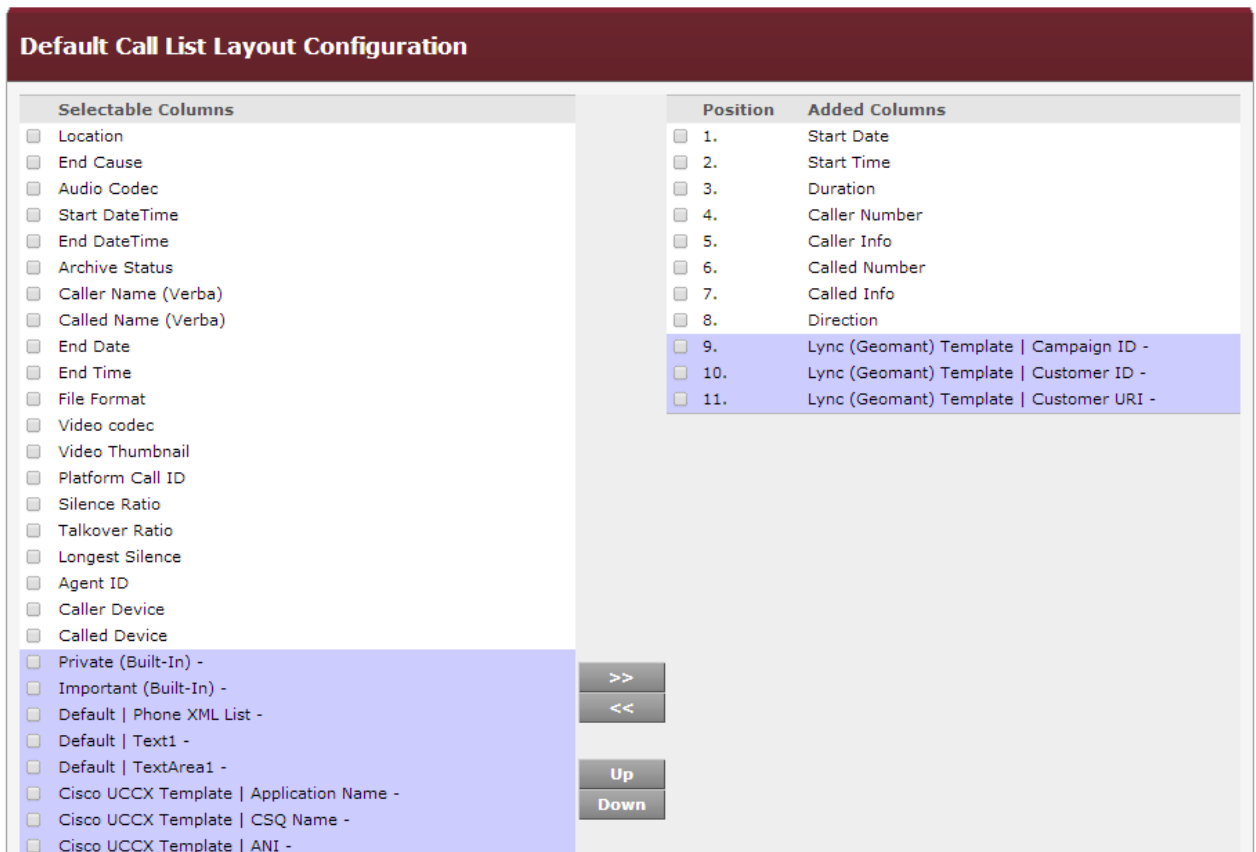
Step 4 Hit the 'Save' button

Adding of contact center metadata fields to the call layouts

Add fields to the default call list layout

To add these fields to the default search layout follow the instructions bellow:

Step 1 Select 'Administration/Default Call List Layout'



Step 2 Select the fields what you want to add to the default layout by checking the check boxes

Step 3 Adding them to the right column

Step 4 Hit the 'Save' button

Add fields to user's search layout

If the metadata template is added to the user's group the user is able to use the metadata fields as a search filter.

To add these fields to the user's search layout follow the instructions bellow:

Step 1 Go to 'Search' page

Step 2 On the top right corner of search result you can find a gear icon click on it

Call List Layout Configuration

Selectable Columns	Position	Added Columns
<input type="checkbox"/> Location	<input type="checkbox"/> 1	Start Date
<input type="checkbox"/> End Cause	<input type="checkbox"/> 2	Start Time
<input type="checkbox"/> Audio Codec	<input type="checkbox"/> 3	Duration
<input type="checkbox"/> Start DateTime	<input type="checkbox"/> 4	Caller Number
<input type="checkbox"/> End DateTime	<input type="checkbox"/> 5	Caller Info
<input type="checkbox"/> Archive Status	<input type="checkbox"/> 6	Called Number
<input type="checkbox"/> Caller Name (Verba)	<input type="checkbox"/> 7	Called Info
<input type="checkbox"/> Called Name (Verba)	<input type="checkbox"/> 8	Direction
<input type="checkbox"/> End Date	<input type="checkbox"/> 9	Lync (Geomant) Template Camp
<input type="checkbox"/> End Time	<input type="checkbox"/> 10	Lync (Geomant) Template Cust
<input type="checkbox"/> File Format	<input type="checkbox"/> 11	Lync (Geomant) Template Cust
<input type="checkbox"/> Video codec		
<input type="checkbox"/> Video Thumbnail		
<input type="checkbox"/> Platform Call ID		
<input type="checkbox"/> Silence Ratio		
<input type="checkbox"/> Talkover Ratio		
<input type="checkbox"/> Longest Silence		
<input type="checkbox"/> Agent ID		
<input type="checkbox"/> Caller Device		
<input type="checkbox"/> Called Device		
<input type="checkbox"/> Private (Built-In)		
<input type="checkbox"/> Important (Built-In)		
<input type="checkbox"/> Default Phone XML List		
<input type="checkbox"/> Default Text1		
<input type="checkbox"/> Default TextArea1		

Items displayed in yellow background are your metadata fields. The metadata fields that had been disassociated from you are displayed in blue background.

Save Cancel

Step 3 Add the 3 fields by selecting them and adding to the right column

Step 4 Hit the 'Save' button

Use metadata fields for search filtering

These fields can be used as a search filter parameter in the 'Search' page of Verba

Setting the search filter follow the next steps:

Step 1 On the Search page you can find the search criteria panel

Search

▼ **Basic Search Options**

January, 2014							
Today							
wk	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1			1	2	3	4	5
2	6	7	8	9	10	11	12
3	13	14	15	16	17	18	19
4	20	21	22	23	24	25	26
5	27	28	29	30	31		

Time: Select date

January, 2014							
Today							
wk	Mon	Tue	Wed	Thu	Fri	Sat	Sun
1			1	2	3	4	5
2	6	7	8	9	10	11	12
3	13	14	15	16	17	18	19
4	20	21	22	23	24	25	26
5	27	28	29	30	31		

Time: Select date

Time of the day
+

Phone Number (Caller or Called Party)

User

▶ **Advanced Search Options**

▶ **Metadata Fields**

Step 2 Open the 'Metadata Fields' drop down on the panel

▼ **Metadata Fields (*)**

Full text search in metadata

Full text search in markers

Metadata fields

Lync (Geomant) Template: Camp ▼ Geomant Campaign

▼

+

Step 3 Hit the '+' button

Step 4 You can select from the metadata fields which are provided by the metadata template

Migration from Verint

Overview

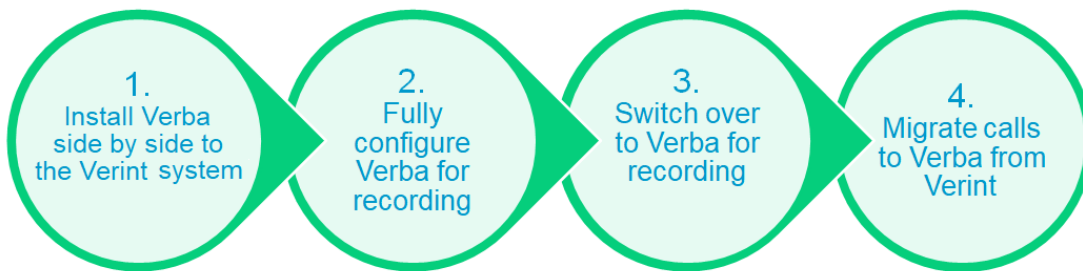
The purpose of the migration is to import the historical recordings from the Verint v11, v15.1 Legacy, and v15.2 solutions to the Verba system.

The migration offers the following features:

- Supported platforms:
 - IMR Financial Trading Recorder (IPC Media Recorder)
 - BT Financial Trading Recorder
 - Verint Financial Trading Recorder
- Migration of historical recordings from Verint v11.1 and v11.2 and v15.1 Legacy and v15.2 systems
- Support for archived calls only
- Supported archive mediums: SMB folder, EMC Centera, Hitachi Content Platform (**tapes, DVDs, or any other removable media is not supported**)
- Storage targets are automatically created based on the archive configuration in Verint
- All Verint file formats and codecs are supported: wave file using G.729, G.723.1, or G.726
- Encrypted calls are not supported
- Both back office and front office (trader voice) calls can be imported
- Users, Groups, and Extension can be migrated only from v15.2 systems. The Users' conversation access scope is not migrated.
- Migrated calls are assigned to users defined in Verba based on their associated recorded extensions (Trader ID / Extension or Phone Number / SIP URI)

Migration process

The migration consists of multiple steps, outlined below:



1. Phase: Install Verba side by side to the Verint system

In this phase, a complete Verba system is deployed to allow recording of the communication platforms (both trader voice and telephony or unified communication). The Verba system is deployed on new servers, side-by-side to the existing Verint installation. Certain parts of the existing infrastructure can be reused potentially. This includes the SQL Server, where the Verba database is hosted and the storage infrastructure where the recordings will be stored. The Verint and Verba software applications cannot be installed on the same operating system.

