Verint Verba Collaboration Compliance Platform

This document includes chapters exported from the online Verba Knowledge Base. For the latest online version of the content ofthis document, please visit kb.verba.com

Advanced Compliance Guide

This guide contains articles about the features in Verba that were created specifically to make it possible for organizations to comply with regulatory requirements.

License requirements

In order to use some of the capabilities described in this guide, all recorded users should have the user add-on called **Verba Add-on Advanced Compliance License**.

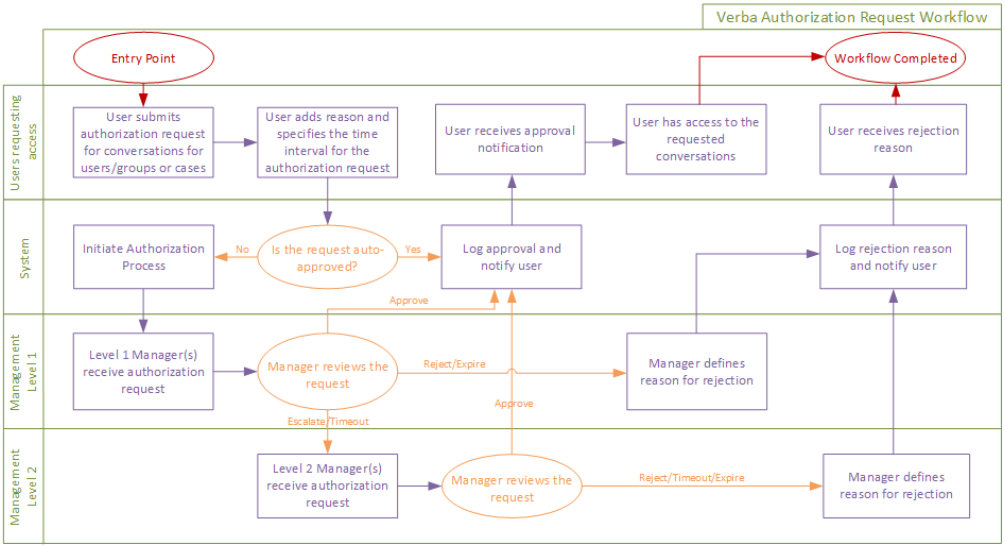
Note! This add-on license is also required for some of the supported external Storage Targets. For details please review the Storage targets article.

Approval Workflows

The Approval Workflows module in the system makes it possible for end users to request access to certain conversations. Their managers can then approve or reject the request based on the reason explanation that the users submit. The managers can also choose to escalate the authorization workflow to the next level if they cannot decide on the appropriate action. The managers one level higher can make the decision in that case.

Access can be requested based on users/groups, conversations marked with a specific label or conversations in a certain case.

The diagram below shows the architecture of the approval workflows.



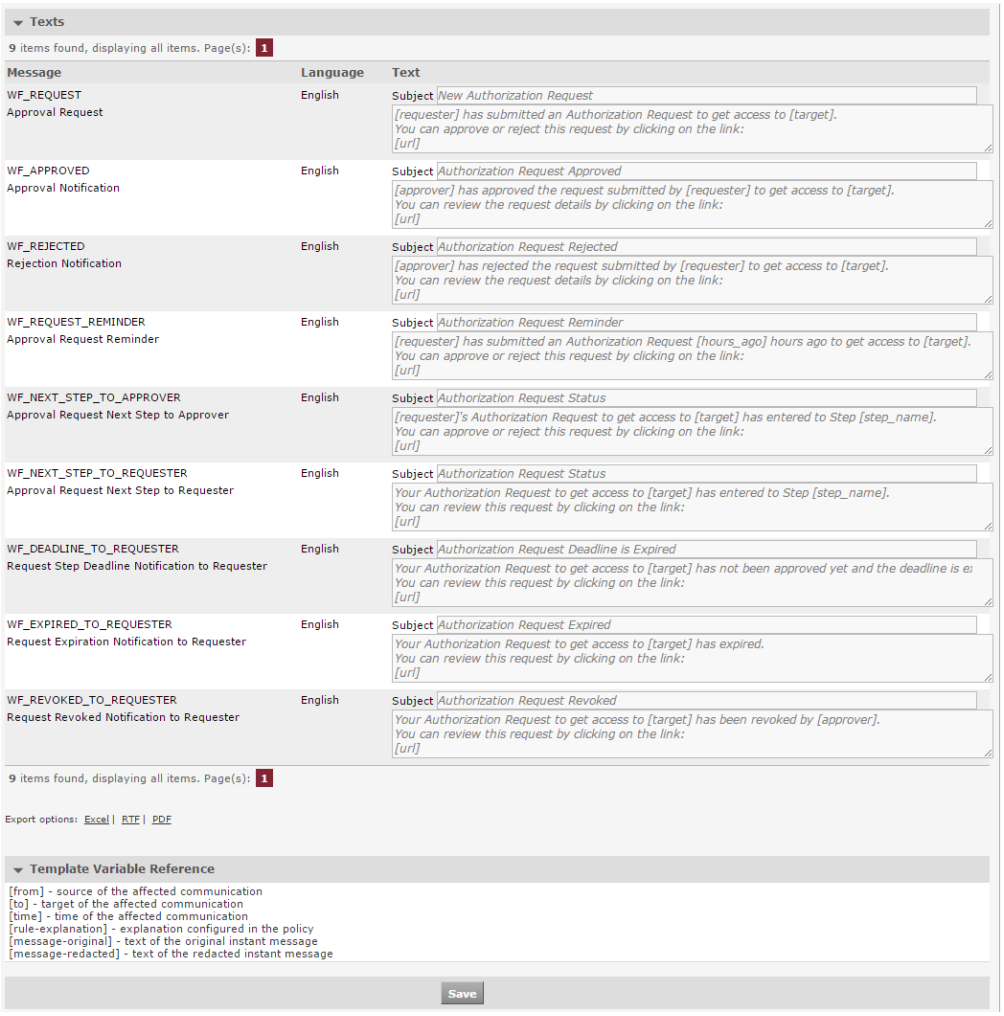
The articles in the Approval Workflows section showcase and describe what Approval Workflows (Compliance Workflows) are, how they can be configured and used throughout the system.

- Approval Workflow Message Templates
- Assigning Workflows to Users
- Authorization Requests
- Creating a Workflow

Approval Workflow Message Templates

Approval Workflow Message templates define what texts should be displayed for the users when progressing through the approval process.

To add new templates or change the existing ones, in the menu structure navigate to **Workflow -> Workflow Message Templates**, then click on the **Add New Template** button in the top-right corner.



Each event has a different text associated to it. These messages are sent to the appropriate users in email.

The texts are also different for each language that is defined in the template. New languages can be added by clicking on the **Add New Language** button.

> Notifications will be sent to users in their own language that is defined on the user configuration page

Data can be dynamically inserted into the messages at the time of the notification being sent. Refer to the *Template Variable Reference* section at the bottom of the page to see what variables can be inserted this way.

To see how the template can be used for certain workflows and how the default language can be selected refer to the Creating a Workflow article.

Assigning Workflows to Users

Overview

This page describes how the administrators can decide which workflow should each user go through to gain access to conversations.

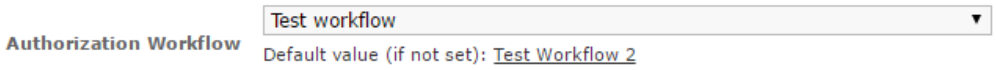
To see how workflows can be created refer to the Creating a Workflow article.

Three factors determine which workflow will be used for a certain user.

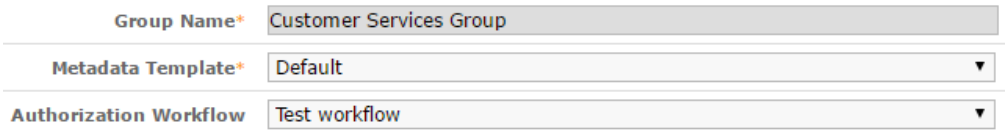
- Workflow defined on the configuration page of the user
- Workflows assigned to the Groups that the user is part of
- The priority of workflows, that can be configured when creating a workflow.

Configuration

If a workflow is defined on the configuration page of the user, then this workflow will be used.



If there is no workflow defined on the user configuration page, then the workflow will be selected from the workflows that are assigned to the Groups that the user is part of. From these workflows, the one with the highest priority will be selected.



When creating a workflow, the priority can be configured for each one. For more information refer to the Creating a Workflow article

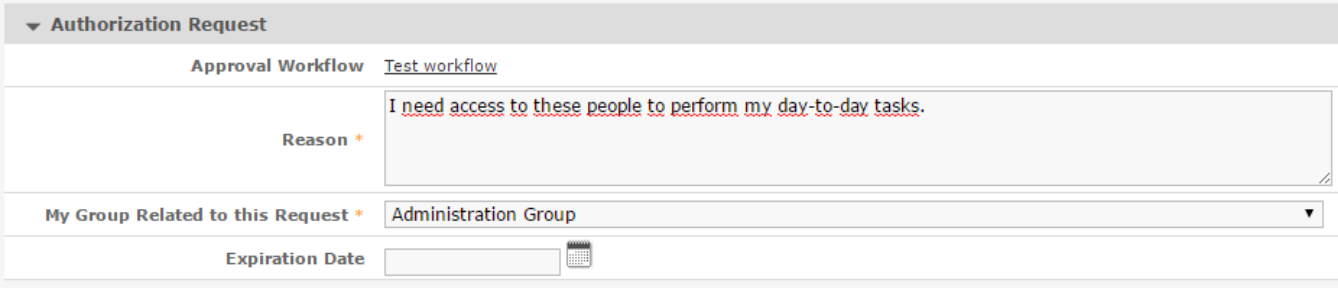
Authorization Requests

Users can request access to conversations based on users/groups, cases and labels.

In the menu, navigate to **Workflows -> Request Access** menu. If there is an existing workflow based on the user or group settings of the logged in user, then the **Requested Data** drop-down menu will appear. Select one of the available options:

- **Request Access to Users/Groups**
- **Request Access to Case**
- **Request Access to Label**

Once the Request Data setting is set, the workflow details appear. At the Authorization Request section, general information has to be provided.

