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.

- Approval Workflows
- Cases
- Legal Hold
- Voice Quality Check
- Announcement
- Call Blocking on Recording Failure
- Encryption and integrity protection
- CDR reconciliation
- Customer Identification Data Masking

ⓘ **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**.

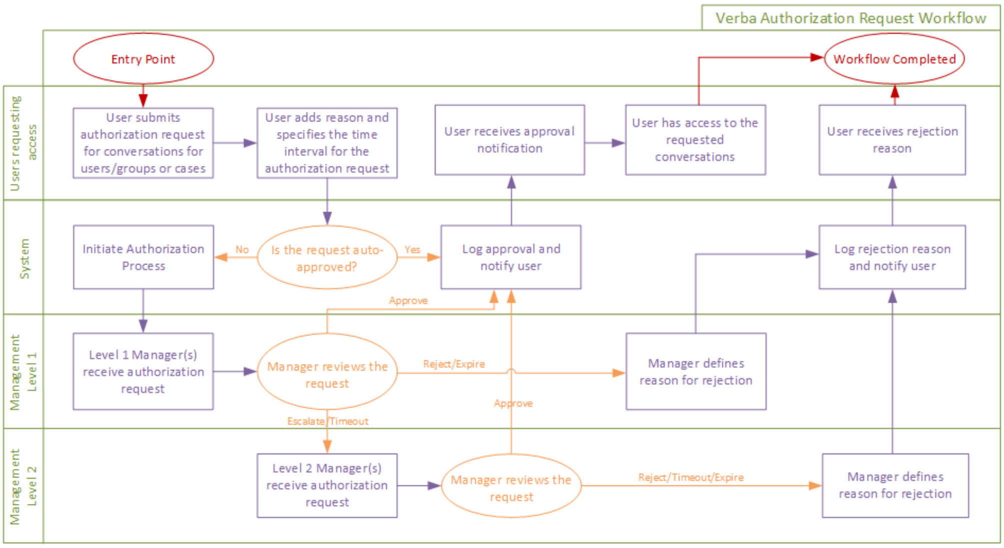
Note! This add-on license is also required for some of the supported external Storage Targets. For details please review the Storage and export targets article.

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.


Verba Authorization Request Workflow
Users requesting access
System
Management Level 1
Management Level 2
Entry Point
Workflow Completed
User submits authorization request for conversations for users/groups or cases
User adds reason and specifies the time interval for the authorization request
User receives approval notification
User has access to the requested conversations
User receives rejection reason
Initiate Authorization Process
No
Is the request auto-approved?
Yes
Log approval and notify user
Log rejection reason and notify user
Approve
Level 1 Manager(s) receive authorization request
Manager reviews the request
Reject/Expire
Manager defines reason for rejection
Approve
Escalate/Timeout
Level 2 Manager(s) receive authorization request
Manager reviews the request
Reject/Timeout/Expire
Manager defines reason for rejection

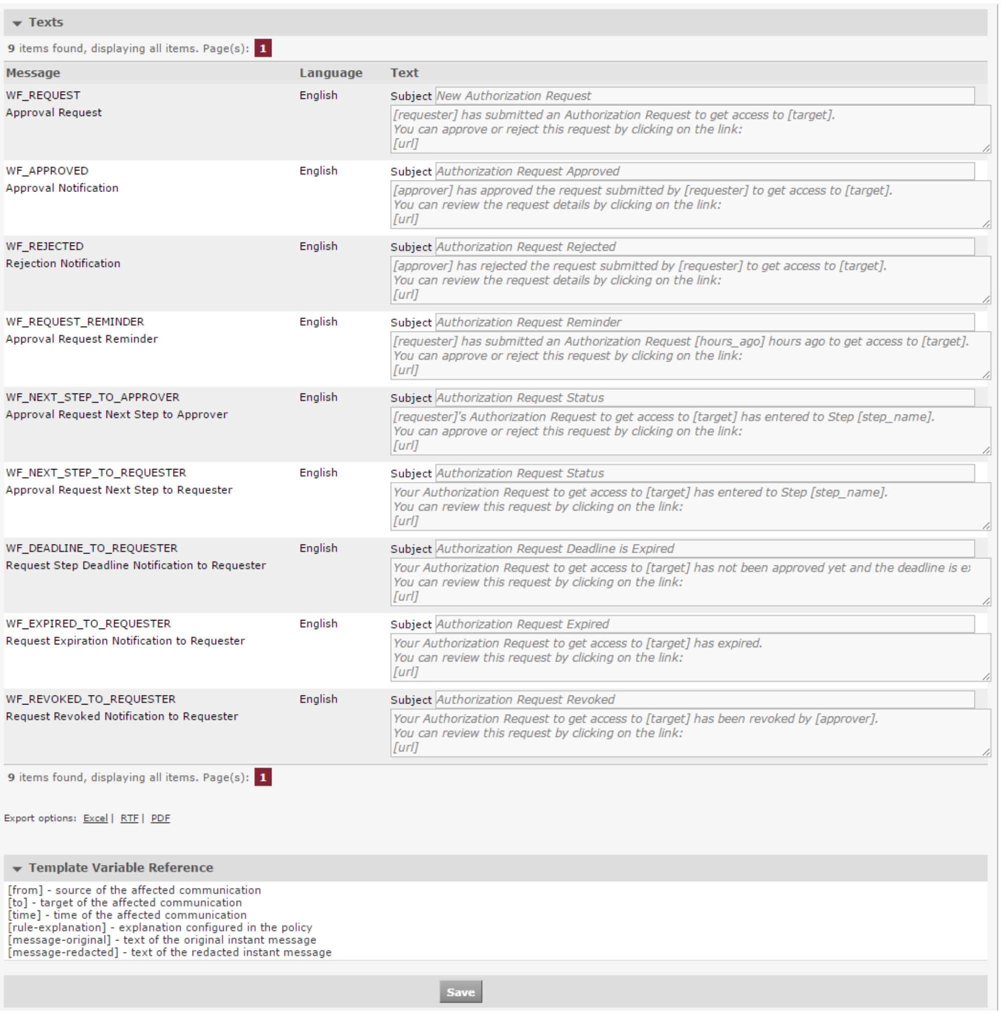
The articles in the Approval Workflows section showcase and describe what Approval Workflows (Compliance Workflows) are, how they can be configured and used throughout the system.

- 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.