2. Phase: Fully configure the Verba system for recording

In this phase, the Verba system is fully configured for recording and archiving. All users are configured, including any historical user and recorded extension (trader ID, phone number, SIP URI) configuration which is necessary to assign the imported calls to users.

Access control settings have to be recreated or Active Directory synchronization should be enabled. If the Verint system version is 15.2 then User, Groups, and Extensions can be pulled from the Verint database at this phase, before the actual call migration started. The system has to be fully tested after completing this stage.

3. Phase: Switch over to Verba for recording

Once everything is configured and tested, the recording is cut over to the new Verba platform. The recording on the Verint system is turned off. This step has to be carefully designed with the appropriate fallback plans in place. This might be done in multiple phases and gradually moving users over to the new Verba platform if the integration allows using multiple recording systems at once.

4. Phase: Migrate calls to Verba from Verint

After the Verint system stops recording calls, the historical calls can be imported to the Verba system.

Archive considerations

During migration, the system imports call data into the Verba database. However, media files stay on their existing location in the Verint archives. The system imports the references to the files (*.tar) and the Verba system has new features that allow accessing these files without the need to move, copy, untar or transcode them. Because of the different archiving and storage concepts in the two systems, certain features are not available for the imported calls. The following table provides an overview of the differences.

	Verba recordings	Recordings imported from Verint, stored in Verint Archive	Notes
Archive Format	Individual file for each call	TAR files grouping several calls together	The TAR file concept introduces multiple limitations because the files cannot be managed individually in the TAR. This is the reason for not supporting all storage /archive features for imported calls.
Multiple Archives	No ❌	Yes ✅	The Verint system allows archiving the same call multiple times, while the Verba system only supports a single copy in the archive. During migration, all archive entries are imported, but the oldest archive is selected as the primary archive which is then linked with the CDR entry in the database, which is used for playback, download, and export (to be compatible with Verba). Subsequent archive copies are not accessible through the Verba system, but the system manages the retention period settings and attempts to delete the copies after the retention period expires. If for some reason, the primary copy is selected for deletion, the system chooses the next available archive copy as the primary automatically.
Playback	Yes ✅	Yes ✅	
Playback multiple files at once	Yes ✅	Yes ✅	
Playback marked segment	Yes ✅	Yes ✅	
Download	Yes ✅	Yes ✅	

Download multiple files at once	Yes	Yes	
Export	Yes	Yes	
Copy Media	Yes	No	The system filters out imported calls for the policy automatically
Move Media	Yes	No	The system filters out imported calls for the policy automatically
Upload	Yes	No	The system filters out imported calls for the policy automatically
Archive in DB and Move Media	Yes	No	The system filters out imported calls for the policy automatically
Archive in DB	Yes	Yes	
Delete, Policy-based	Yes	Yes	The system will delete the CDRs, but only delete the TAR files once all calls are deleted
Delete, Manual	Yes	Yes	The system will delete the CDRs, but only delete the TAR files once all calls are deleted
Legal Hold	Yes	Yes	For imported calls, the system is not able to set the legal hold flag on EMC Centera, only in the Verba system
File Verification	Yes	No	The system filters out imported calls for the policy automatically
Increase Retention Period	Yes	No	Custom SQL script can be used to update the retention in the Verba database
Deduplicate Recordings	Yes	No	The system filters out imported calls for the policy automatically
Encrypt and Sign	Yes	No	The system filters out imported calls for the policy automatically
Voice Quality Check	Yes	Yes	
Transcode	Yes	No	The system filters out imported calls for the policy automatically
Transcription	Yes	No	The system filters out imported calls for the policy automatically
Phonetic Indexing	Yes	No	The system filters out imported calls for the policy automatically

Configuring the migrating from Verint systems

The configuration of the migration is slightly different for v11/v15.1 Legacy and v15.2 systems. Follow the instructions of the related guides specific to your environment:

- [Migration from Verint v11 and v15.1 Legacy systems](#)

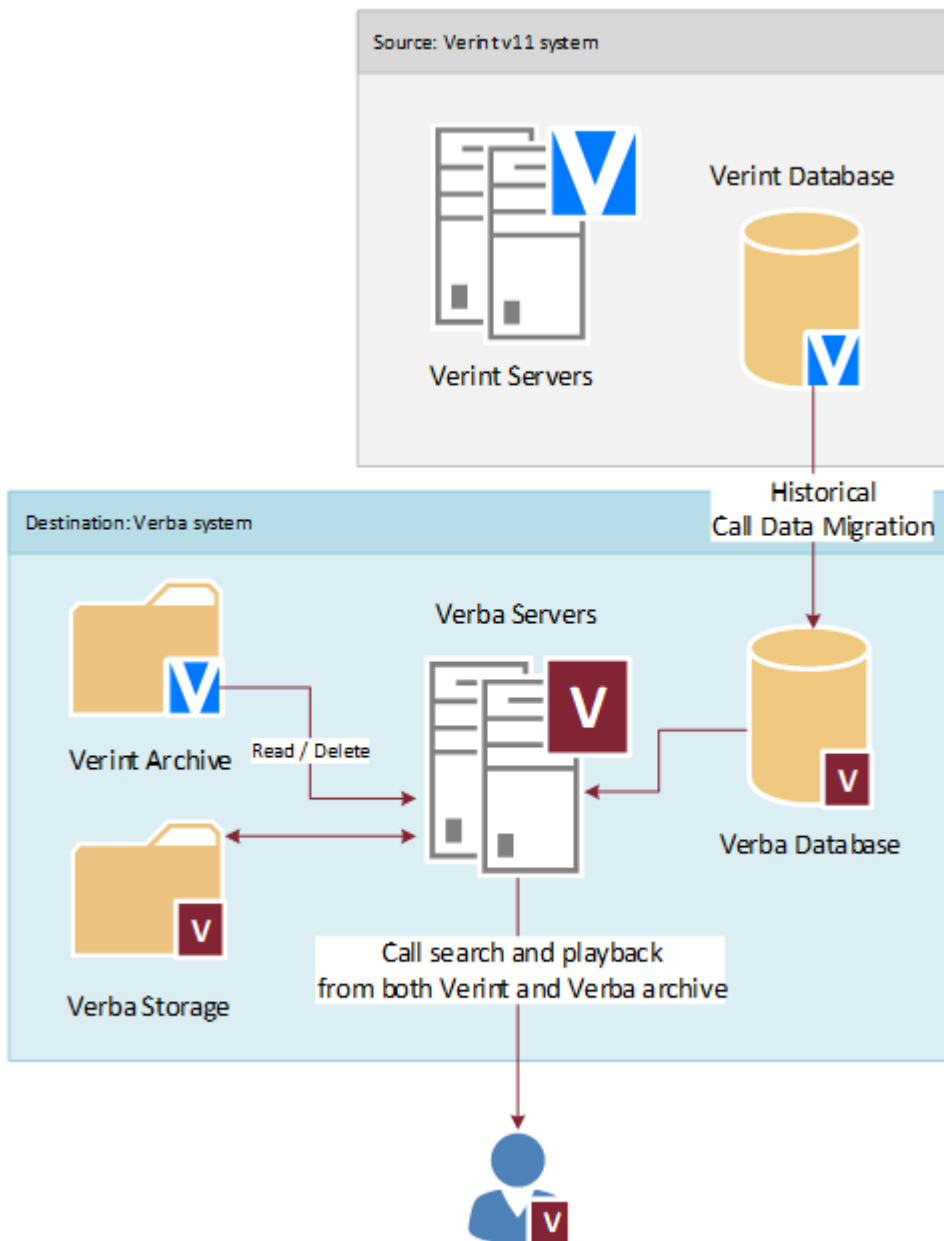
- [Migration from Verint v15.2 systems](#)

Migration from Verint v11 and v15.1 Legacy systems

- [Overview](#)
- [Migration process](#)
- [Archive Considerations](#)
- [Prerequisites](#)
 - [Running the SQL scripts](#)
 - [Running the SQL scripts on the Verba database](#)
 - [Running the SQL scripts on the Verint database](#)
- [Migration tool](#)
 - [Enabling the migration tool](#)
 - [Source databases](#)
 - [Back Office \(Telephony and Unified Communication\)](#)
 - [Front Office \(Trader Voice\)](#)
 - [Data preview](#)
 - [Running the migration](#)
- [Post-migration tasks](#)
- [Removing imported calls from Verba and resetting the import](#)

Overview

The purpose of the migration is to import the historical recordings from the Verint v11, v15.1 Legacy systems to the Verba platform.



The migration offers the following features:

- Supported platforms:
 - IMR Financial Trading Recorder (IPC Media Recorder)
 - BT Financial Trading Recorder
 - Verint Financial Trading Recorder
- Migration of historical recordings from Verint v11.1 and v11.2 and v15.1 Legacy systems
- Support for archived calls only
- Supported archive mediums: SMB folder or EMC Centera, Hitachi Content Platform (**tapes, DVDs, or any other removable media is not supported**)
- Storage targets are automatically created based on the archive configuration in Verint
- All Verint file formats and codecs are supported: wave file using G.729, G.723.1, or G.726
- Encrypted calls are not supported
- Both back office and front office (trader voice) calls can be imported
- Users, Groups, and Extension can be migrated only from v15.2 systems. The Users' conversation access scope is not migrated.
- Migrated calls are assigned to users defined in Verba based on their associated recorded extensions (Trader ID / Extension or Phone Number / SIP URI)

Migration process

See [Migration from Verint](#) for more information on the migration process.

Archive Considerations

See [Migration from Verint](#) for more information on limitations of the archive features.