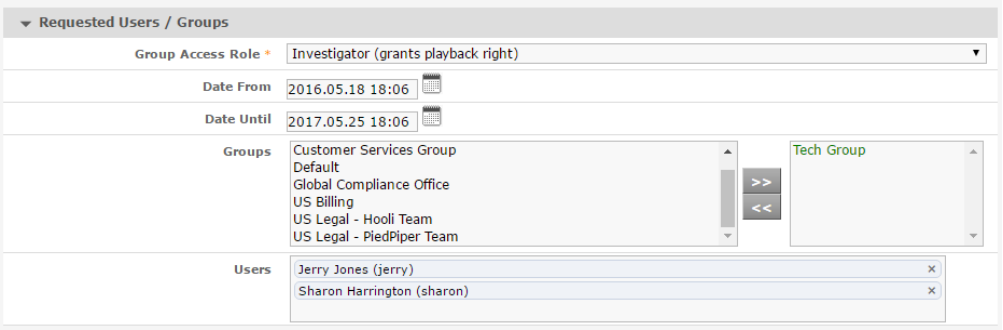


Line Item	Description
Approval Workflow	This request will go through the steps of the approval workflow that is displayed in that line
Reason	The users need to specify why they are requesting access to conversations. The approvers will see this comment and can decide based on this if the access request is valid or not
My Group Related to this Request	Which Group's Manager needs to approve the request. This option only appears if the workflow has been configured with the option *Group Manager(s) of Requester* for the approvers. For more details refer to the Creating a Workflow artic le
Expiration Date	The authorization request will be automatically dismissed if it has not been approved by the Expiration Date

Requesting Access to Conversations

The following sections describe the required fields based on the option selected at the **Requested Data** setting.

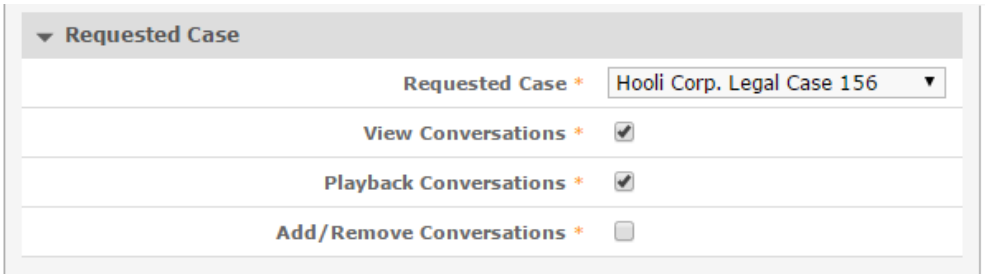
Request Access to conversations of certain Users/Groups



Line Item	Description

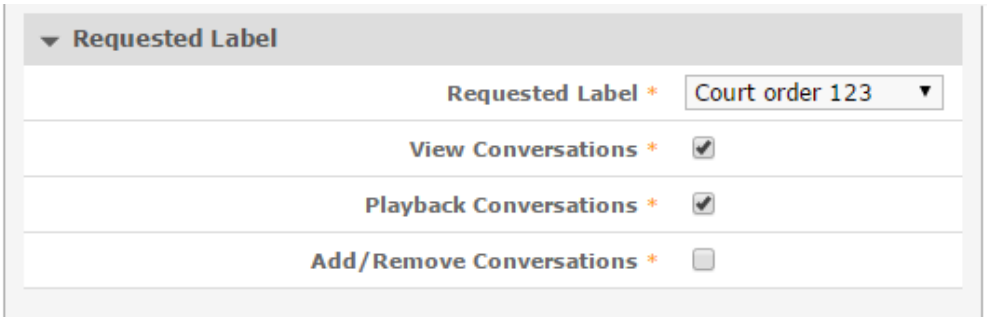
Group Access Role	Defines what type of access is required • **Supervisor** - The user will be able to see the conversations that he is granted to access to, but he will not be able to listen to the conversations. • **Investigator** - The user will be able to see and listen to the conversations that he is granted access to
Date From	Access will be granted to conversations that took place after this date
Date Until	Access will be granted to conversations that took place before this date
Groups	Access will be granted to the conversations of the groups that are moved to the right pane
Users	Access will be granted to the conversations of the users that are added here

Request Access to conversations in certain Cases



Line Item	Description
Requested Case	Access will be granted to the conversations in this Case
View Conversations	The user will be able to see the conversations, but this does not include playback rights
Playback Conversations	The user will be able to listen to the conversations
Add/Remove Conversations	The user will be able to Add/Remove conversations to/from this Case (permission will be given to Add/Remove the labels that belong to this case)

Request Access to conversations that have been marked with specific Labels



Line Item	Description
Requested Label	Access will be granted to the conversations that are marked with this Label
View Conversations	The user will be able to see the conversations, but this does not include playback rights
Playback Conversations	The user will be able to listen to the conversations
Add/Remove Conversations	The user will be able to Add/Remove this Label to/from conversations

If everything is set, click on the **Save** button to submit the workflow.

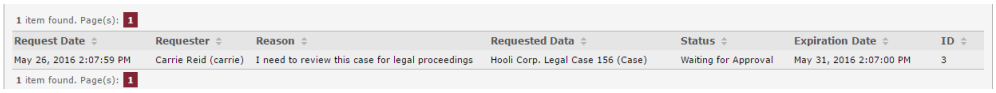
Displaying Submitted Requests

Users can see the submitted requests under the **Workflow > Requests** menu item. The following filters are available:

- **My Requests** - Users can see the requests that they have submitted
- **All Requests** - Users can see the requests that have been submitted. (Only those are displayed that the user has access to)
- **Requests to Approve** - The requests that are currently waiting to be approved by the logged in user

Requests to Approve page

The Authorization Requests are displayed on this page that the logged in user has the rights to approve.

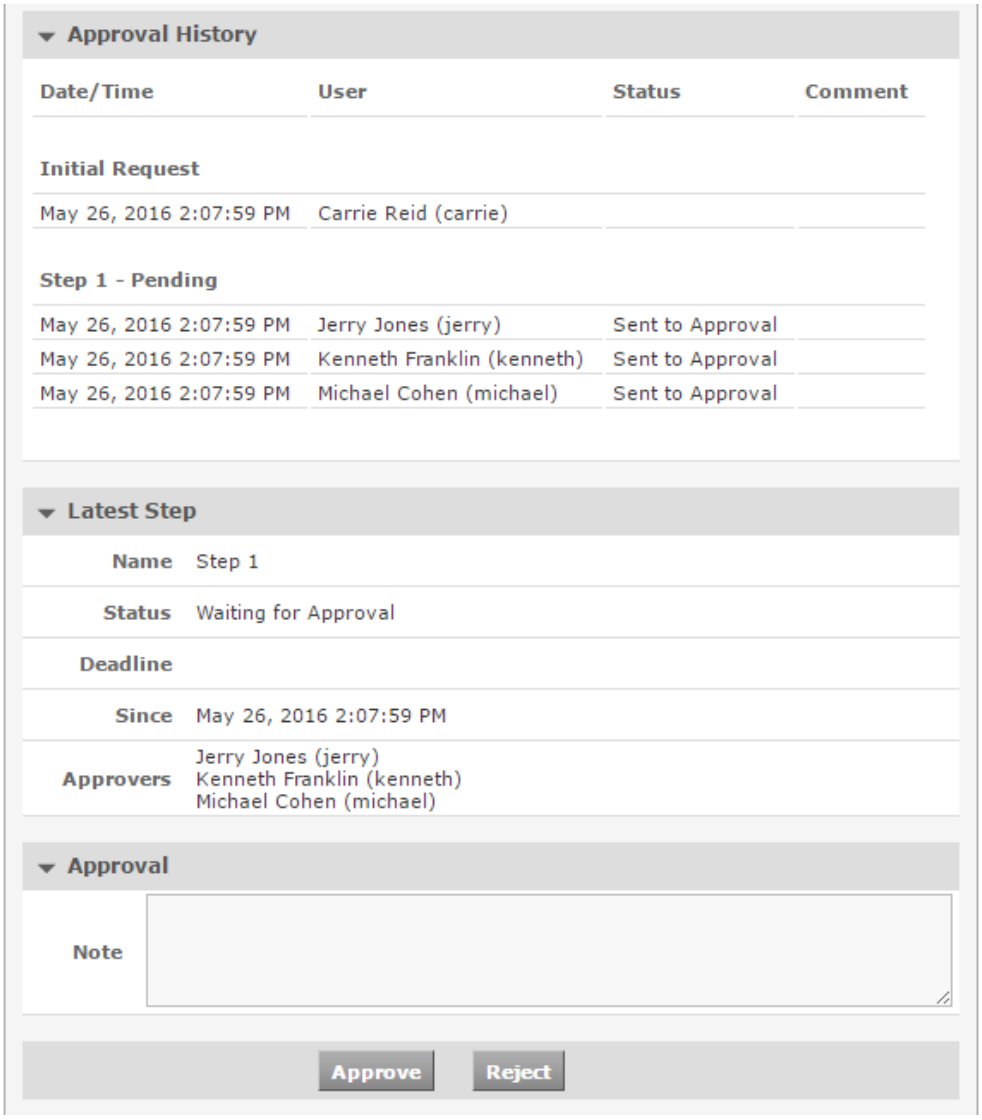

1 item found. Page(s): 1

Request Date	Requester	Reason	Requested Data	Status	Expiration Date	ID
May 26, 2016 2:07:59 PM	Carrie Reid (carrie)	I need to review this case for legal proceedings	Hooli Corp. Legal Case 156 (Case)	Waiting for Approval	May 31, 2016 2:07:00 PM	3

1 item found. Page(s): 1

It shows who submitted the request and when, displays the reason that the requester entered and what data the user would like to gain access to.

The request can be approved, rejected or escalated after clicking on the request.



Section	Description
Approval History	In the Approval History section, it is clearly visible who submitted the request and which steps the workflow has progressed through so far. The events are also listed, like who received the Approval Request or who accepted, escalated or rejected the request.
Latest Step	In the Latest Step section, the system shows which step the workflow is currently in and what is needed to complete this step. In the Approvers line, all of the people are listed who have the right to approve this request. Only one person needs to evaluate the request (accept, escalate, reject)
Approval	In the Approval section, the approver can comment on why he is making the given decision (For example explaining why the user cannot gain access to what has been requested)

Configuring Workflow Rights

The user rights connected to compliance workflows can be configured for each role in the system.

Regular User Permissions section

Preview Conversation - This will only give the user the ability to play back the first part of the conversation (Duration is configurable, default is 15 seconds). Based on that they can submit an authorization request for those conversations.