▾ Texts

9 items found, displaying all items. Page(s): 1

Message	Language	Text
WF_REQUEST Approval Request	English	Subject *New Authorization Request* *[requester] has submitted an Authorization Request to get access to [target].* *You can approve or reject this request by clicking on the link:* *[url]*
WF_APPROVED Approval Notification	English	Subject *Authorization Request Approved* *[approver] has approved the request submitted by [requester] to get access to [target].* *You can review the request details by clicking on the link:* *[url]*
WF_REJECTED Rejection Notification	English	Subject *Authorization Request Rejected* *[approver] has rejected the request submitted by [requester] to get access to [target].* *You can review the request details by clicking on the link:* *[url]*
WF_REQUEST_REMINDER Approval Request Reminder	English	Subject *Authorization Request Reminder* *[requester] has submitted an Authorization Request [hours_ago] hours ago to get access to [target].* *You can approve or reject this request by clicking on the link:* *[url]*
WF_NEXT_STEP_TO_APPROVER Approval Request Next Step to Approver	English	Subject *Authorization Request Status* *[requester]'s Authorization Request to get access to [target] has entered to Step [step_name].* *You can approve or reject this request by clicking on the link:* *[url]*
WF_NEXT_STEP_TO_REQUESTER Approval Request Next Step to Requester	English	Subject *Authorization Request Status* *Your Authorization Request to get access to [target] has entered to Step [step_name].* *You can review this request by clicking on the link:* *[url]*
WF_DEADLINE_TO_REQUESTER Request Step Deadline Notification to Requester	English	Subject *Authorization Request Deadline is Expired* *Your Authorization Request to get access to [target] has not been approved yet and the deadline is e* *You can review this request by clicking on the link:* *[url]*
WF_EXPIRED_TO_REQUESTER Request Expiration Notification to Requester	English	Subject *Authorization Request Expired* *Your Authorization Request to get access to [target] has expired.* *You can review this request by clicking on the link:* *[url]*
WF_REVOKED_TO_REQUESTER Request Revoked Notification to Requester	English	Subject *Authorization Request Revoked* *Your Authorization Request to get access to [target] has been revoked by [approver].* *You can review this request by clicking on the link:* *[url]*

9 items found, displaying all items. Page(s): 1

Export options: Excel | RTF | PDF

▾ Template Variable Reference

[from] - source of the affected communication
[to] - target of the affected communication
[time] - time of the affected communication
[rule-explanation] - explanation configured in the policy
[message-original] - text of the original instant message
[message-redacted] - text of the redacted instant message

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.

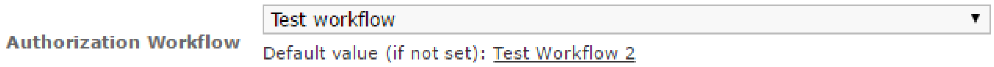
To see how workflows can be created refer to the Creating a Workflow article.

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.

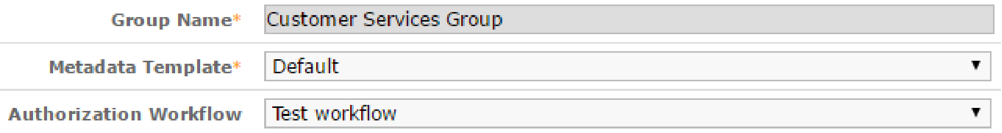
Configuration

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



Authorization Workflow	Test workflow ▼ Default value (if not set): Test Workflow 2

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.



Group Name*	Customer Services Group
Metadata Template*	Default ▼
Authorization Workflow	Test workflow ▼

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

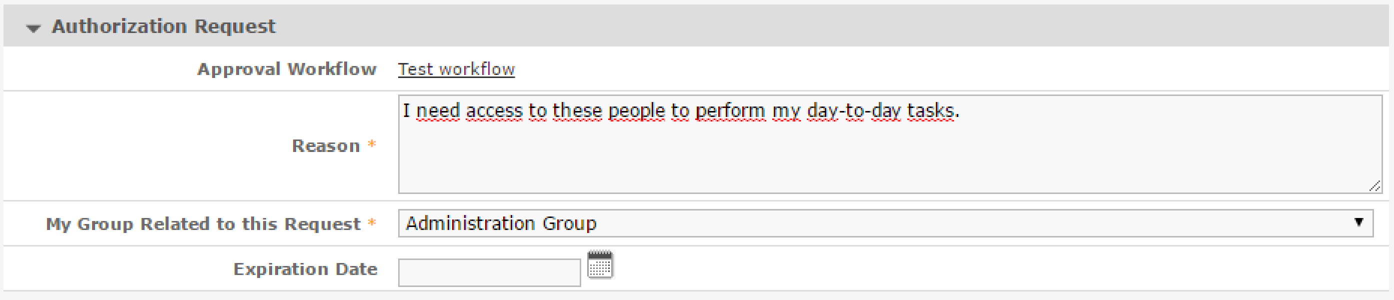
Authorization Requests

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.



Authorization Request

Approval Workflow: Test workflow

Reason *: I need access to these people to perform my day-to-day tasks.

My Group Related to this Request *: Administration Group

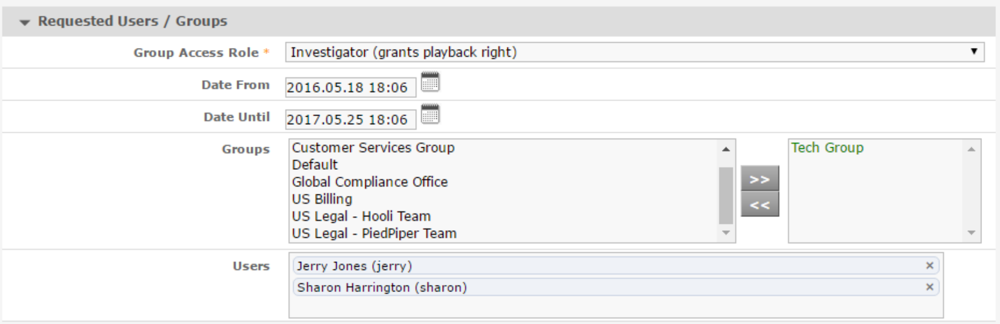
Expiration Date:

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 article
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



Requested Users / Groups

Group Access Role *: Investigator (grants playback right)

Date From: 2016.05.18 18:06

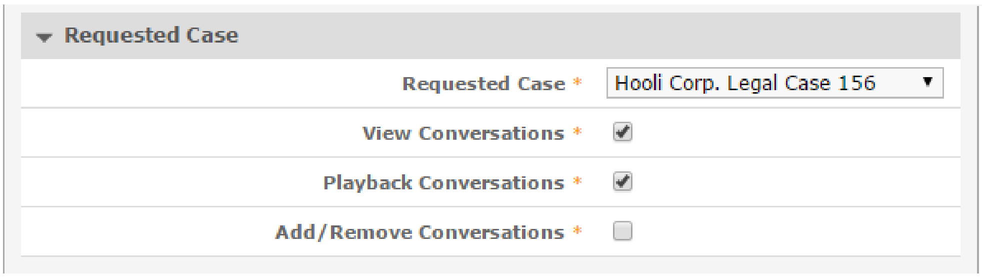
Date Until: 2017.05.25 18:06

Groups: Customer Services Group, Default, Global Compliance Office, US Billing, US Legal - Hooli Team, US Legal - PiedPiper Team → Tech Group

Users: Jerry Jones (jerry), Sharon Harrington (sharon)