Prerequisites

Before you begin the migration, the following items must be completed and checked:

- The Verba system is deployed, configured, and tested.
- The Verba database is properly sized to accommodate the imported calls. Sizing estimate: ~5 KByte / imported call
- Sufficient time is planned for the migration. We recommend running the migration tool out of business hours to minimize the impact on the Verba database.
Front-office migration time estimate: ~5 million calls / hour
Back-office migration time estimate: ~3.5 million calls / hour
- All calls in Verint are archived, calls cannot be in the call buffer on the Verint recorders.
- The user configuration is complete in the Verba system for historical calls.
- The metadata mapping is checked and confirmed for both front-office and back-office calls.
- The SQL Servers are linked:

The Verint database has to be configured as a linked server on the Verba database server so the system can run queries on both systems during the migration. Server Options / RPC Out needs to be set to True in the Linked Server configuration. Once the migration is finished, the linked server configuration can be removed.

Alternatively, the Verint databases (Archive, BPMAINDB, EWareCalls, and EWareConfig) can be backed up and restored on the Verba database server.

For more information on configuring a linked server, see <https://docs.microsoft.com/en-us/sql/relational-databases/linked-servers/create-linked-servers-sql-server-database-engine>

- The recording functionality is turned off on the Verint recorders. This step is to ensure that no new calls are created on the Verint platform, so the system can migrate all historical calls. The migration supports partial migrations by defining date ranges. However, it has to be very carefully designed and tested to ensure all calls are migrated.
- All 3rd party database maintenance tools are disabled on both the Verint and the Verba database servers.
- The Verba Maintenance Job is disabled. For more information on disabling SQL Server jobs, see <https://docs.microsoft.com/en-us/sql/ssms/agent/disable-or-enable-a-job>.
- Verba database backup is created to be able to restore the system in the event of a fatal system error during the migration
- The necessary SQL scripts are executed on the Verba and the Verint databases (see below).
- The Verint system is upgraded to 11.1 HFR 9 or later.

Running the SQL scripts

SQL scripts have to be executed on both the Verba and Verint databases before the migration can be started. The SQL scripts can be executed using the Microsoft SQL Server Management Studio which can be downloaded from <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms>.

Running the SQL scripts on the Verba database

In order to run the SQL scripts on the Verba database, the SQL user requires the **ALTER ANY LINKED SERVER** permission or the **sysadmin** role to run these scripts. If you need help granting the permission, follow the article at <https://docs.microsoft.com/en-us/sql/t-sql/statements/grant-server-permissions-transact-sql>.

The SQL script files can be found on the Verba Media Repository Server under the c:\Program Files\Verba\resources\db\verintmig folder. Execute them in alphabetical order on the Verba database before starting the migration:

1. update-programs-verintmig-aaa-common.sql
2. update-programs-verintmig-aaa-common-inum.sql
4. update-programs-verintmig-bo.sql
5. update-programs-verintmig-fo-cti.sql
6. update-programs-verintmig-fo-cti-15.sql (only from Verba 9.5)
7. update-programs-verintmig-fo-vox.sql
8. update-programs-verintmig-fo-vox-15.sql (only from Verba 9.5)
9. update-programs-verintmig-us.sql (only from Verba 9.5)
10. update-programs-verintmig-zzz-common.sql

Running the SQL scripts on the Verint database

Additionally, another SQL script must be executed on the Verint EWareCalls database. This script is located at c:\Program Files\Verba\tomcat\webapps\verba\WEB-INF\verintmig\verintmig-download\verba-verint-ewarecalls.sql, or can be downloaded from the Verba UI at the Verint Migration Source Database configuration page.

The script will add a new column to the Archive.dbo.Media table named verba_prio. **Before starting the migration, this column has to be populated.** Storage locations that are more likely to be available should be given a higher number.

Migration tool

The migration tool, available through the Verba user interface, provides the following features:

- Permission / Role-based access
- Multiple Verint database sources can be added
- For each database, multiple subsets have to be defined:
 - Front-Office (based on time and selected Verint datasources)
 - Back-Office (based on time and selected Verint v11 views)
- Field mapping configuration for Back-Office calls
- Migration status information, configuration warnings (e.g. subsets configured does not cover all calls in the Verint v11 database)
- Planning stage with data preview
- Data is migrated in monthly chunks
- The migration process can be paused and resumed later
- If the migration fails, it can be restarted from the last finished month
- Detailed logs
- The migration process is executed by the Web Application Service so the user can log off from Verba web UI and can turn their PC off
- No server restart is needed after the migration
- The performance of the Verba database can be degraded after the migration, if that happens, then the Verba Maintenance Job should be executed. This process might take several hours.
- The Verint databases are not changed, only four very simple helper procedures are installed (see Running the SQL scripts on the Verint database)

The Migration Tool migrates one call type (Back-Office calls or Front-Office calls) at a time. Once the first call type migration is complete, you are ready to migrate the remaining call type. The order in which you migrate the call data is not important.

The tool can be run from only one of the Media Repository / Application Servers. For example, you cannot run the tool on multiple servers at the same time.

The Back-Office and Front-Office database migrations move records from the EWareCalls and Archive databases into the Verba database and associate the calls with the existing users when available. The users must exist in the Verba database before the migration begins. Depending on the customer and the number of calls in the Verint database, data migration can encompass several million or more records.

Enabling the migration tool

The migration tool has to be enabled before the migration can take place.

Step 1 - Navigate to **System / Servers** or **System / Configuration Profiles** (in case you want to update the configuration profile used by the recording servers), then select the server which runs the Web Application service or the configuration profile.

Step 2 - Select the **Change Configuration Settings** tab and change the **Web Application / Miscellaneous / Verint Migration Enabled** setting to **Yes**.

Step 3 - Save the changes by clicking on the



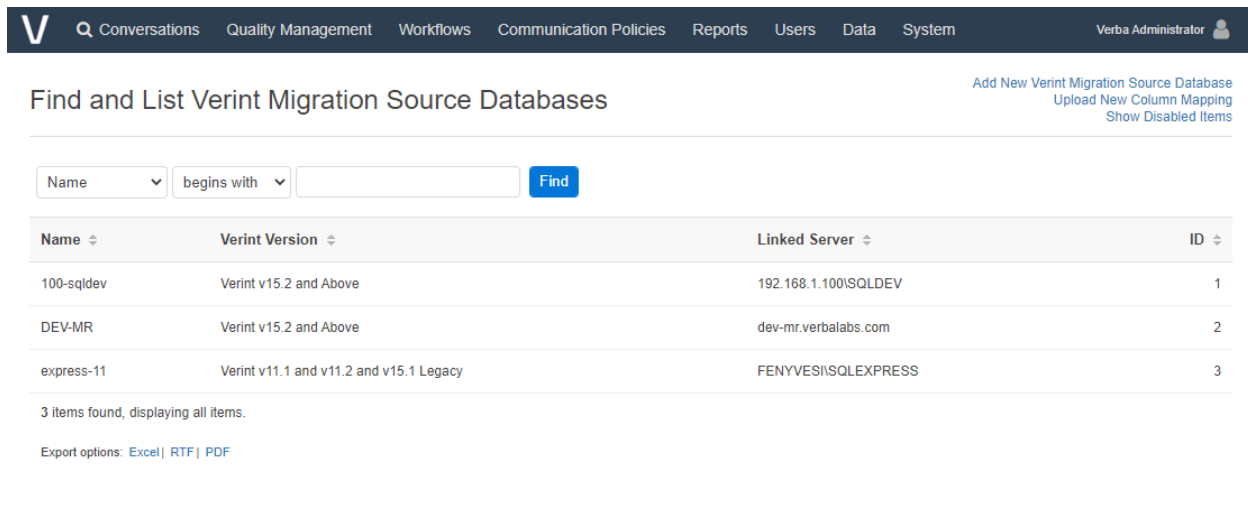
icon.

Step 4 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 5 - The **Data / Verint Migration** menu item will be visible when the logged-in user has Verint Migration permission, and the SQL scripts ran successfully.

Source databases

The menu opens the list of the Verint Migration Source Databases. In most cases, there will be one Source Database, but the system allows migrating from multiple databases.



The screenshot shows the 'Find and List Verint Migration Source Databases' interface. At the top, there is a navigation bar with the Verint logo and menu items: Conversations, Quality Management, Workflows, Communication Policies, Reports, Users, Data, System, and Verba Administrator. Below the navigation bar, there are three links: 'Add New Verint Migration Source Database', 'Upload New Column Mapping', and 'Show Disabled Items'. The main content area has a search bar with 'Name' and 'begins with' dropdowns, a text input field, and a 'Find' button. Below the search bar is a table with the following data:

Name	Verint Version	Linked Server	ID
100-sqldev	Verint v15.2 and Above	192.168.1.100\SQLDEV	1
DEV-MR	Verint v15.2 and Above	dev-mr.verbalabs.com	2
express-11	Verint v11.1 and v11.2 and v15.1 Legacy	FENYVESI\SQLEXPRESS	3

Below the table, it says '3 items found, displaying all items.' and 'Export options: Excel | RTF | PDF'.

Click on the Add New Verint Migration Source Database link at the top right folder to add a new source database. First of all, the Verint version has to be specified: **Verint v11.1 and v11.2 and v15.1 Legacy**.

When the Linked Server is empty, then the Verint databases (Archive, BPMAINDB, EWareCalls, and EWareConfig) have to be on the same server where the Verba database is. This can speed up the migration dramatically.

Details of a Source Database:



The screenshot shows the 'Verint Migration Source Database Configuration' page. At the top, there is a navigation bar with the Verint logo and menu items: Conversations, Quality Management, Workflows, Communication Policies, Reports, Users, Data, System, and Verba Administrator. Below the navigation bar, there are four links: 'Refresh', 'Add New Subset', 'Add New Verint Migration Source Database', and 'Back to Previous Page'. The main content area has a 'Basic Information' section with a dropdown arrow and the text 'ID 2'.