Send Authorization Requests - Gives the user the right to submit authorization requests as shown in the first part of this article

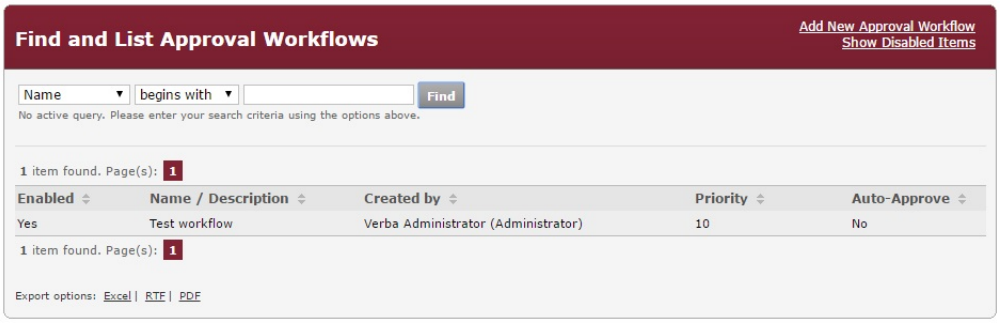
View Authorization Requests - Gives the user the right to see the authorization requests that have been submitted by other people. In most cases this is a right for a system supervisor

Administrative Permissions

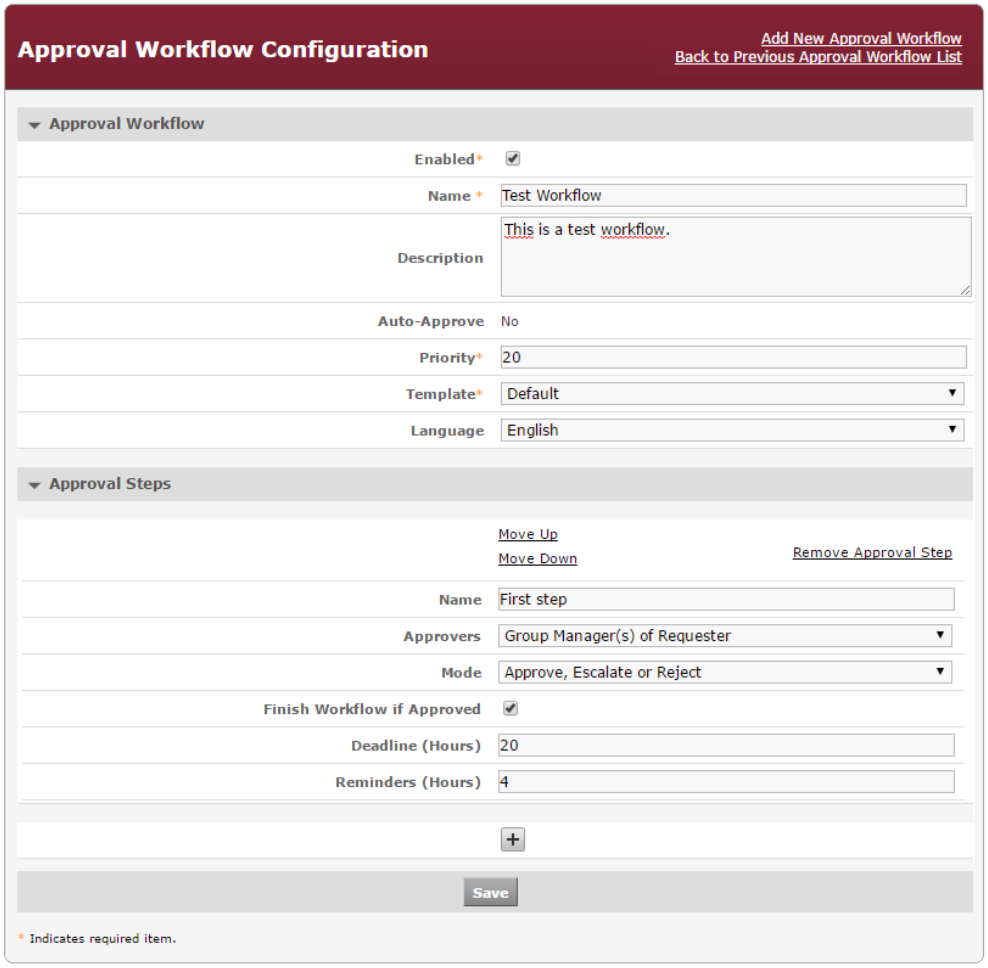
Workflow Configuration - Each person can have different rights regarding the configuration of compliance workflows. The following rights can be given: Read, Update, Create, Delete

Creating a Workflow

In the menu navigate to **Workflows -> Workflows**. This page lists the previously created Workflows



To add a new Workflow, click on the **Add New Approval Workflow** button at the top-right corner of the page



Line Item	Description
Name	When a user is requesting access to certain conversations using this workflow, this name will appear
Description	Describes what type of access and which people this workflow is being used for
Auto-Approve	This field automatically changes to Yes when there are no approval steps added below and changes to No when there is at least one step added. This changes after the workflow has been saved

Priority	This number defines which workflow will be used for an access request when there is more than one workflow available for a certain requester. The workflow with the highest priority will be selected (highest number)
Template	Shows which Approval Workflow Message template's text will be used throughout the approval process. For more information refer to the Approval Workflow Message Templates article
Default Language	The notifications throughout the approval workflow will be sent in the language to the user that is defined on the user configuration page. However, if the user's language is not defined in the selected template, then the message will be sent in the default language that is set here.

New workflow steps can be added by clicking on the

icon, or can be removed with the ***Remove Approval Step*** link. The workflow will progress through these steps (from top to bottom). You can change the sequence of the steps with the ***Move Up*** and ***Move Down*** buttons.

Line Item	Description
Name	This name will be displayed for this step in the approval process
Approvers	Determines which people will be able to decide what happens in this phase (step) of the request (approve, escalate or reject) • **Selected User(s)** - The authorization request will be sent to the selected users • **Group Manager(s) of Selected Group(s)** - The authorization request will be sent to the manager(s) of the selected group(s) • **Group Manager(s) of Requester** - The authorization request will be sent to the manager(s) of the requesting user. If the user is part of more than one group, then he will be able to select which group's manager the request should be submitted to
Mode	Determines what actions the Approvers are able to make in this phase (step) of the request • **Approve or Reject** - The manager can either approve or reject the request • **Approve, Escalate or Reject** - The manager can approve, reject or escalate the request. In the case of escalation the access request transitions to the next step • **Escalate or Reject** - The manager does not have the right to approve, he can only reject the request or escalate it to the next workflow step
Finish Workflow if Approved	If this checkbox is checked, then upon the approval of this step the workflow is completed, the user gains access. If the checkbox is left unchecked then upon approval of this step the approval process moves to the next step in the workflow
Deadline (Hours)	The access request step will be valid for the amount of time (hours) defined here. After the deadline is passed, the request is automatically escalated to the next step in the process, or if there are no additional steps after the current one, then the request is rejected with a timeout event
Reminders (Hours)	The system will send reminders of this approval step pending to the manager

For information on which workflow is selected for each user when submitting requests refer to the Assigning Workflows to Users article

Cases

Cases are collections of conversations that have been tagged with one or more of the labels belonging to the case. They are used to identify a specific set of conversations, make them easily searchable and extend List or Play access to them.

> To use cases, it is important to have a good understanding of Labels. please refer to the corresponding section of the Verba Administration Guide.

Cases are created using the Case Configuration page by choosing the included labels, users and type of access.

To easily limit conversation search and listing to a specific case, use the Case Context setting on the Search page.

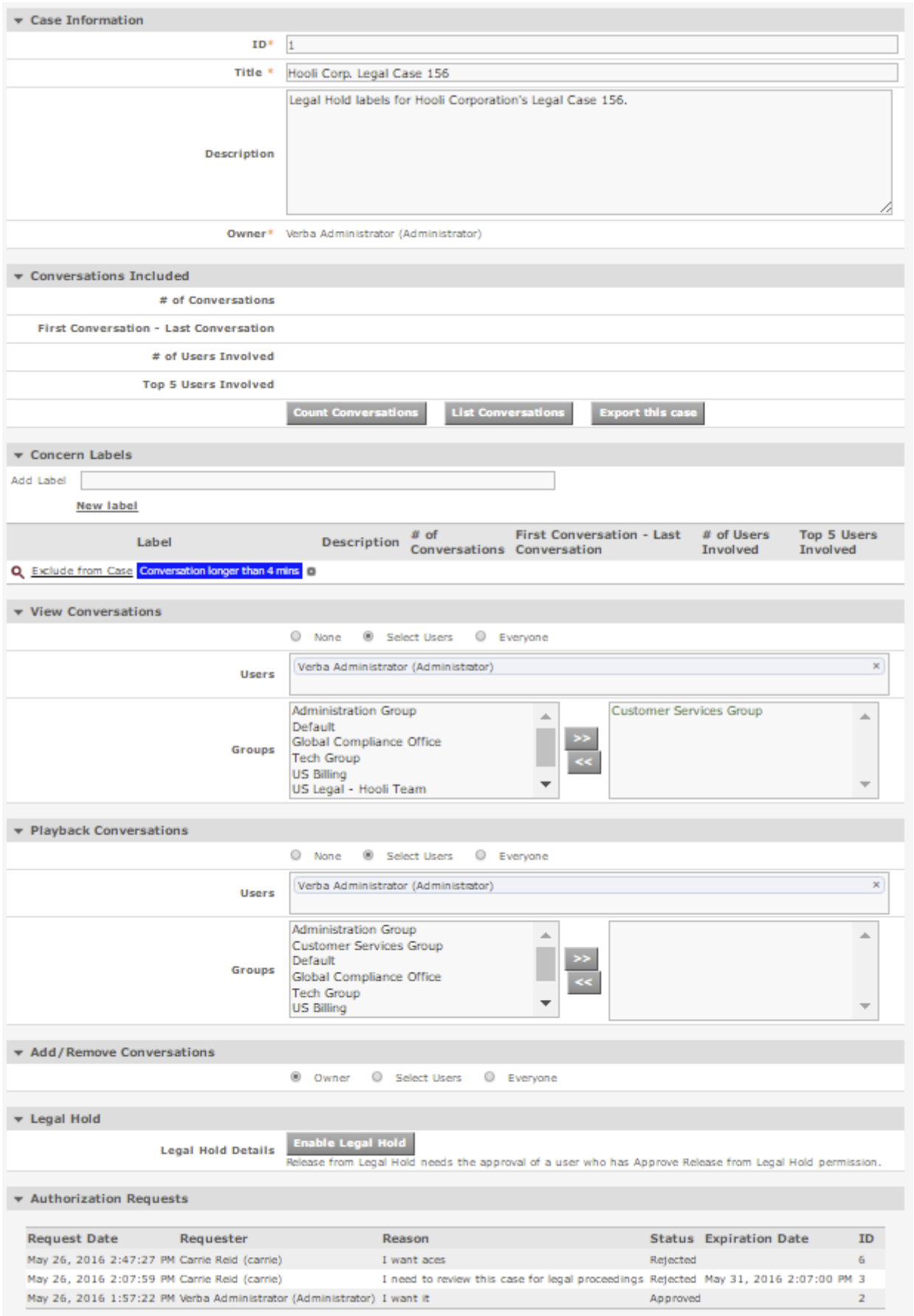
- Case Configuration
- Case Context

Case Configuration

This article contains details about the Case Configuration page of the Verba Web Interface.