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


Requested Case

Requested Case * Hooli Corp. Legal Case 156 ▼

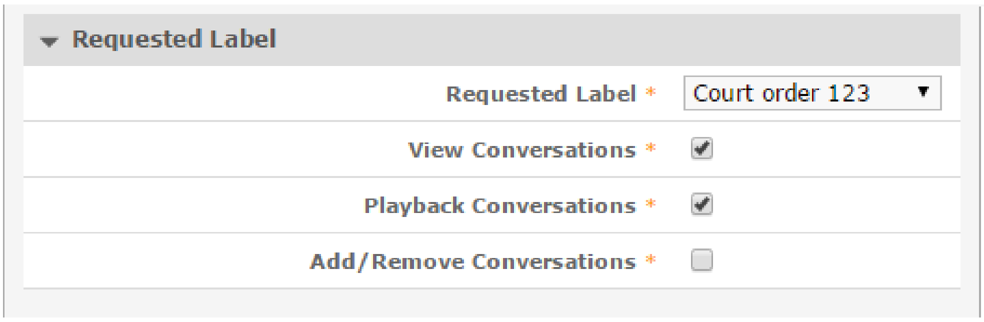
View Conversations * ☑

Playback Conversations * ☑

Add/Remove Conversations * □

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


Requested Label

Requested Label * Court order 123 ▼

View Conversations * ☑

Playback Conversations * ☑

Add/Remove Conversations * □

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.

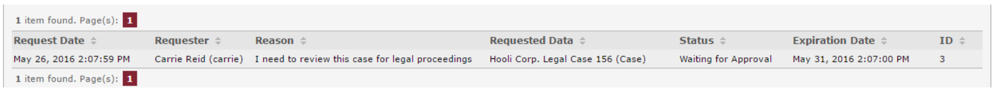
Displaying Submitted Requests

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.



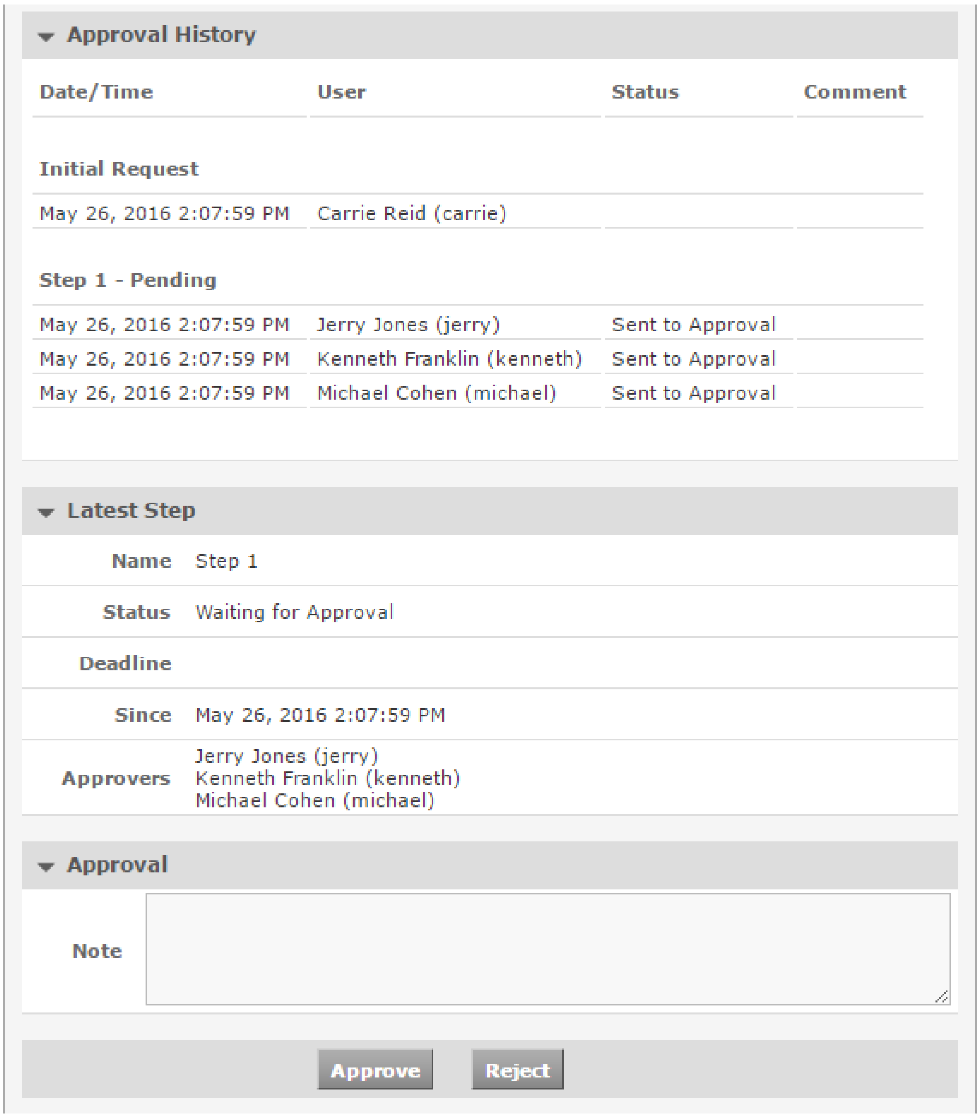
1 item found. Page(s): 1

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.



▾ Approval History

Date/Time	User	Status	Comment
Initial Request			
May 26, 2016 2:07:59 PM	Carrie Reid (carrie)		
Step 1 - Pending			
May 26, 2016 2:07:59 PM	Jerry Jones (jerry)	Sent to Approval	
May 26, 2016 2:07:59 PM	Kenneth Franklin (kenneth)	Sent to Approval	
May 26, 2016 2:07:59 PM	Michael Cohen (michael)	Sent to Approval	

▾ Latest Step

Name	Step 1
Status	Waiting for Approval
Deadline	
Since	May 26, 2016 2:07:59 PM
Approvers	Jerry Jones (jerry) Kenneth Franklin (kenneth) Michael Cohen (michael)

▾ Approval

Note

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

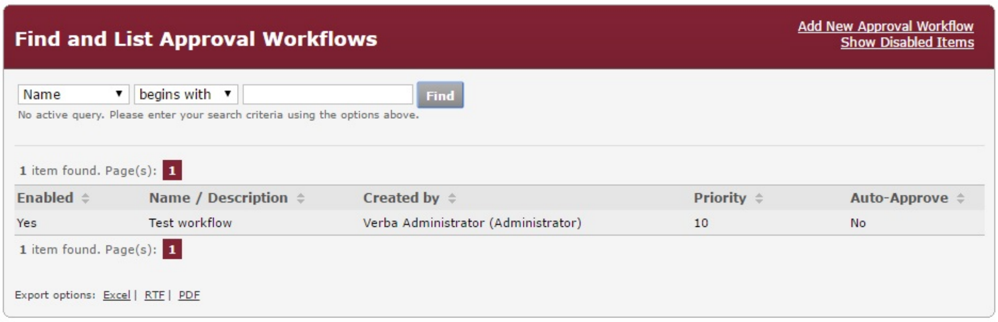
View Authorization Requests - Gives the user the right to see the authorization requests that have been submitted by other people. In most cases this is a right for a system supervisor

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



Find and List Approval Workflows

Add New Approval Workflow
Show Disabled Items

Name ▾ begins with ▾ Find

No active query. Please enter your search criteria using the options above.