Name * DEV-MR

Enabled * Yes

Verint Version * Verint v15.2 and Above

Linked Server dev-mr.verbalabs.com

Set to empty if the Verint databases are on the same server where the Verba database is.
 If a Linked Server is used, then the Server Options / RPC Out option needs to be set to True in the Linked Server configuration.

[Download CentralContact helper scripts](#)

Storage Targets Synchronized 4

Users / Groups [Synchronize Users](#)

Already Existing Users / Groups / Extensions will not be affected

Subsets

[Add New Subset](#)

Type	Name	Status	Datasource	Processed Until	Interval	Total # of Days	Processed Days	Progress	Source Records	Imported Records	ID
Back Office (Telephony and Unified Communication)	Cisco	Planning	151: Cisco (-505013: Cisco Unified Call Manager)				0			0	8
Back Office (Telephony and Unified Communication)	avaya	Planning	51: Avaya (-505002: Avaya Communication Manager/Definity)				0			0	7
Front Office (Trader Voice)	IP Trade	Planning	101: IPTrade (IP; -505041: IP Trade)				VOX: 0 CTI: 0		VOX: 0 CTI: 0	VOX: 0 CTI: 0	6
Front Office (Trader Voice)	IPC-Alliance	Planning	1: Alliance_DS (TDM; -505029: IPC Alliance)				VOX: 0 CTI: 0		VOX: 0 CTI: 0	VOX: 0 CTI: 0	5
Users	uuuu	Finished	Users, Groups, Extensions						9	7	4

Export options: [Excel](#) | [RTF](#) | [PDF](#)

[Save](#)

Creation Date: Nov 18, 2020, 3:47:46 PM
 Created By: Verba Administrator (Administrator)
 Last Modification Date: Nov 18, 2020, 3:49:03 PM
 Last Modified By: Verba Administrator (Administrator)
[View Change History](#)

The setup, the log entries, the calculated numbers, and basically everything is stored in database tables and will not be deleted after completing the migration.

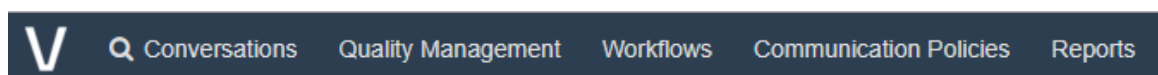
The Storage Targets will be synchronized during the migration of the first subset.

The source data is divided into Subsets. A Subset can be either Back Office or Front Office, and only one Subset may run at a time. The v15.2 User migration also creates a new Subset in order to simply track the process and the log.

The "Total" and "Source" numbers will be calculated either when the subset runs for the first time, or when you click on the Update Numbers button.

The Back Office Subsets in the case of v11 and v15.1 are summed by the system and compared to the "Total # of Back-Office records". A mismatch will generate a warning.

Back Office (Telephony and Unified Communication)



Verint Migration Database Subset Configuration

[Subset Details](#) [Preview Data](#)

Basic Information

Source Database LOCAL: (#1)

ID 7

Type * Back Office (Telephony and Unified Communication)

Database VIEW * CSCMAvayaCallsView

Name * bo-avaya-02

From [Clear](#)

To [Clear](#)

Status Planning

▼ Column Mapping

Mandatory columns (already mapped to the appropriate Verba fields) INum, PrevINum, NextINum, StartedAtUtc, Duration, FormatId

Source	Destination	
StartedAt	--Choose--	
StartedAtUTC	--Choose--	
Channel	Native ID	
FormatId	--Choose--	
INum	--Choose--	
Duration	--Choose--	
Digits	From	



Save Save and Run Delete

First of all, a Database VIEW has to be selected. Then the system reads the columns of the view and displays the Column Mapping setup.

The VIEW has to contain the following mandatory columns: INum, PrevINum, NextINum, StartedAtUtc, Duration, FormatId. These columns are already mapped to the appropriate Verba fields, so no need to map them again.

You can optionally set From and To times to narrow down the migrated time interval.

Front Office (Trader Voice)

The process is similar to the Back Office, but instead of a VIEW, a Datasource has to be selected, and the column mapping is not configurable on the GUI.

Verint Migration Database Subset Configuration Add New Verint Migration Database Subset
Back to Previous Page

Subset Details | Preview Data VOX-Media | Preview Data CTI-CDR

▼ Basic Information

Source Database LOCAL: (#1)
ID 2

Type * Front Office (Trader Voice) ▼

Datasource * 1: UnigyV2 (IP; -505026: IPC Unigy) ▼

Name * fo-01

From Clear

To Clear

Status Planning

Save Save and Run Delete

Creation Date: Jul 2, 2019 5:56:31 PM
Created By: Verba Administrator (Administrator)
Last Modification Date:
Last Modified By:
[View Change History](#)

* Indicates required item.

The column mapping is actually similar to the Back Office mapping, but it is shipped with the product. If it has to be changed, then the new XML mapping file can be uploaded in the Verint Migration Source Databases List screen, using the **Upload New Front Office Mapping** link at the top right corner.

Data preview

A preview of the data (the first 100 records) is available on the Preview tab:

Verint Migration Database Subset Configuration

Subset Details | **Preview Data**

inum	previnum	nextinum	Start Time	End Time	FormatId	From	avaya / Owner	Files
743001000000027.0000			2016-06-09 17:26:49.543	2016-06-09 17:27:56.543	4		1,10.156.15.17 :10.156.42.140	
743001000000034.0000			2016-06-09 17:28:50.02	2016-06-09 17:29:51.02	4		1,10.156.15.17 :10.156.42.140	CLMedia (
743001000000039.0000			2016-06-09 17:30:40.103	2016-06-09 17:30:52.103	4		1,10.156.15.17 :10.156.42.140	CLMedia (
743001000000042.0000			2016-06-09 17:31:40.857	2016-06-09 17:32:15.857	4		1,10.156.15.17 :10.156.42.140	

Running the migration

When the setup is complete and the Preview looks good, then use the **Save and Run** button to start the migration. The system will migrate one month at a time.

The **Logs** tab displays the progress and log messages:



Verint Migration Database Subset Configuration

[Subset Details](#)
[Preview Data](#)
[Logs](#)

Select Run: Jul 8, 2019 11:12:24 AM - Jul 8, 2019 11:12:24 AM on HUN-500796 #1106

Select Types: Messages SQLs

▼ Basic Information

Status **Finished**

Processed Until Jul 1, 2016 12:00:00 AM

Total # of Days 30

Processed Days 30

Progress 100%

Source Records 4

Imported Records 4

▼ Logs

Start Time	End Time	Affected Rows	Message
2019-07-08 11:12:24			Compute best_location_id
2019-07-08 11:12:24	2019-07-08 11:12:24		Create idx_tempmiginums_hml index on ##inum_migrate_data
2019-07-08 11:12:24			Compute has_multiple_locations
2019-07-08 11:12:24			Transfer container
2019-07-08 11:12:24			Create indexes on ##inum_inum_location
2019-07-08 11:12:24			Transfer inum_location
2019-07-08 11:12:24	2019-07-08 11:12:24		About to generate topinums for related call association
2019-07-08 11:12:24	2019-07-08 11:12:24		Create indexes on ##inum_migrate_data
2019-07-08 11:12:24	2019-07-08 11:12:24	4	Transferred 4 BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			Transfer BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			About to migrate Back Office calls from ewarecalls.dbo.CSCMAvayaCallsView BETWEEN 2016-06-01 mapping 4
2019-07-08 11:12:24	2019-07-08 11:12:24	1	Transferred 1 BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			About to migrate Back Office calls from ewarecalls.dbo.CSCMAvayaCallsView BETWEEN 2016-06-01 mapping 4
2019-07-08 11:12:24			Time interval: 2016-06-01 17:28:00 - 2016-07-01 00:00:00
2019-07-08 11:12:24			Initializing the execution of 1 (type: bo)

The **Select Run** listbox contains one entry for one execution, so if the migration stopped or failed, and someone restarted, then a new entry will be inserted.

Use the **SQLs** checkbox to turn on detailed log entries with the actual SQL statements.

The execution can be paused by the **Pause** button. Pressing the button will not cause the termination immediately, but will change the status to **Pausing**. Once the migration of the current month finished, the status will go to **Paused**. The buttons are not refreshed automatically so if the Pause button is not visible while the migration is in progress, then go back to the list of the subsets and open the details again.

When the execution paused, finished, or failed, then the first tab will display the **Run Again** button that can be used to restart the migration of the Subset. Already migrated calls will not be migrated again, because they are saved in the `verintmig_migrated_xxx` tables.

One month is one transaction, and in case of an error in the middle, the whole transaction will be rolled back. In order to be able to effectively log to DB tables, we have to get out from the transaction, because otherwise, the log entries would not be visible to other DB sessions. In order to do this, a loopback Linked Server is created during the installation named `verba_loopback`.

If the execution fails, then the status of the Subset will be Failed, and the error message will be shown in the **Logs** tab. Unfortunately, there are errors that cannot be caught, and in that case, the subset will remain in the Running state. If you are sure that the process died, then click on the **Mark as Failed** button to set the state to Failed, then fix the problem and start the Subset again.

If a process is still running, then starting another one will throw an error: "Error during `pr_verintmig_bo`: Cannot acquire lock (Lock State: -1), probably another migration is still running (16, 1)".

Post-migration tasks

After the migration completed, the following items must be completed and checked:

- If the media files are stored on EMC Centera, then copy the PEA file to a location accessible by the Verba Media Repository Servers and change the configuration of the Verba Storage Targets to point to the new PEA file location
- If the media files are stored on the Hitachi Content Platform, then the Verba Storage Targets have to be configured with the correct API User and Password, because the Password was not copied from the Verint database
- Verify that calls are searchable and accessible through the Verba system.
- Verify that all Verint archive locations are available as storage targets in the Verba system.
- Verify that all calls are migrated by checking the information displayed on the subsets page.