To manage Cases, go to **Compliance --> Cases** in the Verba Web Interface. Click on any of the Cases in the list to edit an existing Case or click **Add New Case** to create a new one.

The screenshot below is an example of the Case configuration page. Below are the detailed descriptions of each configuration option available on the page.


Case Information
ID*
1
Title *
Hooli Corp. Legal Case 156
Description
Legal Hold labels for Hooli Corporation's Legal Case 156.
Owner*
Verba Administrator (Administrator)
Conversations Included
# of Conversations
First Conversation - Last Conversation
# of Users Involved
Top 5 Users Involved
Count Conversations
List Conversations
Export this case
Concern Labels
Add Label
New label
Label
Description
# of Conversations
First Conversation - Last Conversation
# of Users Involved
Top 5 Users Involved
Exclude from Case
Conversation longer than 4 mins
View Conversations
None
Select Users
Everyone
Users
Verba Administrator (Administrator)
Groups
Administration Group
Default
Global Compliance Office
Tech Group
US Billing
US Legal - Hooli Team
>>
<<
Customer Services Group
Playback Conversations
None
Select Users
Everyone
Users
Verba Administrator (Administrator)
Groups
Administration Group
Customer Services Group
Default
Global Compliance Office
Tech Group
US Billing
>>
<<
Add/Remove Conversations
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.
Authorization Requests
Request Date
Requester
Reason
Status
Expiration Date
ID
May 26, 2016 2:47:27 PM Carrie Reid (carrie) I want aces Rejected 6
May 26, 2016 2:07:59 PM Carrie Reid (carrie) I need to review this case for legal proceedings Rejected May 31, 2016 2:07:00 PM 3
May 26, 2016 1:57:22 PM Verba Administrator (Administrator) I want it Approved 2

Configuration Options

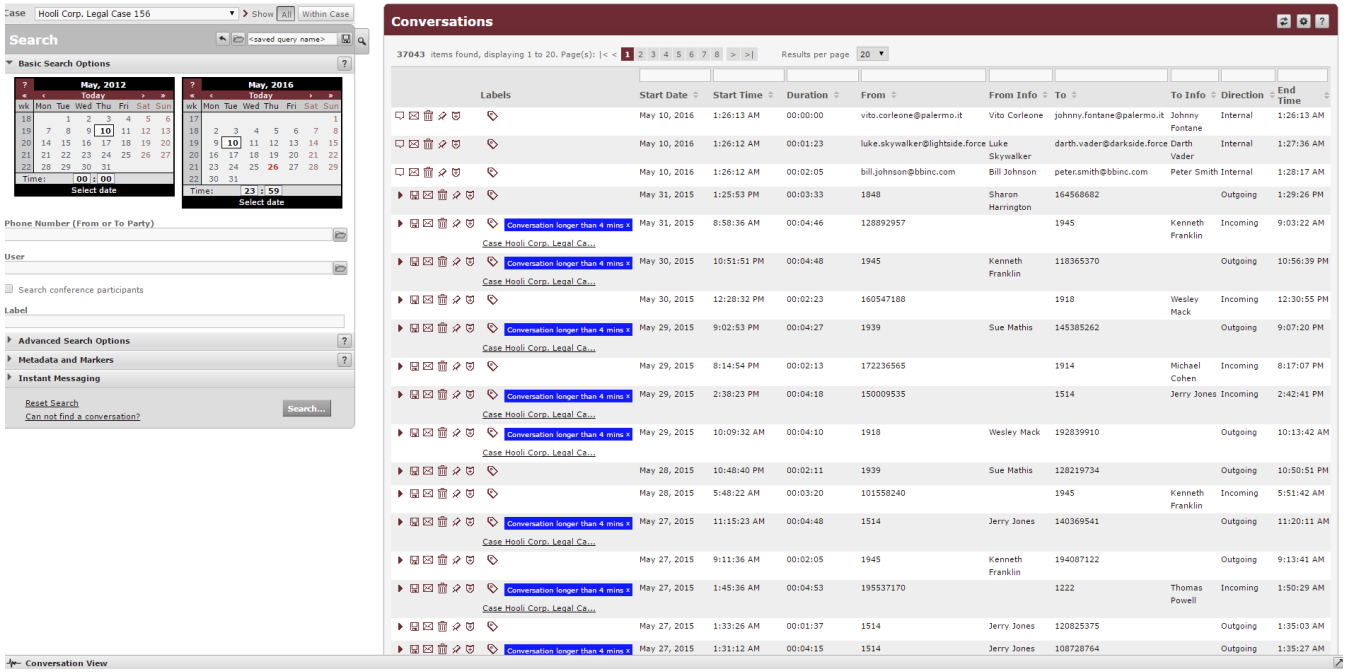
Line Item	Description
ID	The ID of the Case
Title	The name of the Case used to identify it across the web interface.
Description	Optional description of the Case.
Owner	The owner of the case is the user who created it.
Conversations Included	Summary statistics the conversations belonging to this case. The Count, List and Export buttons allow these actions to be carried out on the conversations belonging to the case.
Concern Labels	The list of labels belonging to the case. These labels define which conversations are part of the Case. All conversations tagged with any of the labels in this ist are part of the case. To add a label, type the name of the label in the Add Label field. To remove a label, click the Exclude from Case button next to the label in the list.
View Conversations	View Access to the conversations belonging to the case will be extended to the users or groups specified in this section. • None: Access will not be extended by this case meaning the conversations can only be accessed by users who have been granted access by other means. • Select Users: Extends access to the users or groups specified. • Everyone: Every user in the system will be granted access to the conversations.
Playback Conversations	Play Access to the conversations belonging to the case will be extended to the users or groups specified in this section.
Add / Remove Conversations	Specify which users are able to include / exclude additional conversations in the case by adding / removing labels belonging to the case to / from conversations.
Legal Hold	Enable legal hold for the labels belonging to the case. For more information on Legal Hold, please refer to the corresponding article: Legal Hold.
Authorization Requests	List of conversation access requests for this Case. For more information on authorization requests, please refer to the corresponding article: Authorization Requests.

Case Context

Context Switching is available on the Search page of the Verba Web Interface.

There is a separate context available for every previously created Case. Switching to the context of a Case limits the available labels that can be manually placed on conversations to the labels belonging to the Case.

The screenshot below shows the search interface with a context enabled.



To switch between Case Contexts, use the dropdown in the top left corner of Search page.

To limit the list of displayed and searchable conversations to the ones included in the current Case Context, click the **Within Case** button. To show all conversations, click the **All** button.

Legal Hold

Available in version 8.0 and later

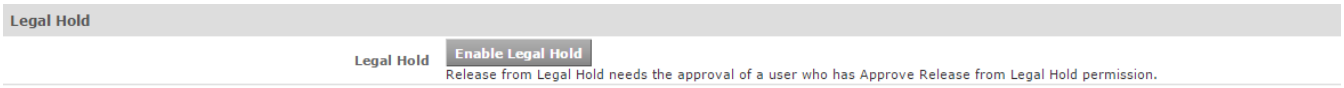
This article provides a guide for using Legal Hold in Verba.

Legal hold is a special property for labels. When Legal hold is enabled for a label, the conversations the label is applied to cannot be deleted by any user (even if they have the Delete conversation right) or automated process (data retention policy).
In addition, labels with legal hold enabled cannot be removed from conversations and cannot be deleted.

If legal hold has been activated for a label, it can only be deactivated (released) by at least two administrators or supervisors with the sufficient rights. One of them has to initiate the release of legal hold and the other has to approve it.

Enabling Legal Hold for labels

To make a label include legal hold, open the Verba web interface and select the Labels > Manage labels menu item, then click on the desired label in the list (or create a new one).

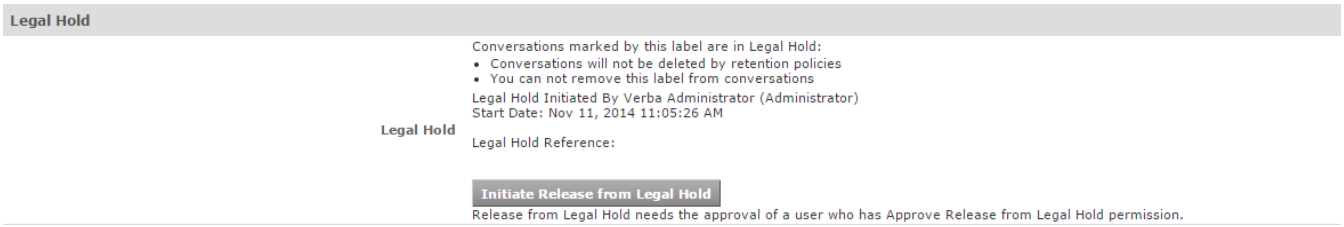


On the label management page, click the 'Enable Legal Hold' button. Optionally add a description to the Legal Hold Reference text field then click Save to confirm.

After saving, the legal hold will be applied to all conversations that are tagged with the associated label.

Releasing Legal Hold

To release legal hold, an administrator or supervisor with the sufficient right has to initiate the release. To do this go to the configuration page of the label by selecting it from the list of labels, the click the 'Initiate Release from Legal Hold' button.



This will place the legal hold in a state waiting for approval of release by another user with sufficient privileges. The other user will have to log into the web interface and go to the label's configuration page, then click the "Release Legal Hold' button.