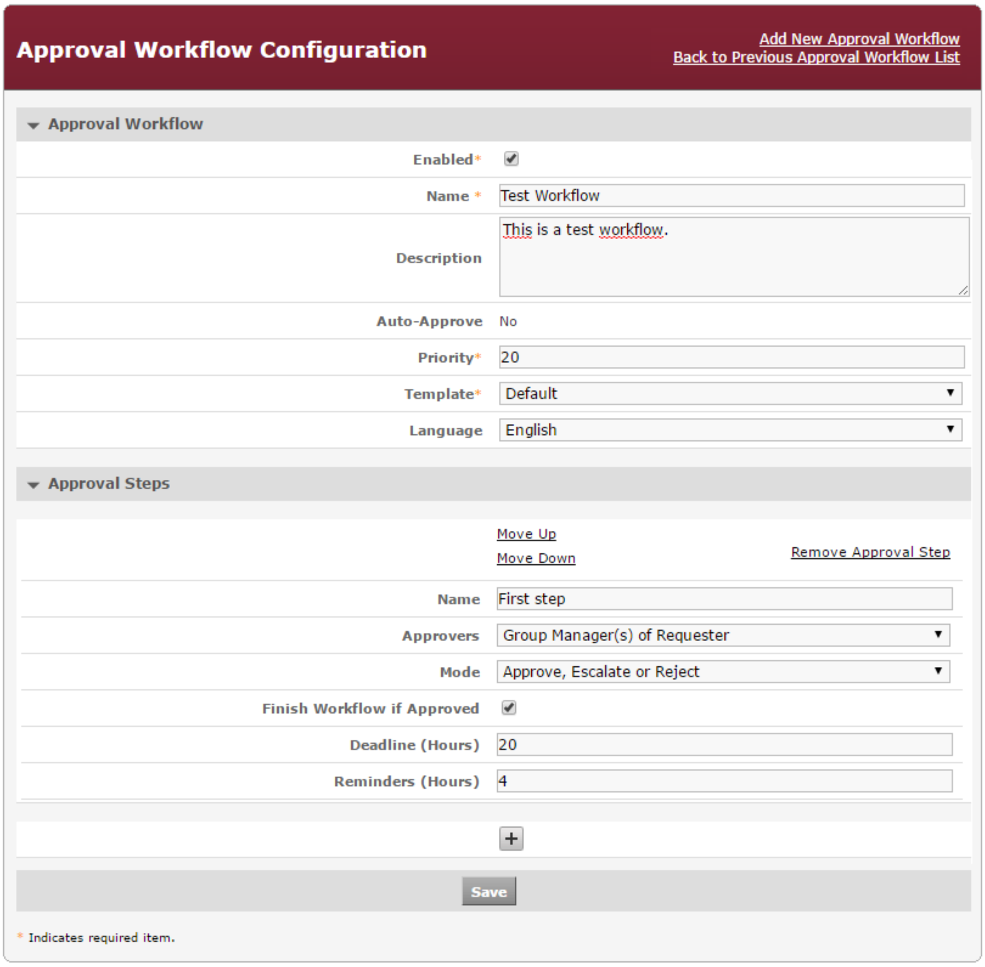
1 item found. Page(s): 1

Enabled	Name / Description	Created by	Priority	Auto-Approve
Yes	Test workflow	Verba Administrator (Administrator)	10	No

1 item found. Page(s): 1

Export options: Excel | RTF | PDF

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



Approval Workflow Configuration

Add New Approval Workflow
Back to Previous Approval Workflow List

Approval Workflow

Enabled*	☑
Name *	Test Workflow
Description	This is a test workflow.
Auto-Approve	No
Priority*	20
Template*	Default
Language	English

Approval Steps

Move Up
Move Down
Remove Approval Step

Name	First step
Approvers	Group Manager(s) of Requester
Mode	Approve, Escalate or Reject
Finish Workflow if Approved	☑
Deadline (Hours)	20
Reminders (Hours)	4

+

Save

* Indicates required item.

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.

- Automation Rules - Cases
- Case Management

Automation Rules - Cases

This article provides a guide to set up and manage the automatic case assignment.
Automatic case assignment allows you to create Automation Rules - Cases that apply and / or remove a configurable set of layers to calls selected by the specified criteria.

Enabling the Automation Rules - Cases

Step 1 - Login to the web interface with System administrator rights.

Step 2 - Navigate to the **System / Servers** menu item and select one of your Verba Media Repository servers.

Step 3 - Click on the **Service Activation** tab.

Step 4 - Activate the **Verba Label Processor Service** using the ⚙ button.

Step 5 - Go to the **Service Control** tab.

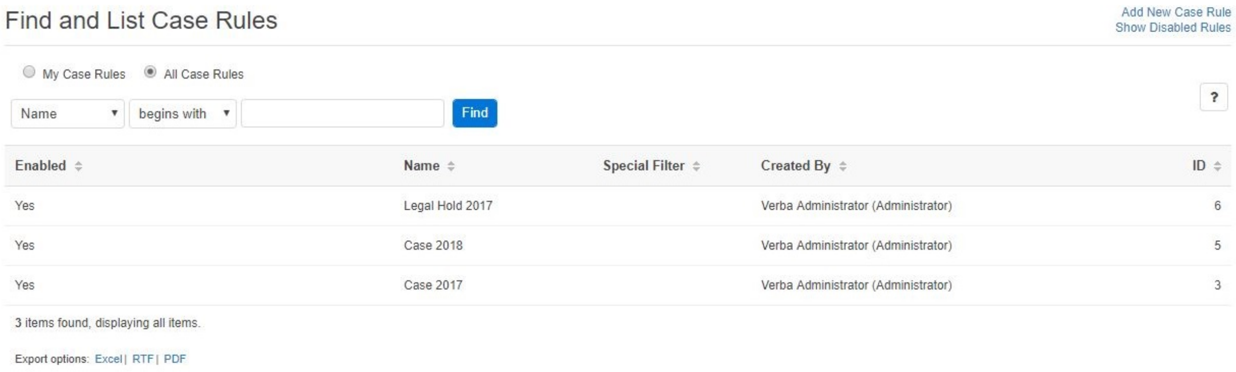
Step 6 - Start the **Verba Label Processor Service** by clicking on the ▶ icon.

Step 7 - After the Verba Label Processor Service was started, the restart of the **Verba Web Application Service** is required.

Creating Automation Rules - Cases

To set up and manage Automation Rules - Cases, open the Verba Web interface and select Data > Automation Rules - Cases.