Removing imported calls from Verba and resetting the import

If the migrated calls should be deleted and the Subset status should be "Planning", then use the `manual-verintmig-delete-subset-calls.sql` can be found on the Verba server in the `Verba\resources\db\util` folder. Set the ID of the Subset at the beginning of the file:

```
@subset_id INT = 0 -- TODO set subset id
```

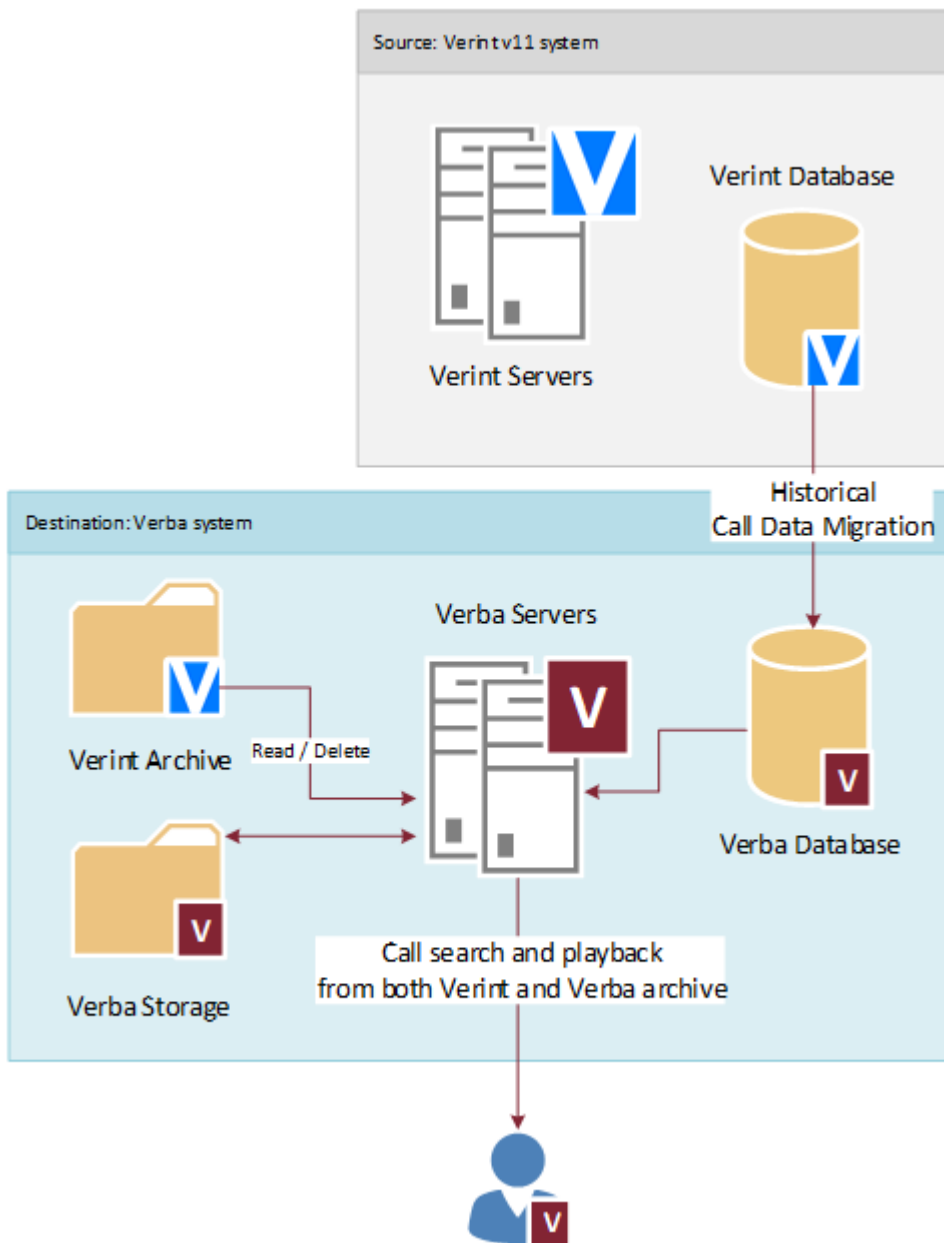
Then execute the SQL in SQL Server Management Studio. The script will delete all calls of the Subset from the Verba database, and will reset the state of the Subset to "Planning".

Migration from Verint v15.2 systems

- [Overview](#)
- [Migration process](#)
- [Archive Considerations](#)
- [Prerequisites](#)
 - [Running the SQL scripts](#)
 - [Running the SQL scripts on the Verba database](#)
 - [Running the SQL scripts on the Verint database](#)
- [Migration tool](#)
 - [Enabling the migration tool](#)
 - [Source Databases](#)
 - [Front Office \(Trader Voice\) and Back Office \(Telephony and Unified Communication\)](#)
 - [Data preview](#)
 - [Running the migration](#)
 - [Users, Extensions, and Groups](#)
 - [Users](#)
 - [Extensions](#)
 - [Groups](#)
- [Post-migration tasks](#)
- [Removing imported calls from Verba and resetting the import](#)

Overview

The purpose of the migration is to import the historical recordings from the Verint v15.2 solutions to the Verba system.



The migration offers the following features:

- Supported platforms:
 - IMR Financial Trading Recorder (IPC Media Recorder)
 - BT Financial Trading Recorder
 - Verint Financial Trading Recorder
- Migration of historical recordings from Verint v15.2 systems
- Support for archived calls only
- Supported archive mediums: SMB folder or EMC Centera, Hitachi Content Platform (**tapes, DVDs, or any other removable media is not supported**)
- Storage targets are automatically created based on the archive configuration in Verint
- All Verint file formats and codecs are supported: wave file using G.729, G.723.1, or G.726
- Encrypted calls are not supported
- Both back office and front office (trader voice) calls can be imported
- Users, Groups, and Extension can be also migrated from v15.2 systems. The Users' conversation access scope is not migrated.
- Migrated calls are assigned to users defined in Verba based on their associated recorded extensions (Trader ID / Extension or Phone Number / SIP URI)

Migration process

See [Migration from Verint](#) for more information on the migration process.

Archive Considerations

See [Migration from Verint](#) for more information on the limitations of the archive features.

Prerequisites

Before you begin the migration, the following items must be completed and checked:

- The Verba system is deployed, configured, and tested.
- The Verba database is properly sized to accommodate the imported calls. Sizing estimate: ~5 KByte / imported call
- Sufficient time is planned for the migration. We recommend running the migration tool out of business hours to minimize the impact on the Verba database.
Front-office migration time estimate: ~5 million calls / hour
Back-office migration time estimate: ~3.5 million calls / hour
- All calls in Verint are archived, calls cannot be in the call buffer on the Verint recorders.
- The user configuration is complete in the Verba system for historical calls.
- The metadata mapping is checked and confirmed for both front-office and back-office calls.
- The SQL Servers are linked:

The Verint database has to be configured as a linked server on the Verba database server so the system can run queries on both systems during the migration. Server Options / RPC Out needs to be set to True in the Linked Server configuration. Once the migration is finished, the linked server configuration can be removed.

Alternatively, the Verint databases (Archive, BPMAINDB, CentralContact, and CommonDB) can be backed up and restored on the Verba database server.

For more information on configuring a linked server, see <https://docs.microsoft.com/en-us/sql/relational-databases/linked-servers/create-linked-servers-sql-server-database-engine>

- The recording functionality is turned off on the Verint recorders. This step is to ensure that no new calls are created on the Verint platform, so the system can migrate all historical calls. The migration supports partial migrations by defining date ranges. However, it has to be very carefully designed and tested to ensure all calls are migrated.
- All 3rd party database maintenance tools are disabled on both the Verint and the Verba database servers.
- The Verba Maintenance Job is disabled. For more information on disabling SQL Server jobs, see <https://docs.microsoft.com/en-us/sql/ssms/agent/disable-or-enable-a-job>.
- Verba database backup is created to be able to restore the system in the event of a fatal system error during the migration
- The necessary SQL scripts are executed on the Verba and the Verint databases (see below).

Running the SQL scripts

SQL scripts have to be executed on both the Verba and Verint databases before the migration can be started. The SQL scripts can be executed using the Microsoft SQL Server Management Studio which can be downloaded from <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms>.

Running the SQL scripts on the Verba database

In order to run the SQL scripts on the Verba database, the SQL user requires the **ALTER ANY LINKED SERVER** permission or the **sysadmin** role to run these scripts. If you need help granting the permission, follow the article at <https://docs.microsoft.com/en-us/sql/t-sql/statements/grant-server-permissions-transact-sql>.

The SQL script files can be found on the Verba Media Repository Server under the c:\Program Files\Verba\resources\db\verintmig folder. Execute them in alphabetical order on the Verba database before starting the migration:

1. update-programs-verintmig-aaa-common.sql
2. update-programs-verintmig-aaa-common-inum.sql
4. update-programs-verintmig-bo.sql
5. update-programs-verintmig-fo-cti.sql
6. update-programs-verintmig-fo-cti-15.sql (only from Verba 9.5)
7. update-programs-verintmig-fo-vox.sql
8. update-programs-verintmig-fo-vox-15.sql (only from Verba 9.5)
9. update-programs-verintmig-us.sql (only from Verba 9.5)
10. update-programs-verintmig-zzz-common.sql

Running the SQL scripts on the Verint database

Additionally, another SQL script must be executed on the Verint CentralContact database. If a DB backup was taken and the Verint databases were restored on the Verba SQL Server, then this script should be executed in the Verba SQL Server. So the programs this script will install are needed in the source Verint database.

This script is located at c:\Program Files\Verba\tomcat\webapps\verba\WEB-INF\verintmig\verintmig-download\verba-verint-centralcontact.sql, or can be downloaded from the Verba UI at the Verint Migration Source Database configuration page.