Click Save to apply the changes. After this point all restrictions provided by Legal Hold will be removed from this label.

Listing legal holds

The Legal Hold menu in the web interface allows you to display lists of labels associated with legal holds.

The List Legal Holds option displays a list of labels that are currently under Legal Hold.

The Waiting for Approval option displays a list of labels where the release of Legal hold was requested and they are awaiting the approval of another user with sufficient rights.

Voice Quality Check

This article contains a description of the Voice Quality Check feature.

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.

Scoring the call

A total score is determined based on the following characteristics/features which may be extended in the future. The score of the call is the total of the feature scores, a feature score might become negative in case of several low scores to effectively reflect errors in the overall score. Scoring is done based on the following features:

Recording statistics

- RTP loss
- SRTP decryption errors
- Decoding errors
- Media mixing errors

Media features

- Volume
- Silence
- Noise
- Beeps and clicks
- Sharp amplitude changes
- Unnatural silence
- Waveform envelope variance

To see how to configure the policy in the system, refer to the Voice Quality Check action article.

Lync Announcement

The Verba Lync Recording Announcement service is able to notify the participants that the call will be recorded. The service can be used for meetings, incoming/outgoing PSTN and federated calls. To configure it you will need a Trusted Application Pool/Server in your Lync topology.

It supports Lync 2010, Lync 2013 and Skype for Business environments. The Verba Lync Recording Announcement service is transparent, which means that the Lync endpoints receiving the call don't see that the call was actually transferred by the announcement service and the transfers are not visible in the Verba Call Records either.

It has five different ways of operating depending on the call scenarios it's used in.

- **Announcement service for Incoming PSTN calls**
  The incoming PSTN calls are forwarded to the Verba announcement service, which notifies the caller that the call will be recorded, then the service transfers the call to the original called party.

- **Announcement service for Outgoing PSTN calls**
  The outgoing PSTN calls are forwarded to the Verba announcement service, which notifies the caller that the call is on hold and the call will be connected. In the meanwhile, the announcement service initiates an outgoing call to the original callee and notifies him/her about the recording and connects the two call legs.

- **Announcement service for Incoming Federated calls**
  The incoming federated calls are forwarded to the Verba announcement service, which notifies the caller that the call will be recorded, then the service transfers the call to the original called party.

- **Announcement service for Outgoing Federated calls**
  The outgoing federated calls are forwarded to the Verba announcement service, which notifies the caller thar the call is on hold and the call will be connected. In the meanwhile, the announcement service initiates an outgoing call to the original callee and notifies him/her about the recording and connects the two call legs.

- **Announcement service for meetings**
  The Announcement service automatically joins the meeting when the recording is started and plays the announcement to the participants as well as sending an IM message to the conversation window. When new participants join the conference, the announcement service notifies them privately, without disturbing the meeting.

By default, the Verba Lync Announcement service uses the same prompt for all Incoming/Outgoing calls and conferences. But it's also possible to configure **prompts on a per user basis**.

For information on how to install and configure this service, refer to the Installing and configuring the Verba SfB - Lync Announcement service article.

Call Blocking on Recording Failure

Call blocking is available on Lync 2010 and 2013 and Skype for Business 2015 platforms.When the Verba recording system is experiencing technical difficulties and is unable to record conversations, it can block all new calls and disconnect ongoing calls if possible for configured recorded users. This feature allows mitigating the risk associated with not recording a certain conversation.

- Both voice and video calls can be blocked, IM conversation blocking is not supported.
- The system blocks all calls for the configured recorded users, so it is most suitable for always-on recording scenarios.
- The components participating in call blocking (Lync Filter plugin, Proxy server) are logging details of each call that has been blocked into an audit log file.
- Ongoing calls can only be blocked when proxy based recording is used, otherwise, only new calls can be blocked.

Call blocking scenarios

The table below summarizes the different failure and call blocking scenarios:

Recording method	Failure scenario	Description
Proxy server based recording	Verba Proxy Server fails	• All ongoing calls will be automatically disconnected on the proxy server that went down, as it will stop relaying RTP streams. • The Verba Lync Filter applications (on the Lync Front End servers) will notice the problem (in 5 seconds). • If none of the proxy servers are available for a Lync Filter, the plugin will send a "SIP ERROR(603)" response to each new SIP INVITE.
Proxy server based recording	Verba Lync Filter fails	• All ongoing calls will stay connected and recorded but SIP BYE messages will not be captured and the system will terminate these calls after the timeout period. • New calls cannot be blocked or recorded, as the Verba Lync Filter is down.
Proxy server based recording	Verba Recording Server fails	• The proxy service notices the problem (in 5 seconds). • If there is at least one recorder available, the proxy service will automatically restart recording on the available recorder. • If there is no available recorder left, the proxy stops relaying RTP streams and calls get disconnected. • If all of the recorders are offline for the proxy, it notifies the Verba Lync Filter (on the Lync Front End server) that all of the recorders are offline for the proxy. • If the associated proxy server for the new call reports that no recorders are available, the Lync Filter plugin will send a "SIP ERROR(603)" response to each new SIP INVITE.
Proxy server based recording	Verba Media Collector fails on Edge	• All ongoing calls will stay connected, but recording will be stopped, and the system will end these calls after timeout. • The Verba Lync Filter applications (on the Lync Front-End servers) will notice the problem (in 5 seconds). • If the Media Collectors is not available which would handle the call then the filter will prevent the call setup
Mediation and/or Edge based recording	Verba Media Collector fails	• All ongoing calls will stay connected, but the recording will stop and the system will terminate these calls after the timeout period. • The Verba Lync Filter applications (on the Lync Front-End servers) will notice the problem (in 5 seconds). • If none of the Media Collectors are available, the Lync Filter plugin will send a "SIP ERROR(603)" response to each new SIP INVITE.
Mediation and/or Edge based recording	Verba Lync Filter fails	• All ongoing calls will stay connected and will be recorded but SIP BYE messages will not be captured and the system will terminate these calls after the timeout period. • New calls cannot be blocked, as the Verba Lync Filter is down.
Mediation and/or Edge based recording	Verba Recording Server fails	• All ongoing calls will stay connected, but the recording will stop and the system will terminate these calls after the timeout period. • The Verba Lync Filter applications (on the Lync Front-End servers) will NOT notice the problem and new calls will not be blocked.

For more information refer to the Configuring Lync call blocking on recording failure article.

A basic call blocking feature is available with the **Truphone** integration. If there are no recorders at the time of call

establishment, the call can be blocked.

Encryption and integrity protection

AVAILABLE IN VERSION 8.6 AND LATER

The Verba system provides a public key cryptography based encryption and digital signing solution to store recordings in a secure and encrypted format, and to protect the integrity of the recordings from tampering. Key features include:

- Windows Certificate Store (WCS) integration for key management
- Industry standard crypto technologies such as RSA, AES, SHA
- Separate certificates for encryption and signing
- Data retention policy based configuration for encryption and/or signing
- Support for defining any number of certificates
- Support for all storage file formats
- Both media and file-based metadata can be encrypted and signed
- Seamless playback option over HTTPS
- Automatic integrity check by validating the signature during playback
- Ability to export recordings in non-encrypted format
- Ability to configure certificates without the private key to disable playback in Verba completely
- OpenSSL scripts available to decrypt and check signatures on recordings outside of the Verba system

The chapters below provide more details on the subject:

> The encryption and digital signing features available prior version 8.6 are not compatible with the new version.

Overview

Encryption

The system allows encrypting recorded media and metadata files. If encryption is configured, the system will encrypt all available files for a recorded conversations:

- Audio file
- Video file
- Screen capture file
- IM transcript file
- Metadata XML file

Encryption can be turned on by configuring a data retention policy:

- Using the Upload and Move policies to encrypt recordings during the execution (before) the upload/move policy
- Using the Encryption and Signing policy

Encryption process

The system encrypts the recorded media and metadata file (option) after the recording process is finished or in a configured time based on the data retention policy configuration. The encryption process consists of the following key steps:

1. The Storage Management Service executes a data retention policy where encryption is configured
2. Based on the configuration, the service retrieves the certificate(s) from the WCS using the configured Windows service user credentials
3. For each to be encrypted file (media and metadata XML), generates a session-key and saves the session-key with RSA encryption (public key) into the crypto information file
4. Encrypts the file stream with AES-256-CTR

Decryption and playback process when private key is available

Encrypted recordings can be played back on the web-based user interface in a seamless way. The decryption process includes the following steps:

1. User initiates playback (HTTPS)
2. The Content Server Service on the Media Repository retrieves the certificate (the one used to encrypt the recording) from the WCS using the configured Windows service user credentials
3. Decrypts the session-key parameters from the crypto information file with the related certificate/private key
4. Decrypts symmetric cipher encrypted media with the session key
5. Transcodes media to MP3 and streams it to the player in the browser over HTTPS (only)

Decryption and playback process when private key is not available

The system allows configuring certificates without private keys to disable decryption/playback in the Verba system. In this case, the Verba system is not able to provide any capability which requires access to the encrypted media files including playback, waveform, transcoding, export to not-encrypted media.