A list of Automation Rules - Cases is displayed showing the previously created rules.



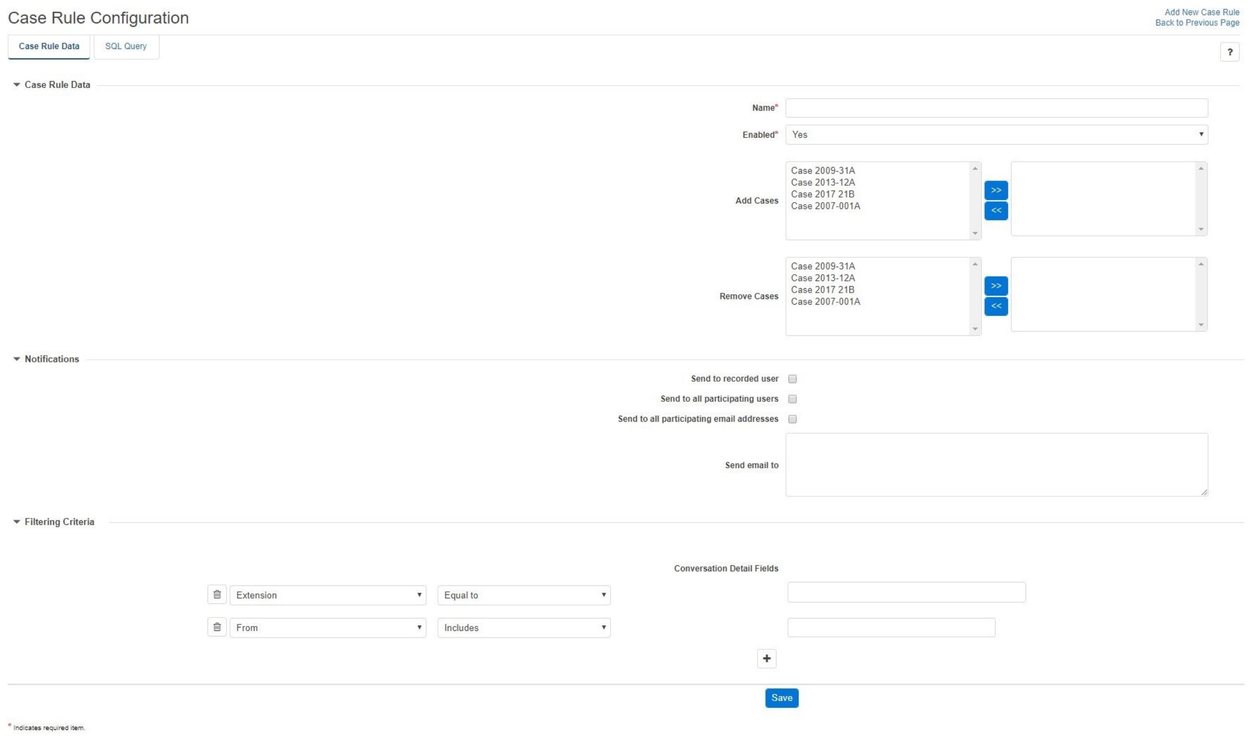
Find and List Case Rules

Enabled	Name	Special Filter	Created By	ID
Yes	Legal Hold 2017		Verba Administrator (Administrator)	6
Yes	Case 2018		Verba Administrator (Administrator)	5
Yes	Case 2017		Verba Administrator (Administrator)	3

3 items found, displaying all items.

Export options: Excel | RTF | PDF

To create a new rule, click the 'Add New Case Rule' button. On the rule configuration page, you have the following options:



Case Rule Configuration

Case Rule Data | SQL Query

Case Rule Data

Name*

Enabled*: Yes

Add Cases: Case 2009-31A, Case 2013-12A, Case 2017 21B, Case 2007-001A

Remove Cases: Case 2009-31A, Case 2013-12A, Case 2017 21B, Case 2007-001A

Notifications

Send to recorded user □

Send to all participating users □

Send to all participating email addresses □

Send email to

Filtering Criteria

Conversation Detail Fields

Extension | Equal to

From | Includes

* 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 Cases	Choose the cases 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 Cases	Choose the cases 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	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. To delete a filter, click the trash icon next to it.

When finished, click Save to save the rule. If the Enabled option was set to 'Yes', the rule is now active.

Filtering Criteria

The table below summarizes the available conversation details fields which can be configured as a filter for the Automatic Case 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	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: • 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	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 Case 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.

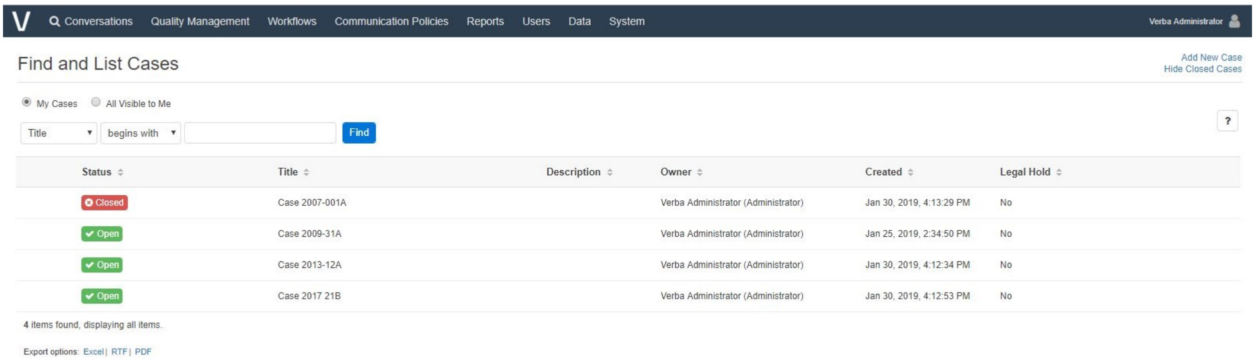
You can use the 'Delete' button to delete the rule.

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.

Case Management

This article provides a guide for managing cases.

To access case management open the Verba Web interface and select **Data > Manage Cases**.



Find and List Cases

● My Cases ○ All Visible to Me

Title ▾ begins with ▾

Status	Title	Description	Owner	Created	Legal Hold
Closed	Case 2007-001A		Verba Administrator (Administrator)	Jan 30, 2019, 4:13:29 PM	No
Open	Case 2009-31A		Verba Administrator (Administrator)	Jan 25, 2019, 2:34:50 PM	No
Open	Case 2013-12A		Verba Administrator (Administrator)	Jan 30, 2019, 4:12:34 PM	No
Open	Case 2017 21B		Verba Administrator (Administrator)	Jan 30, 2019, 4:12:53 PM	No

4 items found, displaying all items.