The script will add a new column to the Archive.dbo.Media table named verba_prio. **Before starting the migration, this column has to be populated.** Storage locations that are more likely to be available should be given a higher number.

Migration tool

The migration tool, available through the Verba user interface, provides the following features:

- Permission / Role-based access
- Multiple Verint database sources can be added
- For each database, multiple subsets have to be defined:
 - Front-Office (based on time and selected Verint datasource)
 - Back-Office (based on time and selected Verint datasource)
- Migration status information, configuration warnings (e.g. subsets configured does not cover all calls in the Verint database)
- Planning stage with data preview
- Data is migrated in monthly chunks
- The migration process can be paused and resumed later
- If the migration fails, it can be restarted from the last finished month
- Detailed logs
- The migration process is executed by the Web Application Service so the user can log off from Verba web UI and can turn their PC off
- No server restart is needed after the migration
- The performance of the Verba database can be degraded after the migration, if that happens, then the Verba Maintenance Job should be executed. This process might take several hours.
- The Verint databases are not changed, only four very simple helper procedures are installed (see Running the SQL scripts on the Verint database)

The Migration Tool migrates one call type (Back-Office calls or Front-Office calls) at a time. Once the first call type migration is complete, you are ready to migrate the remaining call type. The order in which you migrate the call data is not important.

Enabling the migration tool

The migration tool has to be enabled before the migration can take place.

Step 1 - Navigate to **System / Servers** or **System / Configuration Profiles** (in case you want to update the configuration profile used by the recording servers), then select the server which runs the Web Application service or the configuration profile.

Step 2 - Select the **Change Configuration Settings** tab and change the **Web Application / Miscellaneous / Verint Migration Enabled** setting to **Yes**.

Step 3 - Save the changes by clicking on the



icon.

Step 4 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.

Step 5 - The **Data / Verint Migration** menu item will be visible when the logged-in user has Verint Migration permission.

Source Databases

The menu opens the list of the Verint Migration Source Databases. In most cases, there will be one Source Database, but the system allows migrating from multiple databases.

Find and List Verint Migration Source Databases

[Add New Verint Migration Source Database](#)
[Upload New Column Mapping](#)
[Show Disabled Items](#)

Name begins with [Find](#)

Name	Verint Version	Linked Server	ID
100-sqldev	Verint v15.2 and Above	192.168.1.100\SQLDEV	1
DEV-MR	Verint v15.2 and Above	dev-mr.verbalabs.com	2
express-11	Verint v11.1 and v11.2 and v15.1 Legacy	FENYVESI\SQLEXPRESS	3

3 items found, displaying all items.

Export options: [Excel](#) | [RTF](#) | [PDF](#)

Click on the [Add New Verint Migration Source Database](#) link at the top right folder to add a new source database. First of all, the Verint version has to be specified: **Verint v15.2 and Above**.

When the Linked Server is empty, then the Verint databases (Archive, BPMAINDB, CentralContact, and CommonDB) have to be on the same server where the Verba database is. This can speed up the migration dramatically.

Details of a Source Database:

Verint Migration Source Database Configuration

Refresh
 Add New Subset
 Add New Verint Migration Source Database
 Back to Previous Page

▼ Basic Information

ID 2

Name * DEV-MR

Enabled * Yes

Verint Version * Verint v15.2 and Above

Linked Server dev-mr.verbalabs.com

Set to empty if the Verint databases are on the same server where the Verba database is.
 If a Linked Server is used, then the Server Options / RPC Out option needs to be set to True in the Linked Server configuration.
[Download CentralContact helper scripts](#)

Storage Targets Synchronized 4

Users / Groups [Synchronize Users](#)

Already Existing Users / Groups / Extensions will not be affected

▼ Subsets

Add New Subset

Type	Name	Status	Datasource	Processed Until	Interval	Total # of Days	Processed Days	Progress	Source Records	Imported Records	ID
Back Office (Telephony and Unified Communication)	Cisco	Planning	151: Cisco (-505013: Cisco Unified Call Manager)				0			0	8
Back Office (Telephony and Unified Communication)	avaya	Planning	51: Avaya (-505002: Avaya Communication Manager/Definity)				0			0	7
Front Office (Trader Voice)	IP Trade	Planning	101: IPTTrade (IP; -505041: IP Trade)				VOX: 0 CTI: 0		VOX: 0 CTI: 0	VOX: 0 CTI: 0	6
Front Office (Trader Voice)	IPC-Alliance	Planning	1: Alliance_DS (TDM; -505029: IPC Alliance)				VOX: 0 CTI: 0		VOX: 0 CTI: 0	VOX: 0 CTI: 0	5
Users	uuuu	Finished	Users, Groups, Extensions						9	7	4

Export options: Excel | RTF | PDF

[Save](#)

Creation Date: Nov 18, 2020, 3:47:46 PM
 Created By: Verba Administrator (Administrator)
 Last Modification Date: Nov 18, 2020, 3:49:03 PM
 Last Modified By: Verba Administrator (Administrator)
[View Change History](#)

The setup, the log entries, the calculated numbers, and basically everything is stored in database tables and will not be deleted after completing the migration.

The Storage Targets will be synchronized during the migration of the first subset.

The source data is divided into Subsets. A Subset can be either Back Office or Front Office, and only one Subset may run at a time. The v15.2 User migration also creates a new Subset in order to simply track the process and the log.

The “Total” and “Source” numbers will be calculated either when the subset runs for the first time, or when you click on the Update Numbers button.

Front Office (Trader Voice) and Back Office (Telephony and Unified Communication)

First of all, a Datasource has to be selected.

You can optionally set From and To times to narrow down the migrated time interval.

V Conversations Quality Management Workflows Communication Policies Reports Users Data System

Verint Migration Database Subset Configuration

[Add New Verint Migration Database Subset](#)
[Back to Previous Page](#)

Subset Details Preview Data VOX-Media Preview Data CTI-CDR

▼ Basic Information

Source Database LOCAL: (#1)
ID 2

Type * Front Office (Trader Voice)

Datasource * 1: UnigyV2 (IP: -505026: IPC Unigy)

Name * fo-01

From Clear

To Clear

Status Planning

Save Save and Run Delete

Creation Date: Jul 2, 2019 5:56:31 PM
Created By: Verba Administrator (Administrator)
Last Modification Date:
Last Modified By:
[View Change History](#)

* Indicates required item.

The column mapping is pre-configured and cannot be changed on the UI. If it has to be changed, then the new XML mapping file can be uploaded in the Verint Migration Source Databases List screen, using the **Upload New Column Mapping** link at the top right corner.

Data preview

A preview of the data (the first 100 records) is available on the Preview tab:

Verint Migration Database Subset Configuration

Subset Details **Preview Data**

inum	previnum	nextinum	Start Time	End Time	FormatId	From	avaya / Owner	Files
743001000000027.0000			2016-06-09 17:26:49.543	2016-06-09 17:27:56.543	4		1,10.156.15.17 :10.156.42.140	
743001000000034.0000			2016-06-09 17:28:50.02	2016-06-09 17:29:51.02	4		1,10.156.15.17 :10.156.42.140	CLMedia (
743001000000039.0000			2016-06-09 17:30:40.103	2016-06-09 17:30:52.103	4		1,10.156.15.17 :10.156.42.140	CLMedia (
743001000000042.0000			2016-06-09 17:31:40.857	2016-06-09 17:32:15.857	4		1,10.156.15.17 :10.156.42.140	

Running the migration

When the setup is complete and the Preview looks good, then use the **Save and Run** button to start the migration. The system will migrate one month at a time.

The **Logs** tab displays the progress and log messages:

V
Q
Conversations
Quality Management
Workflows
Communication Policies
Reports
Users
Data
System

Verint Migration Database Subset Configuration

Subset Details
Preview Data
Logs

Select Run:

Select Types: Messages SQLs

▼ Basic Information

Status Finished

Processed Until Jul 1, 2016 12:00:00 AM

Total # of Days 30

Processed Days 30

Progress 100%

Source Records 4

Imported Records 4

▼ Logs

Start Time	End Time	Affected Rows	Message
2019-07-08 11:12:24			Compute best_location_id
2019-07-08 11:12:24	2019-07-08 11:12:24		Create idx_tempmignums_hml index on ##inum_migrate_data
2019-07-08 11:12:24			Compute has_multiple_locations
2019-07-08 11:12:24			Transfer container
2019-07-08 11:12:24			Create indexes on ##inum_inum_location
2019-07-08 11:12:24			Transfer inum_location
2019-07-08 11:12:24	2019-07-08 11:12:24		About to generate topinums for related call association
2019-07-08 11:12:24	2019-07-08 11:12:24		Create indexes on ##inum_migrate_data
2019-07-08 11:12:24	2019-07-08 11:12:24	4	Transferred 4 BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			Transfer BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			About to migrate Back Office calls from ewarecalls.dbo.CSCMAvayaCallsView BETWEEN 2016-06-01 mapping 4
2019-07-08 11:12:24	2019-07-08 11:12:24	1	Transferred 1 BO INums BETWEEN 2016-06-01 17:28:00 AND 2016-07-01 00:00:00
2019-07-08 11:12:24			About to migrate Back Office calls from ewarecalls.dbo.CSCMAvayaCallsView BETWEEN 2016-06-01 mapping 4
2019-07-08 11:12:24			Time interval: 2016-06-01 17:28:00 - 2016-07-01 00:00:00
2019-07-08 11:12:24			Initializing the execution of 1 (type: bo)

The **Select Run** listbox contains one entry for one execution, so if the migration stopped or failed, and someone restarted, then a new entry will be inserted.

Use the **SQLs** checkbox to turn on detailed log entries with the actual SQL statements.