1. User initiates playback (HTTPS)
2. Media Repository returns encrypted media, metadata XML, crypto info files in a single ZIP file
3. User opens the ZIP file in the Verba Offline Player application where the private key is also available
4. The Verba Offline Player application decrypts the session-key parameters from crypto information file with the related certificate/private key
5. Decrypts symmetric cipher encrypted media with the session key
6. Plays media

Integrity Protection / Digital Signing

The system allows signing recorded media and metadata files. If signing is configured, the system will sign all available files for a recorded conversations:

- Audio file
- Video file
- Screen capture file
- IM transcript file
- Metadata XML file

Signing can be turned on by configuring a data retention policy:

- Using the Upload and Move policies to sign recordings during the execution (before) the upload/move policy
- Using the Encryption and Signing policy

Signing process

1. The Storage Management Service executes a data retention policy where signing is configured
2. Based on the configuration, the service retrieves the certificate(s) from the WCS using the configured Windows service user credentials
3. For each to be signed file (media and metadata XML), saves hashing algorithm and certificate into the crypto information file
4. Calculates hash on the content of the file (when encryption is used also, hash calculation is done on the encrypted blocks)
5. Encrypts final hash with the configured certificate (private key) and saves the encrypted hash into the crypto information file

Integrity validation process

The system allows verifying the digital signature through the following process:

1. User initiates check on the user interface
2. The Media Utility Service on the Media Repository retrieves certificate (the one used for signing the recording) from the WCS using the configured Windows service user credentials
3. Calculates hash (when encryption is used also, hash calculation is done on the encrypted blocks)
4. Decrypts signature with the certification public key/cert and matches with the final hash

Key Management / Windows Certificate Store

The system relies on the Windows Certificate Store for storing and managing certificates and keys used for encryption and digital signing. In order to use encryption or signing, the necessary certificates has to be deployed and made accessible on all Verba servers. The system uses the thumbprint of the certificate for identification. The system stores which conversation was encrypted and/or signed by which certificate (thumbprint). Certificate requirements:

- Authorization for Verba service user account
- Availability on all Verba servers
- Certificates must have RSA keys (512, 1025, 2048, 4096)
- Certificates used for encryption and signing must be valid, not expired or revoked
- Certificates for encryption must have a private and a public key (certificates without a private key will also be accepted, but playback will not be available in Verba)
- Strong private key protection must be disabled
- Certificates for digital signing must have a private and a public key
- It is strongly recommended to use different certificates for encryption and signing
- All certificates used at any time (even if expired) must be available to provide decryption and validation for any recording
- Renewing a certificate might generate new keys and thumbprint which need to be configured as a new certificate in Verba

Certificates not satisfying the requirements above will not be used and the system will report an error on an encryption/signing/decryption/validation attempt.

The system uses the Windows service user account for authorization. The following Verba services need access to the certificates:

- Storage Management Service
- Media Streamer and Content Server Service
- Media Utility Service
- Media Transcoder Service

Configuring Certificates

In order to use a certificate in the WCS, the certificate must be registered/configured in the Verba system. For requesting and assigning certificates to the Verba server see: Requesting and assigning certificates

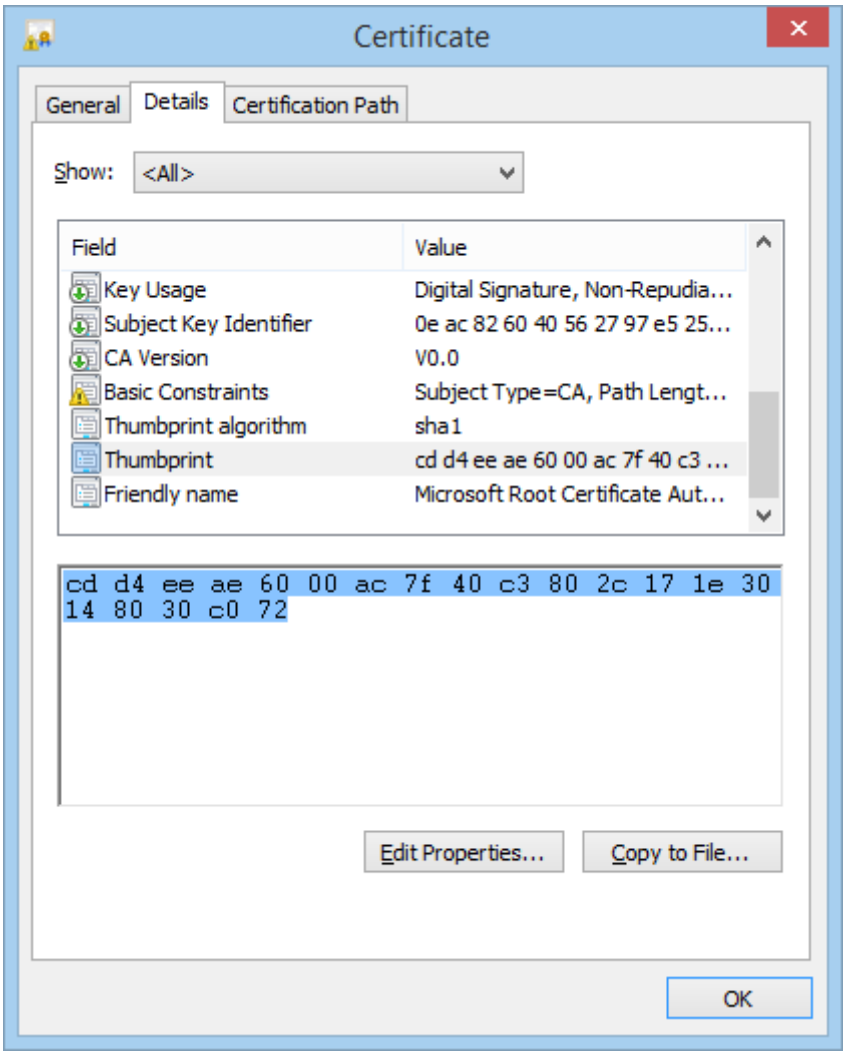
Follow the steps below to configure certificates:

Step 1 - Using the web application, navigate to **System \ Encryption/Signing Certificates**, you must be logged in using an administrative user account with access to certificates

Step 2 - Click on the **Add New Certificate** link.

Step 3 - Enter a name for the certificate.

Step 4 - Enter the thumbprint of the certificate. The thumbprint of a certificate can be obtained by opening the certificate in the **Windows Certificate Manager** on the server/computer where the certificate is available. Double click on the certificate and navigate to the **Details** tab, scroll down to the **Thumbprint** field and copy the hex values.



Step 5 - Configure the certificate, more information on the fields are available below.

Step 6 - Click on the **Save** button.

Field Name	Description	Requirements
Name	The friendly/display name of the certificate used in the Verba system.	Required field Minimum length: 1 Maximum length: 256
Private Key Accessible	Indicates if the private key is available in the certificate or not. When a private key is not available: • the certificate cannot be used for signing • when this certificate is used for encryption, the system will not able to decrypt or play back recordings	-
Compromised	Indicates if the certificate is compromised and can no longer be used. The system does not allow selecting or using certificates marked as compromised.	-
Valid From	Start date of the validation for the certificate. The system does not allow selecting or using expired, not valid certificates.	-
Valid Until	End date of the validation for the certificate. The system does not allow selecting or using expired, not valid certificates.	-

Thumbprint	The unique thumbprint of the certificate in hex values.	Required field

Configuring Encryption

Follow the steps below to configure encryption:

Step 1 - Using the web application, navigate to the **Data \ Data Management Policies** page.

Step 2 - Click on the **Add New Data Management Policy** link.

Step 3 - Set the **Action** to **Upload** when files need to be encrypted before uploading them to the storage location or to **Encrypt and Sign** if the files need to be encrypted in the current storage location.

Step 4 - Select the certificate under the **Encrypt Files with Certificate** option.

Step 5 - Configure the data retention policy based on the requirements. For more information see Data management policies.

Configuring Signing

Follow the steps below to configure signing:

Step 1 - Using the web application, navigate to the **Data \ Data Management Policies** page.

Step 2 - Click on the **Add New Data Management Policy** link.

Step 3 - Set the **Action** to **Upload** when files need to be signed before uploading them to the storage location or to **Encrypt and Sign** if the files need to be signed in the current storage location.

Step 4 - Select the certificate under the **Sign Files with Certificate** option.

Step 5 - Configure the data retention policy based on the requirements. For more information see Data management policies.

Changing the Keys for Already Encrypted or Signed Recordings

In some cases (for instance when a certificate gets compromised and revoked) the certificates used for encryption and signing needs to be replaced with new ones and recordings already encrypted or signed need to be encrypted and signed again with the new certificates. The Enc ryption and Signing data retention policy allows changing the certificates for existing, already encrypted or signed recordings using the following process:

1. Configure an Encryption and Signing policy and filter for one or more specific certificates used (in addition to standard filter options)
2. The Storage Management Service decrypts then encrypts and signs the files using the new certificate(s)

Follow the steps below to change the certificates for already encrypted or signed recordings:

Step 1 - Using the web application, navigate to the **Data \ Data Management Policies** page.

Step 2 - Click on the **Add New Data Management Policy** link.

Step 3 - Set the **Action** to **Encrypt and Sign** to run the policy in the current storage location.

Step 4 - Select the certificate under the **Encrypt Files with Certificate** and the **Sign Files with Certificate** options.

Step 5 - Under the **Data Management Filtering Criteria / Conversation Detail Fields** select the **Encrypted with Certificate** or **Signed with Certificate** options to filter for one or more recordings encrypted and/or signed with the selected certificate(s).

Step 6 - Configure the data retention policy based on the requirements. For more information see Data management policies.

CDR reconciliation

Overview

CDR Reconciliation is a feature in Verba which checks that all recordable conversations have been recorded correctly and warns if conversations have been lost. It works by comparing the original CDRs to the Verba database. The Verba CDR reconciliation offers the following functions:

- Periodically matches the original CDRs with the Verba database records. If a conversation cannot be found in the Verba system, the service creates a database record in Verba and flags it.
- During the process, the service also compares the duration of the conversation to the length of media file, and if the difference is bigger than the configured threshold, flags the record. Other media errors are checked during the recording process by the recording service,
- Conversations which were not completed, such as not answered or busy, are also imported optionally and flagged.
- The service always looks for the CDRs created after the last run of the CDR reconciliation.
- The reconciliation only works for the recorded extensions/addresses/numbers configured in the Verba database. Only extensions, where the recording mode is set to always-on, are used in the process.
- Since recorders might insert the database records later (due to a connection issue with the database), the service periodically rechecks imported records and delete the ones where a matching recorded conversation is found.
- The service can send system alerts if Lost Conversations are identified.
- The standard search interface offers the ability to list conversations which were not recorded (but the reconciliation process inserted them), or conversations where the recorder detected media processing error(s)
- Specific reports are available in the reporting tool for Lost Conversations. The reports can be generated automatically and sent via email.
- The feature is available on Microsoft Lync 2010, 2013, Skype for Business and Cisco (CUCM 8.5 and up) systems.
- The system only processes voice/video conversations.
- This feature increases the load on CDR databases and consequently may have a performance impact. Another side effect is, that users will be able to find Lost Conversations in the Web UI and not answered or established conversations too.

Before turning on this feature, please consult your system administrator to discuss the possible load on your CDR databases. Make sure your users are aware of this feature, and they understand the impact on the system. Once this feature is turned on, users will be able to find not only not recorded conversations, but not answered / not established conversations as well.

If you want to eliminate false alarms or unnecessary imports, consider testing all call scenarios before rolling out the feature.

The configuration for Lync/SfB and Cisco systems is different.

For the SfB CDR configuration, refer to the Configuring Lync - SfB CDR Reconciliation article.