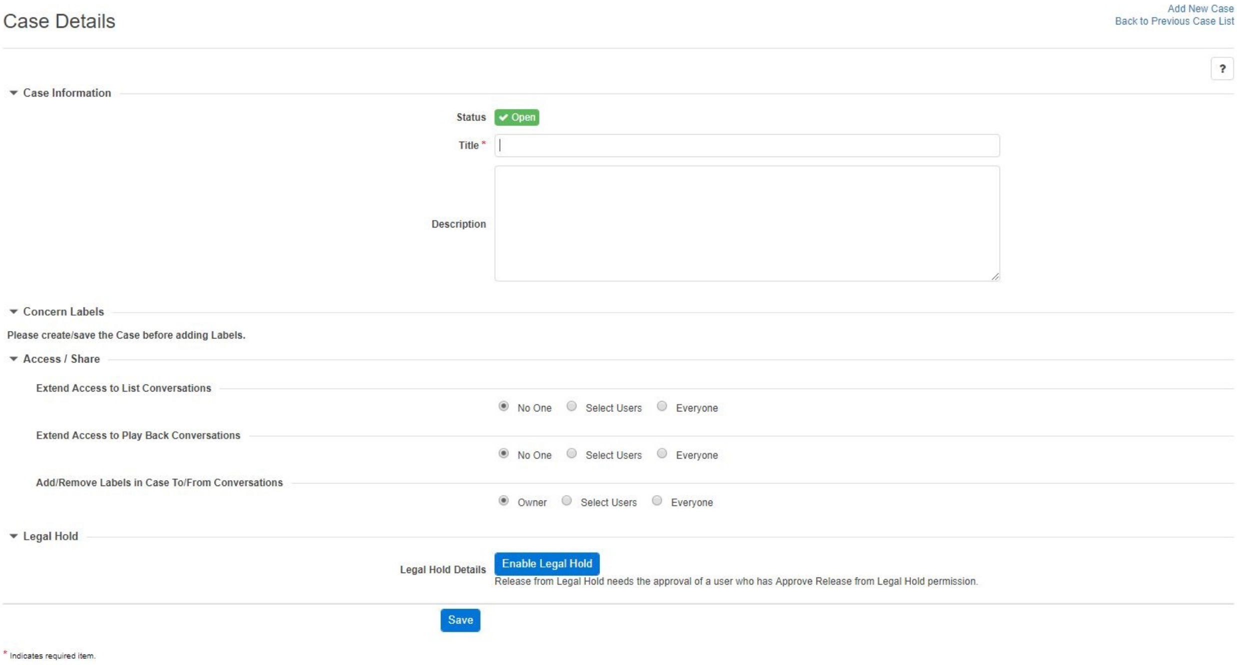
Export options: Excel | RTF | PDF

A list is displayed showing the cases that were previously configured. Clicking on any of the cases you can open it.

On the top of the page, there is an option to display cases created by your user or cases visible to your user. There is also a 'Find' interface to allow you to find the case you would like to manage faster.

Creating new cases

On the Find and List Cases page click the **Add New Case** button. On the Case configuration page, you have the following options.



Case Details

Case Information

Status: Open

Title *

Description

Concern Labels

Please create/save the Case before adding Labels.

Access / Share

Extend Access to List Conversations: ● No One ○ Select Users ○ Everyone

Extend Access to Play Back Conversations: ● No One ○ Select Users ○ Everyone

Add/Remove Labels in Case To/From Conversations: ● Owner ○ Select Users ○ Everyone

Legal Hold

Legal Hold Details: Release from Legal Hold needs the approval of a user who has Approve Release from Legal Hold permission.

* Indicates required item.

Configuration option	Description
Status	The status of the case could be **Open** or **Closed**.

Title	The name of the case. **This will appear on the tag** showing next to each conversation the case is applied to. This is a mandatory field.
Description	Provide an optional description for the case that appears in the case list.
Concern Labels	You can select specific labels which will indicate Case assignment. If one of the specified labels is assigned to a call this case will be assigned too.
Extend Access to List Conversations	This option allows you to **extend access** to list conversations assigned to the case. • **No One**: Access to the conversations assigned to the case 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 assigned to the case to additional users and/or groups. • **Everyone**: selecting this option will grant access to the conversations assigned to the case to every Verba user in the system.
Extend Access to Play Back Conversations	This option allows you to **extend access** to conversations assigned to the case. • **No One**: Access to the conversations assigned to the case 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 assigned to the case to additional users and/or groups. • **Everyone**: selecting this option will grant access to the conversations assigned to the case to every Verba user in the system.
Add/Remove Label to /From Conversations	This option controls which users can **add and remove the case to/from conversations** • **Owner**: only the creator of the case can apply or remove this case to/from conversations • **Select users**: the selected users and the members of the selected groups will be able to apply or remove this case to/from conversations • **Everyone**: every user in the system will be able to apply and remove this case to/from conversations
Legal Hold	This option allows you to **enable Legal Hold** for conversations assigned to the case. For more information on Legal Hold, see the corresponding article.
Save	Click **Save** to save the case.

After the case has been created the users who were granted access to it can apply or remove it to/from conversations they have access to.

Existing Case modification

To edit a case's settings, select it from the Case list. In addition to the adjustable settings covered above, the owner of the Case is displayed, along with a button to query the database for the number of conversations the case is currently applied to ('Count Conversations').

If the case is not marked as Legal Hold, the **Delete** button can be used to delete the case. When a case is deleted, it will be **removed from every conversation**, but the conversations themselves will not be deleted.

You can use the **List Conversations** button to list the conversations which are assigned to this case.

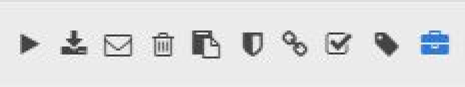
At the bottom of the screen, you can find some additional properties for the case (creation and modification dates) and you can also view a detailed change history by clicking the **View Change History** link.

The **Authorization Requests section** shows all events when access was requested for this specific case.

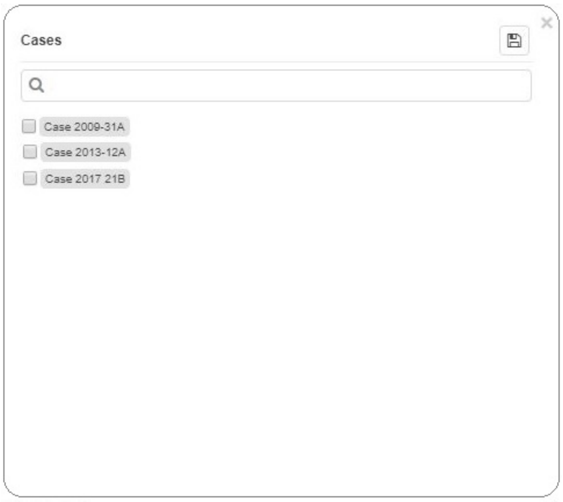
Click the **Save** button to save any changes you made.

Assigning calls to Case(s)

Calls can be assigned to Cases using the suitcase icon next to the calls.



To select the Case that needs to be assigned to the call, click on the suitcase icon. A pop-up window will show up and list the available cases.