The execution can be paused by the **Pause** button. Pressing the button will not cause the termination immediately, but will change the status to **Pausing**. Once the migration of the current month finished, the status will go to **Paused**. The buttons are not refreshed automatically so if the Pause button is not visible while the migration is in progress, then go back to the list of the subsets and open the details again.

When the execution paused, finished, or failed, then the first tab will display the **Run Again** button that can be used to restart the migration of the Subset. Already migrated calls will not be migrated again, because they are saved in the verintmig_migrated_xxx tables.

One month is one transaction, and in case of an error in the middle, the whole transaction will be rolled back. In order to be able to effectively log to DB tables, we have to get out from the transaction, because otherwise, the log entries would not be visible to other DB sessions. In order to do this, a loopback Linked Server is created during the installation named verba_loopback.

If the execution fails, then the status of the Subset will be Failed, and the error message will be shown in the **Logs** tab. Unfortunately, there are errors that cannot be caught, and in that case, the subset will remain in the Running state. If you are sure that the process died, then click on the **Mark as Failed** button to set the state to Failed, then fix the problem and start the Subset again.

If a process is still running, then starting another one will throw an error: "Error during pr_verintmig_bo: Cannot acquire lock (Lock State: -1), probably another migration is still running (16, 1)"

Users, Extensions, and Groups

When migrating from Verint v15.2, the Users, Extensions, and Groups can be pulled from the Verint database. The process can be initiated by clicking on the Synchronize Users button on the Source Database details screen. The details (should Groups and Extension be pulled or not) can be configured on a new Subset configuration screen:

Verint Migration Database Subset Configuration [Back to Previous Page](#)

Subset Details

▼ Basic Information

Source Database DEV-MR: dev-mr.verbalabs.com (#2)

ID

Datasource * Users Groups Extensions

Name *

Status **Planning**

Save

* Indicates required item.

After the Subset saved, use the **Save and Run** button to start the migration.

Users

The created Users will inherit the Language and Timezone settings from the User who is running the migration, and the Standard User Role will be granted to them.

The Verint identifier will be stored in the Verba database, so during call migration, the process will try to assign the calls to a User based on this information. If no migrated User found for a call, then the Extension and User setup will be used for user association.

Extensions

The Verint Users' Extensions can be migrated too, will be set up as Number/Address type with Voice recording enabled.

Groups

The Verba groups are not sorted in a hierarchy tree, so the Group Name will contain the full path to the groups:

Group Name ↕	Metadata Template ↕	Data Source ↕	Authorization Workflow ↕	ID ↕
Root Group (#1)	Default	Verint Migration		2
Impact 360 (#1)	Default	Verint Migration		3
Your Company Name (#1)	Default	Verint Migration		4
Your Company Name / IPC_Org (#1)	Default	Verint Migration		5
Your Company Name / Cisco (#1)	Default	Verint Migration		6

The User-Group membership information is also migrated, but the call visibility scope is not. No migrated user will be a Supervisor in Verba.

Post-migration tasks

After the migration completed, the following items must be completed and checked:

- If the media files are stored on EMC Centera, then copy the PEA file to a location accessible by the Verba Media Repository Servers and change the configuration of the Verba Storage Targets to point to the new PEA file location
- If the media files are stored on the Hitachi Content Platform, then the Verba Storage Targets have to be configured with the correct API User and Password, because the Password was not copied from the Verint database
- Verify that calls are searchable and accessible through the Verba system.
- Verify that all Verint archive locations are available as storage targets in the Verba system.
- Verify that all calls are migrated by checking the information displayed on the subsets page.

Removing imported calls from Verba and resetting the import

If the migrated calls should be deleted and the Subset status should be "Planning", then use the manual-verintmig-delete-subset-calls.sql can be found on the Verba server in the Verba\resources\db\util folder. Set the ID of the Subset at the beginning of the file:

```
@subset_id INT = 0 -- TODO set subset id
```

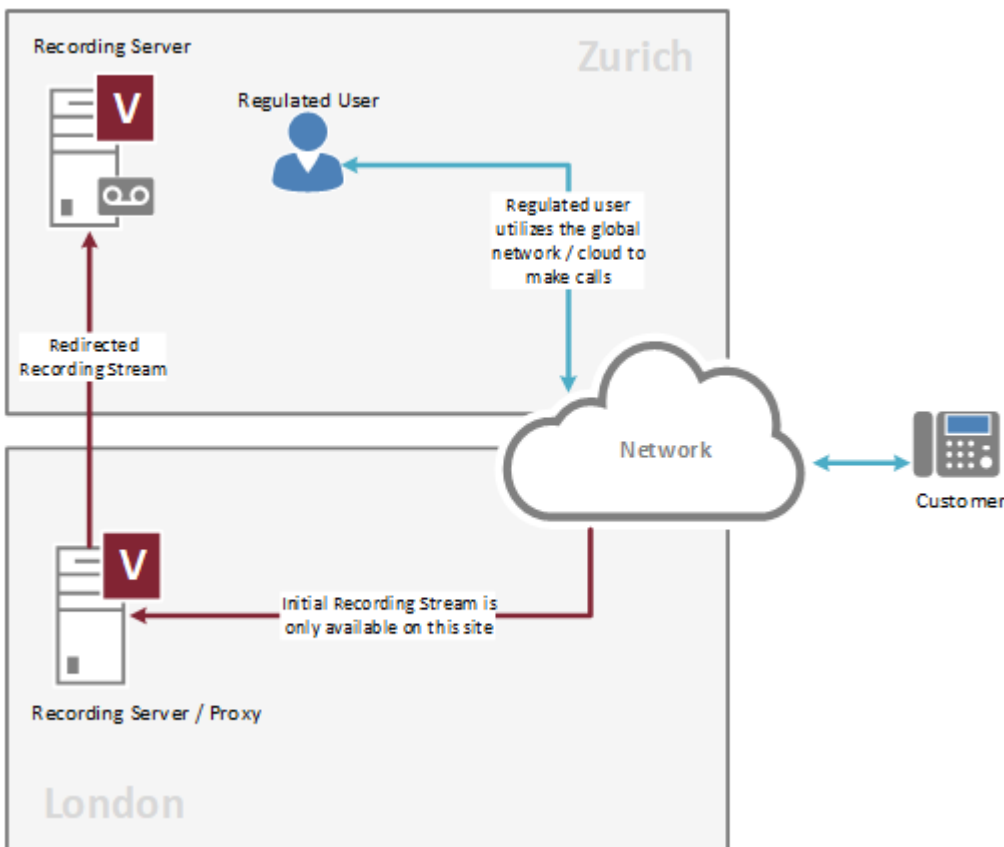
Then execute the SQL in SQL Server Management Studio. The script will delete all calls of the Subset from the Verba database, and will reset the state of the Subset to "Planning".

Sites

- [Overview](#)
- [Enable site configuration](#)
- [Site and site group configuration](#)
 - [Creating a new site](#)
 - [Creating a new site group](#)
- [Assigning users to sites and site groups](#)
 - [Assigning users on the site or site group configuration page](#)
 - [Assigning users by Active Directory synchronization](#)
- [Assigning recorded extensions to sites or site groups](#)
- [Assigning server to sites](#)

Overview

Sites link users (their recorded lines/URIs/User IDs) and servers together to configure a preference for the location of the recording. Regulations in many countries require in-country recording which often interpreted as the recording process must take place in the country (moving WAVE file across borders is not allowed, streaming is OK). Complex networks and communication systems are not always able to meet this requirement and recording streams for specific regulated users might only be available on locations that are not in-country and the recording streams have to be redirected to the right location (server).



Sites can be organized into site groups, e.g. 2 data centers in a city/country. Recording Servers can understand site/location information for regulated/recorded users and can redirect recording streams to another server configured for the site which the user belongs to.

- Supported integrations:
- Symphony (using SIP 300 REDIRECT to route the SIP INVITE to the preferred Recording Server)

When multiple Verba instances are deployed, and the site information has to be shared across the instances, a Verba Hub has to be deployed. For more information, see [Hub](#).

Enable site configuration

Site configuration is disabled by default. In order to enable site configuration for an administrator user, the necessary permission has to be enabled in the role configuration. Follow the steps below to enable site configuration in a role.

Step 1 - In the Verba Web Interface go to **Users / Roles**

Step 2 - Select the role from the list (e.g, System Administrators)

Step 3 - On the **Role Permissions** tab, scroll to **Administrative Permissions / Operation and Maintenance**

Step 4 - Change the **Site Configuration** option to **Read, Update, Create, Delete** to grant full permission to sites configuration

Step 5 - Click on **Save** to save the new role configuration. Users with this role assigned will have access to site configuration after the next login.

Site and site group configuration

Creating a new site

To add a new site, follow the steps below.

Step 1 - In the Verba Web Interface go to **System / Sites**

Step 2 - Click on the **Add New Site** link on the top right

Step 3 - Enter a unique **Name** for the site. If you are using Active Directory synchronization, the system can automatically assign users to sites based on a selected AD attribute. Make sure you are adding sites with the same name.

Step 4 - Click **Save**

Step 5 - Assigning users, extensions and servers to the site, see below

Creating a new site group

Site groups can have multiple sites where each site can be configured as a Primary or a Backup (Secondary) site. In the case of 2N recording, the Primary recorder always tries to redirect to another recorder on a Primary site.

To add a new site, follow the steps below.

Step 1 - In the Verba Web Interface go to **System / Site Groups**

Step 2 - Click on the **Add New Site Group** link on the top right

Step 3 - Enter a unique **Name** for the site group

Step 4 - Click **Save**

Step 5 - Assign sites to the site group on the **Assign Sites** tab. Select a site from the **Available Sites** list, select the priority of the site from the drop-down list and then press **Add**.

Step 6 - Repeat the previous step for each site you want to add to the site group

Step 7 - Click **Save**

Assigning users to sites and site groups

By assigning users to sites or site groups, the system will record the conversations of the users on the servers assigned to the same site or site group. The user assignment automatically assigns the associated extensions of the users to the site or site group. There is no need to add extensions individually.