For the Cisco CDR configuration, refer to the Configuring Cisco CDR Reconciliation article.

> The configuration of the CDR Reconciliation was changed in Verba version 9.0. The settings need to be manually moved from the server configuration to the import policy configuration when upgrading systems from earlier releases. Before an upgrade, save your current CDR connection configuration and re-implement it in an Import policy after the upgrade.

Finding not recorded or incorrect conversations

If CDR reconciliation is enabled, the system can identify not recorded conversations or conversations with incorrect media. The system hides these records by default; the web application has to be configured to display not recorded conversations. Please refer to the previous section for more information.

You can use the standard search feature to list these type of conversations. If you navigate to **Search > Advanced Search Options > Recording audit**, you can find the following options:

Type	Description

Recorded conversations	Conversations recorded properly, without any errors.
Recorded conversations with incorrect media	Conversations with media errors. The system can identify the following media errors: • No media • Length mismatch • RTP loss • RTP duplication • SRTP decryption error • Decoding error • Media mixing error You can search for a specific type of error by using the **Conversation detail record fields** option and selecting the **Media Check** field. The system uses thresholds (server level settings) to identify and mark recordings with media errors. If a certain type of error occurs more than the configured threshold, the recorder will automatically mark the recording.
Not recorded conversation due to error	Conversations which were not recorded at all, but the system should have recorded them. These type of conversations also include conversations where the recorder has managed to insert a database record, but it was unable to record the media.
Not answered conversations	The CDR import process can be configured to import CDRs for not answered / established conversations. Refer to the CDR database connection parameters for more information on the configurations. The system can identify the following conversation types: • Cancelled • Busy • Not found • Error You can search for a specific type of code by using the **Conversation detail record fields** option and selecting the **End Cause** field.

Reporting not recorded or incorrect conversations

If you want to create reports periodically and send them in email, you can use the new report templates available for CDR reconciliation:

- Not Recorded and Incorrect Conversation Details
- CDR Reconciliation Summary
- Users CDR Reconciliation Summary

Monitoring the reconciliation process

The CDR Importer service creates a task entry for each periodic run. These tasks can be monitored at **System / Background Task** page.

Configuring Cisco CDR Reconciliation

For an overview of the CDR Reconciliation feature, refer to the CDR reconciliation article.

> The configuration of the CDR Reconciliation was **changed in Verba version 9.0**. The settings need to be manually moved from the server configuration to the import policy configuration when upgrading systems from earlier releases. Before an upgrade, **save your current CDR connection configuration** and reimplement it in an Import policy after the upgrade. This information in earlier versions can be found in the server configuration of the Media Repository server under *CDR and Archived Content Importer*

Cisco-side configuration

The CUCM can be configured in a way to automatically export the contents of the CDR database to a defined SFTP storage. The Verba CDR reconciliation service imports the Cisco CDR data from this SFTP storage and compares the data found there with the data in the Verba database.

For the configuration steps, see: **Configuring Cisco CAR**

Configuration steps

Follow the steps below to configure CDR reconciliation:

Step 1 - Follow the instructions in the **Cisco-side configuration** section down below

Step 2 - Enable the **Verba Import Service** on one of your Verba servers. We recommend running the service on Verba servers with the Media Repository role

Step 3 - In the Verba web interface, navigate to **Data > Import Sources**

Step 4 - Click on the **Add New Import Source** button at the top-right corner of the page

Step 5 - Define the name of the **Import Source**. This name identifies this source in the system

Step 6 - For the type, select **Cisco IPT CDR**

Step 7 - Configure the **Settings section**, based on the information that is shown in the **Import Source Configuration Reference section** down below

Step 8 - Click on the **Save** icon to save your settings

Step 9 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 10 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 11 - For the action, select **Data Import**

Step 12 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 13 - Configure the policy details, based on the information that is shown in the **Data Import Policy Configuration** reference section down below

Step 14 - Set up how frequently the CDR Reconciliation should be run in the **Scheduling** section

Step 15 - Click on **Save**

Import Source Configuration reference

Configuration Parameter Name	Description
CDR Files Folder	Path to where the Cisco CDR files are exported
Store SIP URI When Available	Store SIP URI instead of Number when available

Store Owner ID	Store Owner ID instead of Number/URI when available
Import Not Established Conversations	Imports not established conversations
On Completion	Defines what should happen to the files in the shared folder after Verba imported the CDRs **Delete Files** - The files will be deleted from the drive **Move Files** - The files can be moved to another location if a copy of them should be kept on the network drives
Move To (optional)	Specify where the files should be moved after Verba has processed them. Only available if the **Move Files** option is selected

Data Import Policy Configuration reference

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
Enable CDR Reconciliation	Enables the reconciliation process on the imported CDRs
SIP URI Modification	This setting controls how the system should transform the SIP URI found in the CDRs. It has to be in line with the settings used for the recorder services
Send Alerts for Not Recorded Calls	If enabled, the service will send alerts if it detects not recorded conversations. The system alert message contains a summary of the number of not recorded conversations. It is useful if the administrators want to be notified of these errors. For standard users, you should use the built-in reporting option or the standard search page
Alerts Threshold [sec]	The system will send alerts only at this frequency (max)
Database Connection Retry Period [msec]	Defines the CDR database connections retry period in milliseconds
Media Length Check Threshold [sec]	The service compares the length of the media files to the duration of the conversations (based on the information available in the database) only for conversation where the media is longer than this value in seconds
Media Length Mismatch Threshold [%]	Defines a percentage value used in considering media length mismatch if the length difference is greater than this value. For instance, if the difference is greater than 3%, the system will mark the conversation with media length mismatch error
Ignore Calls Shorter Than [sec]	The service will ignore calls that were shorter than the defined duration
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Service level Configuration reference

Configuration Parameter Name	Description
Cisco CDR Column Filters	Custom filter based on Cisco CDR csv fields. If the defined field matches the specified regex then the record is skipped from processing. The config lines should be in field:regex format. Matching is case insensitive
Cisco External Device/IP Criteria	Reconciliation is done only on behalf of internal Cisco phones' side. By default each party is considered internal. This might lead to false matches (on behalf of remote extension) in case of inter-cluster or specially routed calls. To make sure we check the call only on "internal" extension's behalf, here a list of regexps can be defined which describes trunk, gw names or IPs. Matching is case insensitive

Configuring Cisco CAR

The Cisco CDR Analysis and Reporting (CAR) configuration is required for the Verba Cisco CDR Reconciliation.

For more information see:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_6_1/car/car/caranrpt.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/service/8_5_1/admin/Serviceability/sacdrm.html

Stage 1: Enabling the Cisco CAR Web Service

Step 1 - Open the Cisco UCM web interface and log into the **Cisco Unified Serviceability**.

Step 2 - Go to the **Tools \ Service Activation** menu.

Step 3 - Select the CUCM node, then tick the checkbox at the **Cisco CAR Web Service**.

Step 4 - Click **Save**.

Stage 2: Verify the parameters

Step 1 - Open the Cisco UCM web interface and log into the **Cisco Unified CM Administration**.

Step 2 - Go to the **System \ Enterprise Parameters** menu.

Step 3 - Verify the following settings:

- **Cluster ID: Not empty**
- **CDR File Time Interval: 1**
- **Allowed CDROnDemand get_file Queries Per Minute: 10**
- **Allowed CDROnDemand get_file_list Queries Per Minute: 20**

Step 4 - Go to the **System \ Service Parameters** menu.

Step 5 - Select the CUCM node, then select the **Cisco CallManager** service.

Step 6 - Verify the following settings:

- **CDR Enabled Flag: True**
- **CDR Log Calls with Zero Duration Flag: True**

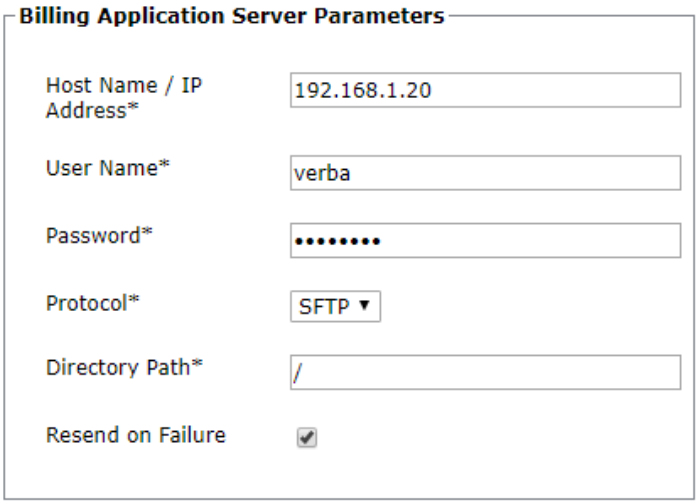
Stage 3: Configure the CDR Management

Step 1 - Open the Cisco UCM web interface and log into the **Cisco Unified Serviceability**.

Step 2 - Go to the **Tools \ CDR Management** menu.

Step 3 - Click **Add new**.

Step 4 - Provide the **address** of the SFTP server, the **User Name**, **Password**, and **Directory Path** settings.



At the Billing Application Server Parameters setting an SFTP/FTP server has to be provided. **This is not the Verba application!**

Step 5 - Click **Add**.

Configuring Lync - SfB CDR Reconciliation

For an overview of the CDR Reconciliation feature, refer to the CDR reconciliation article.