□ Case 2009-31A
□ Case 2013-12A
□ Case 2017 21B

Legal Hold

Available in version 8.0 and later

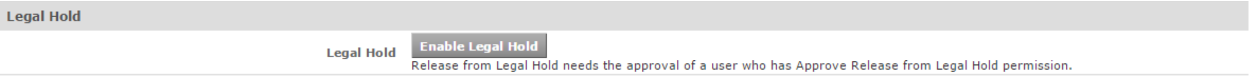
This article provides a guide for using Legal Hold in Verba.

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.

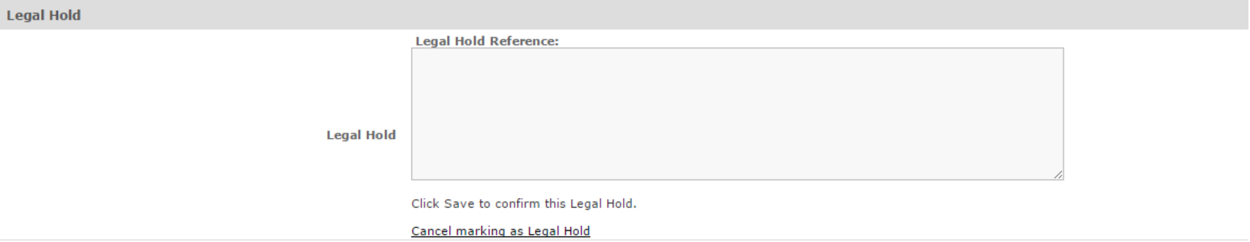
Enabling Legal Hold for labels

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).



Release from Legal Hold needs the approval of a user who has Approve Release from Legal Hold permission.

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.

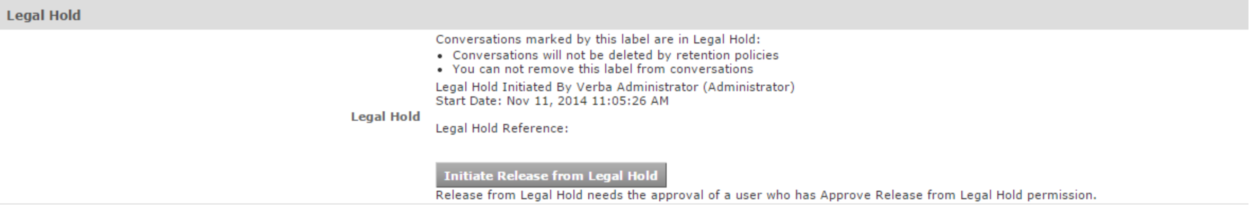


Click Save to confirm this Legal Hold.

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.



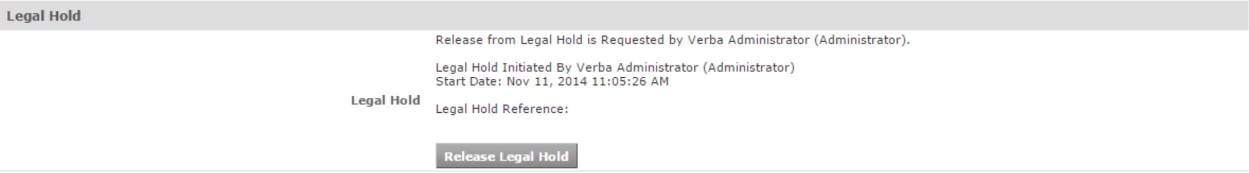
Conversations marked by this label are in Legal Hold:
- Conversations will not be deleted by retention policies
- You can not remove this label from conversations

Legal Hold Initiated By Verba Administrator (Administrator)
Start Date: Nov 11, 2014 11:05:26 AM

Legal Hold Reference:

Release from Legal Hold needs the approval of a user who has Approve Release from Legal Hold permission.

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.



Legal Hold

Legal Hold

Release from Legal Hold is Requested by Verba Administrator (Administrator).

Legal Hold Initiated By Verba Administrator (Administrator)
Start Date: Nov 11, 2014 11:05:26 AM

Legal Hold Reference:

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

The Voice Quality Check storage policy is implemented to check the quality of the voice recordings and detect noise, garbled voice and other problems. The system uses a wide range of checks (acoustic, network, packet and decoding) and proprietary algorithms to derive a Voice Quality Check Score. Because of the varying nature of the recorded environment (recorded user behavior, acoustic environment, and technology), there may be instances where the Quality Check functionality does not identify all calls with issues, or alternatively, it may identify ‘good’ calls as having issues.

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). For more information, see Voice Quality Check policy.

ⓘ Running the quality check puts an extra ~15% CPU load on the recording servers. Check Media Recorder sizing for voice, video, screen - application share recording for more information.

The check only works for calls longer than 15 seconds, shorter calls are automatically skipped.

Scoring

A total score is determined based on multiple 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. The system uses a proprietary algorithm to calculate the individual feature scores and the value of the total score. Scores are normalized to a 0-100 range where 100 is the maximum/best score. We recommend 75 for the overall score threshold. 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

Recording statistics represents exact media capture and processing issues, which can indicate voice quality degradation of the recorded media. The additional media features are used to extend the quality check with additional properties, which can help to detect quality issues in the recordings. Please note, that a poor result of the quality check might not necessarily mean that the recording cannot be played back or it is unintelligible.

Accessing and using the results

- Both the overall score and the individual values of the features are automatically stored as custom metadata and accessible using standard search. In order to display the total score or the individual values of the features, users can configure the search list layout by adding the fields as columns to the search grid. For more information, see Conversation list layout. These metadata fields can be used across the system as filtering options in search, data management policies, export, labeling rules, etc
- An alert is available which is sent by the service checking the quality of the audio. If the service detects that the overall or any of the features scores are below the configured threshold, an alert is sent with call metadata. The configuration is available in the corresponding data management policy. For more information, see Voice Quality Check policy.
- A specific dashboard widget is also available to show the number of calls where the overall voice quality check score is below a configurable threshold. For more information, see Voice Quality Check Trend.
- Reports are available to create print-ready documents for calls where the voice quality is below a configurable threshold. For more information, see Voice Quality Check Details and Voice Quality Check Summary.

Announcement

The system has a built-in feature to play audio notifications for recorded conversations. The announcement capability is currently available for Microsoft Teams, Microsoft Skype of Business and Cisco environments. The announcement is available for certain call scenarios only.

Call Scenario	Microsoft Teams	Microsoft Skype for Business Announcement	Cisco Announcement
Internal call	Yes	No	No
Incoming PSTN call	Yes	Yes	Yes
Outgoing PSTN call	Yes	Yes	Yes
Incoming federated call	Yes	Yes	N/A
Outgoing federated call	Yes	Yes	N/A
Conference call	No	Yes	No

The announcement can be enabled and disabled on a user level where administrators can specify the audio prompt file for each type of cal scenario. Active Directory synchronization allows configuring the announcement parameters through the synchronization profiles without the need to configure users one by one.