A user can be assigned to a single site or site group.

Users can be added to sites or site groups in the following ways:

- Using the site or site group configuration screens
- Using the user configuration page
- Using Active Directory synchronization, a new site or site group attribute can be configured which maps to an AD field (based on the name of the site or site group)

Assigning users on the site or site group configuration page

To assign a recorded user to a site on the site configuration page, follow the steps below.

Step 1 - In the Verba Web Interface go to **System / Sites** or **Site Groups**

Step 2 - Select the site or site group, which the user(s) will be added to, from the list

Step 3 - Click on the **Assing Users** tab

Step 4 - Enter the name of the user in the **Search Users** input field. The system will automatically filter the list of users after entering the first characters. Select the user from the list.

Step 5 - Repeat the previous step for each user you want to add to the site or site group

Step 6 - Click **Save**

Assigning users by Active Directory synchronization

To assign a recorded user to a site or site group using Active Directory synchronization, follow the steps below.

Step 1 - Create a new **Active Directory Synchronization Profile** under **Users / Active Directory Synchronization** or modify an existing one. Follow [Active Directory synchronization](#) for more information.

Step 2 - In the Active Directory Synchronization Profile configuration, define the Active Directory attribute, which will be mapped to sites or site groups, under **Synchronized AD Attributes Mapping / Site Attribute**. The mapping is based on the name of the sites or site groups. If the AD attribute contains a site or site group that is not configured in the system, the AD synchronization process will automatically create a new site and assign the user to it.

Step 3 - Alternatively, select a site or site group from the **Site** drop-down list which will be used when the **Site Attribute** is not set up or the attribute is not filled in for a user in the AD.

Assigning recorded extensions to sites or site groups

The user assignment automatically assigns the associated extensions of the users to the site or site group.

An extension can be assigned to a single site or site group. Extensions can be added to sites or site groups in the following ways:

- Using the site or site group configuration screens
- Using the extension configuration page

To add recorded extensions (lines/URIs/User IDs) to a site or site group on the site or site group configuration page, follow the steps below.

Step 1 - In the Verba Web Interface go to **System / Sites** or **Site Groups**

Step 2 - Select the site or site group, which the extension(s) will be added to, from the list

Step 3 - Click on the **Assing Extensions** tab

Step 4 - Enter the extension in the **Search Extensions** input field. The system will automatically filter the list of extensions after entering the first characters. Select the user from the list.

Step 5 - Repeat the previous step for each extension you want to add to the site or site group

Step 6 - Click **Save**

Assigning server to sites

Servers can be assigned one by one to one or more sites (not site groups) in the following ways:

- Using the site configuration screens
- Using the server configuration page

To add server(s) to a site on the site configuration page, follow the steps below.

Step 1 - In the Verba Web Interface go to **System / Sites**

Step 2 - Select the site, which the server(s) will be added to, from the list

Step 3 - Click on the **Assing Servers** tab

Step 4 - Select one or more servers from the list and click on the **>>** button to assign them to the site.


Step 5 - Click **Save**

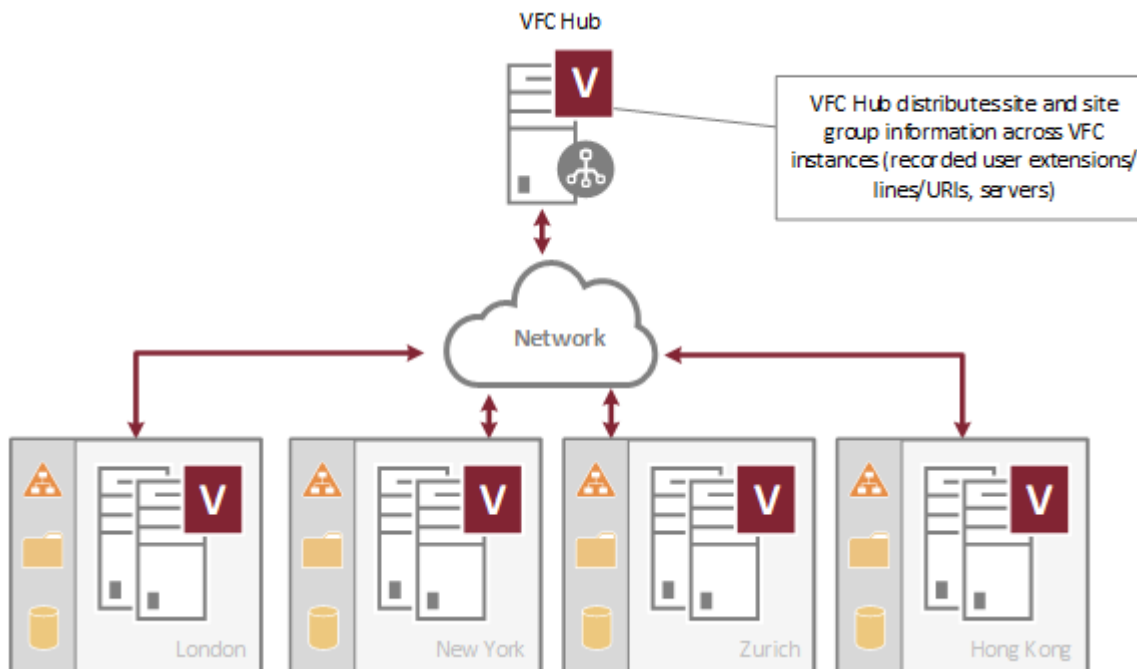
Hub

- [Overview](#)
- [Deploying a Hub](#)
 - [Enable Hub role](#)
- [Hub registration](#)
 - [Enable hub registration](#)
 - [Registering an instance](#)
- [Distributing the configuration across instances](#)
 - [Monitoring configuration updates](#)

Overview

Hub allows using sites across multiple Verba instances. Recording Servers can redirect recording streams across multiple Verba instances (regions with separate Verba deployments). Instances are registered in the Hub and site information with associated recorded extensions (line/URI/User ID) and servers are shared across all registered extensions. The Application Servers (Media Repository) in the instances initiating the connection and the configuration update to the Hub and then the Hub distributes the new configuration to all instances. For more information on site and site group configuration, see [Sites](#).

-  Supported integrations:
Symphony (using SIP 300 REDIRECT to route the SIP INVITE to the preferred Recording Server)



Deploying a Hub

A Hub is a separate Verba instance with one or more Application Servers (Media Repository) and a separate database. A Hub cannot use an existing Verba instance.

To deploy a Hub, follow the installation guide:

- [SQL Server requirements](#)
- [Prerequisites](#)
- [Installing a Verba Media Repository](#)

Multiple Media Repository servers can be deployed to allow load balancing and failover. In this case, a load balancer has to be deployed in front of the servers.

Enable Hub role

Once the Media Repository server(s) are deployed, the Hub role has to be manually enabled:

Step 1 - On the Media Repository server, open **Regedit**

Step 2 - Navigate to **HKLM\Software\Verba**

Step 3 - Change the **Hub** key to 1 (if it doesn't exist, create a new key (DWORD))

Step 4 - Restart the **Verba Web Application Service**

Step 5 - Repeat the previous steps for each Media Repository server in the Hub

Hub registration

To connect a Verba instance to the Hub, the instance has to be registered to the Hub.

Enable hub registration

Hub registration is disabled by default. In order to enable hub registration for an administrator user, the necessary permission has to be enabled in the role configuration. Follow the steps below to enable hub registration in a role.

Step 1 - In the Verba Web Interface go to **Users / Roles**

Step 2 - Select the role from the list (e.g, System Administrators)

Step 3 - On the **Role Permissions** tab, scroll to **Administrative Permissions / Operation and Maintenance**

Step 4 - Change the **Site Configuration** option to **Read, Update, Create, Delete** to grant full permission to sites configuration

Step 5 - Click on **Save** to save the new role configuration. Users with this role assigned will have access to site configuration after the next login.

Registering an instance

To register an instance to the Hub, follow the steps below.

Step 1 - In the Verba Web Interface of the instance which has to be registered, go to **System / Hub**

Step 2 - Enter the information required for the registration. See the description of the fields below:

Field	Description
Local Instance Name	Unique name of the instance, which will appear on the Hub

Local Instance Web Application URL	Web Application URL of the instance. If you have multiple Media Repository serves in the instance, enter the root URL which is configured for the load balancer.
Hub API URL	URL of the Media Repository server(s) in the Hub. If you have multiple Media Repository serves in the Hub, enter the root URL which is configured for the load balancer. <i>https://HUB_FQDN:PORT/verba</i>
Hub API User	API user name configured on the Hub
Hub API Password	API user password

Step 3 - Click **Save**

Step 4 - Click on the **Test Connection** button to validate connectivity with the Hub. If the connection test fails, check the firewall and network connection with your systems/network administrator.

Step 5 - Click on the **Register** button to initiate the registration.

Distributing the configuration across instances

The Hub automatically distributes the site, site group, user, extension and server configuration across the registered instances. The configuration update is triggered by updating the related configuration on one of the instances. When the related configuration is updated, the Apply Configuration feature will list the Hub as a target for the new configuration (among all local servers deployed for the instance). After the **Execute Selected Tasks** button is preseed, the instance will send the new configuration to the Hub and the Hub will trigger the configuration update in all other registered instances.

Monitoring configuration updates

Configuration updates on the instances can be monitored by logging into the Hub and navigating to **System / Instances**.

In the list, you can find all registered instances with the following information:

Field	Description
Name	The name of the instance (provided during registration)
Web Application URL	Web Application URL of the instance
Configuration Last Received	Date and time of receiving the last configuration update from the instance
Last Contacted	Date and time of last configuration query for the instance
Pending Tasks	List of configuration updates from instances which are not yet applied on the instance