> The configuration of the CDR Reconciliation was **changed in Verba version 9.0**. The settings need to be manually moved from the server configuration to the import policy configuration when upgrading systems from earlier releases. Before an upgrade, **save your current CDR connection configuration** and reimplement it in an Import policy after the upgrade. This information in earlier versions can be found in the server configuration of the Media Repository server under *CDR and Archived Content Importer*

Configuration steps

Follow the steps below to configure CDR reconciliation:

Step 1 - Enable the **Verba Import Service** on one of your Verba servers. We recommend running the service on Verba servers with the Media Repository role

Step 2 - In the Verba web interface, navigate to **Data > Import Sources**

Step 3 - Click on the **Add New Import Source** button at the top-right corner of the page

Step 4 - Define the name of the **Import Source**. This name identifies this source in the system

Step 5 - For the type, select **Lync/SfB CDR**

Step 6 - Configure the **Settings section**, based on the information that is shown in the **Import Source Configuration Reference section** down below

Step 7 - Click on the **Save** icon to save your settings

Step 8 - In the Verba web interface, navigate to **Data > Data Management Policies**

Step 9 - Click on the **Add New Data Management Policy** button at the top-right corner of the page

Step 10 - For the action, select **Data Import**

Step 11 - Under Available Import Sources, **select the Import Source** that you created, then click on the Add button just below the text field

Step 12 - Configure the policy details, based on the information that is shown in the **Data Import Policy Configuration** reference section down below

Step 13 - Set up how frequently the CDR Reconciliation should be run in the **Scheduling** section

Step 14 - Click on **Save**

Import Source Configuration reference

Configuration Parameter Name	Description
Database Hostname	Hostname or IP address of the SfB/Lync SQL Server
Database Name	Name of the CDR database (RTC), e.g. LcsCDR
Database QoE Name	Name of the database that holds the QoE data. Default value is *QoEMetrics*
Database Login	Username for SQL authentication (Read right required only)
Database Password	Password for SQL authentication
Failover Partner	Hostname or IP address of the SQL Server mirroring failover partner

Database Multi-Subnet Failover	Should be enabled if multi-subnet failover is turned on in the database
Windows Authentication	Enables Windows authentication for the SQL Server connection, the system will use the Windows service credentials configured for the Verba CDR and Archived Content Importer Service
SSL Encryption	Enables SSL based SQL Server connections
Import not Established Conversations	Allows importing not established calls such as not answered, busy, etc.
Lync Version	Version of the system, the following values apply: • Lync 2010 • Lync 2013 / Skype for Business
Use QoE Metrics	QoE metrics helps to determine RTP packet utilization and discard calls where no, or just a few RTP packets were sent
Import Conference Participants	Data of conference participants can be collected if the meeting was hosted in the home pool where the CDR info comes from. With this option set to yes, conference participant information will not be imported.

Data Import Policy Configuration reference

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
Enable CDR Reconciliation	Enables the reconciliation process on the imported CDRs
SIP URI Modification	This setting controls how the system should transform the SIP URI found in the CDRs. It has to be in line with the settings used for the recorder services
Send Alerts for Not Recorded Calls	If enabled, the service will send alerts if it detects not recorded conversations. The system alert message contains a summary of the number of not recorded conversations. It is useful if the administrators want to be notified of these errors. For standard users, you should use the built-in reporting option or the standard search page
Alerts Threshold [sec]	The system will send alerts only at this frequency (max)
Database Connection Retry Period [msec]	Defines the CDR database connections retry period in milliseconds
Media Length Check Threshold [sec]	The service compares the length of the media files to the duration of the conversations (based on the information available in the database) only for conversation where the media is longer than this value in seconds
Media Length Mismatch Threshold [%]	Defines a percentage value used in considering media length mismatch if the length difference is greater than this value. For instance, if the difference is greater than 3%, the system will mark the conversation with media length mismatch error
Ignore Calls Shorter Than [sec]	The service will ignore calls that were shorter than the defined duration

Skip Calls without QoE Reports	The service will ignore calls where no QoE reports can be found
Execute Only on Selected Servers	If enabled, a specific server can be chosen that will run this policy

Customed Identification Data Masking

Verba provides the ability to mask CID in the service logs and on the user interface. If CID masking is used, the technical staff can access to the GUI and to the logs without the access to sensitive information. In case of the log masking, it means replacement to a hash, so the corresponding numbers still can be found without revealing the actual numbers.

The CID masking on the GUI applies to the following:

- Everything under the Conversations menu
- Phone service
- Mobile interface

and doesn't apply to the following:

- Quality Management
- Reporting
- System configuration and media files

Configuring CID Masking in the Service Logs

Step 1 - Open the Verba Web Interface and go to the **System \ Servers** menu. Alternatively, it can be configured at the profile level, in the **System \ Configuration Profiles** menu.

Step 2 - Select the server or the configuration profile to configure.

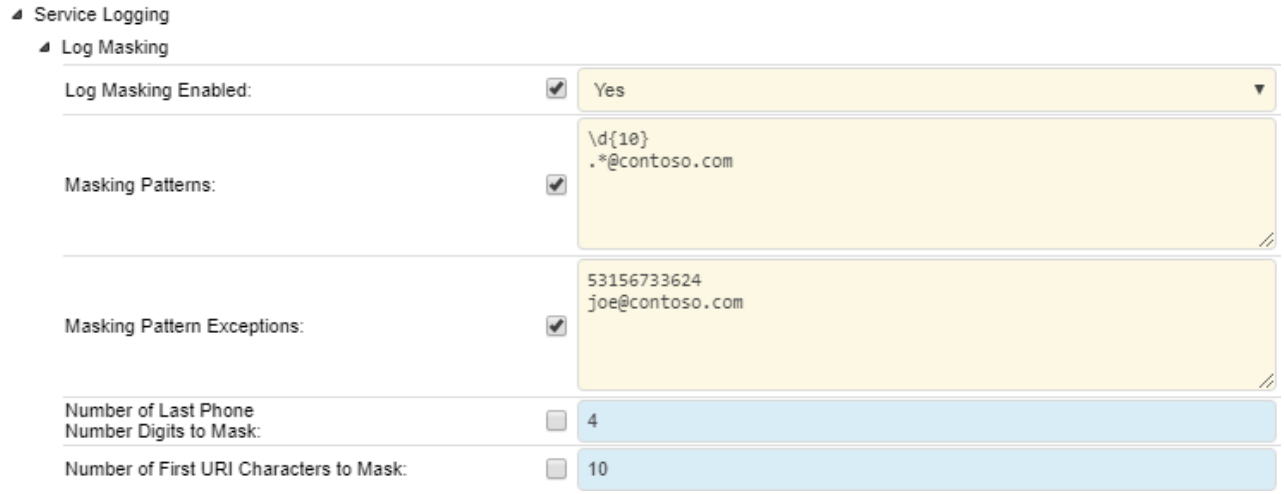
Step 3 - Go to the **Change Configuration Settings** tab.

Step 4 - Expand the **Service Logging \ Log Masking** node.

Step 5 - Set the **Log Masking Enabled** setting to **Yes**.

Step 6 - Provide the regexes at the **Masking Patterns** setting. (one per line)

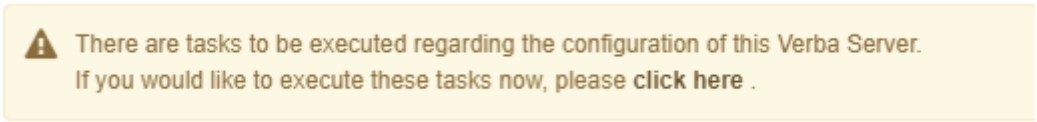
Step 7 - Provide the masking exceptions at the **Masking Pattern Exceptions** setting.



Step 8 - Click on the

icon.

Step 9 - 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.



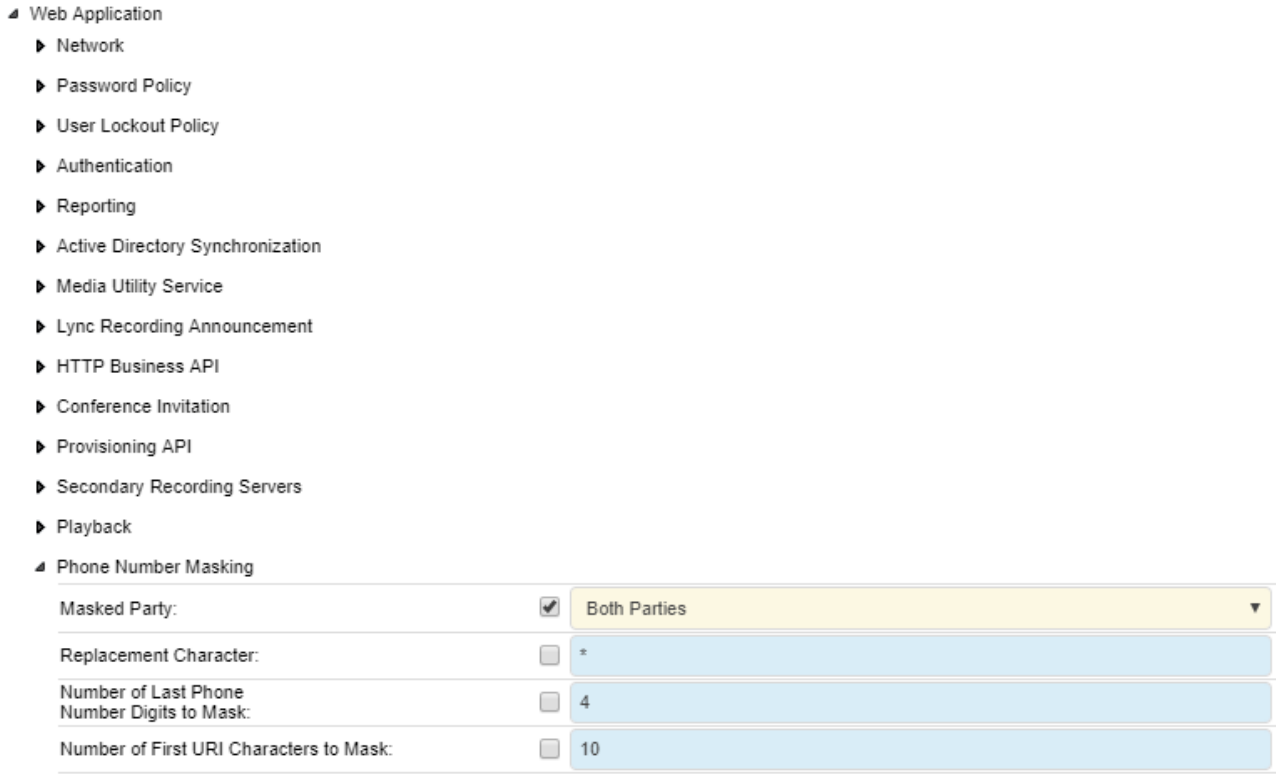
Configuring CID Masking for the GUI

Step 1 - Open the Verba Web Interface and go to the **System \ Servers** menu. Alternatively, it can be configured at the profile level, in the **System \ Configuration Profiles** menu.

Step 2 - Select the Media Repository (or Single) server or the corresponding configuration profile to configure.

Step 3 - Go to the **Change Configuration Settings** tab.

Step 4 - Configure the masking settings under the **Web Application \ Phone Number Masking** node.



Step 5 - Click 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** t ab. Click on the **Execute** button in order to execute the changes.