The announcement audit log provides a log for tracking and searching announcements played by the system (or not). The system stores the audit log entries in the database and provides search and listing for the records. The audit log is turned off by default. The announcement white list allows excluding phone numbers and SIP URIs from an announcement. If a phone number is added to the whitelist, the system will not play the recording announcement for that number. Multiple whitelists can be added and maintained through the user interface as a global configuration in a Verba instance. For more information, refer to:

- Announcement audit log
- Announcement whitelist

The audit log and whitelist features are not available for all integrations:

Integration	Announcement Audit Log	Announcement Whitelist
Microsoft Teams	Yes	No
Microsoft Skype for Business	Yes	Yes
Cisco	Yes	Yes

Microsoft Teams announcement

AVAILABLE IN VERSION 9.7.7 OR LATER

The Verba Microsoft Teams Bot Service is able to notify the participants that the call will be recorded. The Microsoft Teams Bot Service will use the configuration to determine when and what audio prompt has to be played for the calls to which the bot gets invited.

The recording bot is playing back the announcement at the beginning of the call. As the bot is a standard participant in the call, the audio is simultaneously played with other participants' audio, which can result in cross-talk with the users.

The custom audio announcement is available for the following call scenarios:

- Peer to peer internal calls
- Peer to peer PSTN calls
- Peer to peer federated calls

The custom audio announcement is NOT available for:

- Meetings with internal users (no audio prompt is played)
- Meetings with PSTN participants (the built-in audio notice is played in the Teams user's default language)
- Meetings with federated users (no audio prompt is played)

The notification banner cannot be customized at the moment and it is displayed regardless if custom audio prompts are configured for the following Teams endpoints:

- Desktop/web
- Mobile (iOS/Android)
- Teams phones
- Teams rooms

The bot, depending on the configuration, can play the audio prompt in the following scenarios:

Call Scenario	Operation
Incoming PSTN calls	Once the call has been established with the bot, the bot plays the audio into the call. The audio prompt will be heard by both participants. The audio prompt will not be recorded by the bot, because the bot only records the audio received from the call.
Outgoing PSTN calls	Once the call has been established with the bot, the bot plays the audio into the call. The audio prompt will be heard by both participants. The audio prompt will not be recorded by the bot, because the bot only records the audio received from the call.
Incoming Federated calls	Once the call has been established with the bot, the bot plays the audio into the call. The audio prompt will be heard by both participants. The audio prompt will not be recorded by the bot, because the bot only records the audio received from the call.
Outgoing Federated calls	Once the call has been established with the bot, the bot plays the audio into the call. The audio prompt will be heard by both participants. The audio prompt will not be recorded by the bot, because the bot only records the audio received from the call.
Internal calls	Once the call has been established with the bot, the bot plays the audio into the call. The audio prompt will be heard by both participants. The audio prompt will not be recorded by the bot, because the bot only records the audio received from the call. When two recorded users are calling each other and both users have a custom announcement configured, the bot plays the announcement of the called party only. In this case, the audio prompt will be recorded for the caller party.

For information on how to install and configure custom announcements, refer to the Installing and configuring Microsoft Teams custom announcement article.

Microsoft Skype for Business announcement

The Verba Lync/SfB 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 2015 environments. The Verba Lync/SfB Announcement Service is transparent, which means that the 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 call records either. It has five different ways of operating depending on the call scenarios it's used in:

Call Scenario	Operation
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.

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.
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.
Outgoing Federated calls	The outgoing federated 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.
Meetings / Conference calls	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.

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

Cisco announcement

The Verba Cisco Announcement Service is able to notify the participants that the call will be recorded. The service can be used for incoming /outgoing PSTN calls. The feature relies on the External Call Control (ECC) capability of the Cisco UCM. The solution works with any type of endpoints, it does not require Cisco phones. As long as the call is routed through a CUCM and an ECC profile can be triggered, the announcement can be played. It has 3 different ways of operation depending on the call scenarios it's used in:

Call Scenario	Operation
Incoming PSTN calls	The system supports 2 configurations for inbound announcements: • 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. • The incoming PSTN calls are forwarded to the CUCM, which notifies the caller that the call will be recorded, then the service transfers the call to the original called party.
Outgoing PSTN calls	The outgoing PSTN calls are forwarded to the Verba announcement service, which provides a ringback to the caller. 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.

For information on how to install and configure this service, refer to:

- Configuring Verba Cisco Recording Announcement for Inbound Calls
- Configuring Verba Cisco Recording Announcement for Inbound Calls (CUCM based)
- Configuring Verba Cisco Recording Announcement for Outbound PSTN Calls

Announcement audit log

The announcement audit log provides a log for tracking and searching announcements played by the system (or not). The system stores the audit log entries in the database and provides search and listing for the records. The audit log is turned off by default.

Supported unified communication platforms: Cisco, Microsoft Skype for Business, Microsoft Teams

Supported voice announcements:

- Cisco: Inbound, Outbound (depending on the ECC profile triggers)
- Microsoft Skype for Business: PSTN Inbound, PSTN Outbound, Federated Inbound, Federated Outbound, Conference
- Microsoft Teams: PSTN Inbound, PSTN Outbound, Federated Inbound, Federated Outbound, Internal

The audit log entries are created by the related services:

- Cisco Announcement Service
- Lync/SfB Announcement Service
- Microsoft Teams Bot Service

Limitations:

- There is no direct link between a recorded conversation and an announcement. Users should use time and participant information to identify the corresponding announcement audit log entry.
- Not all types of announcement failures are logged because there could be cases when the related announcement service cannot be reached, etc.

The content of this page:

Configuring audit log for Microsoft Teams announcements

In order to enable the audit log for Microsoft Teams announcements, follow the steps below:

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

Step 2 - Select the server or the configuration profile of the servers where the Microsoft Teams Bot Service is deployed.

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

Step 4 - Expand the **Microsoft Teams Bot / General** node.

Step 5 - Set the **Audit Log for Customisable Announcement** setting to **Yes**.

Step 6 - Click on the 💾 **icon** to save the changes.

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

Configuring audit log for Microsoft Skype for Business announcements

In order to enable the audit log for Microsoft Skype for Business announcements, follow the steps below:

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

Step 2 - Select the server or the configuration profile of the servers where the SfB/Lync Announcement Service is deployed.

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

Step 4 - Expand the **Sfb/Lync Recording Announcement \ General** node.

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

Step 6 - Click on the
💾
icon to save the changes.

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

Configuring audit log for Cisco announcements

In order to enable the audit log for Cisco announcements, follow the steps below:

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

Step 2 - Select the server or the configuration profile of the servers where the Cisco Announcement Service is deployed.

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

Step 4 - Expand the **Cisco Recording Announcement** node.

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

Step 6 - Click on the
💾
icon to save the changes.

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

Granting access to the announcement audit log

The audit log is available to users with a role where the **Announcement Audit Log** permission is enabled. In order to grant this permission to a user, change one or more of the roles:

Step 1 - Open the Web Interface and go to **Users \ Roles**.

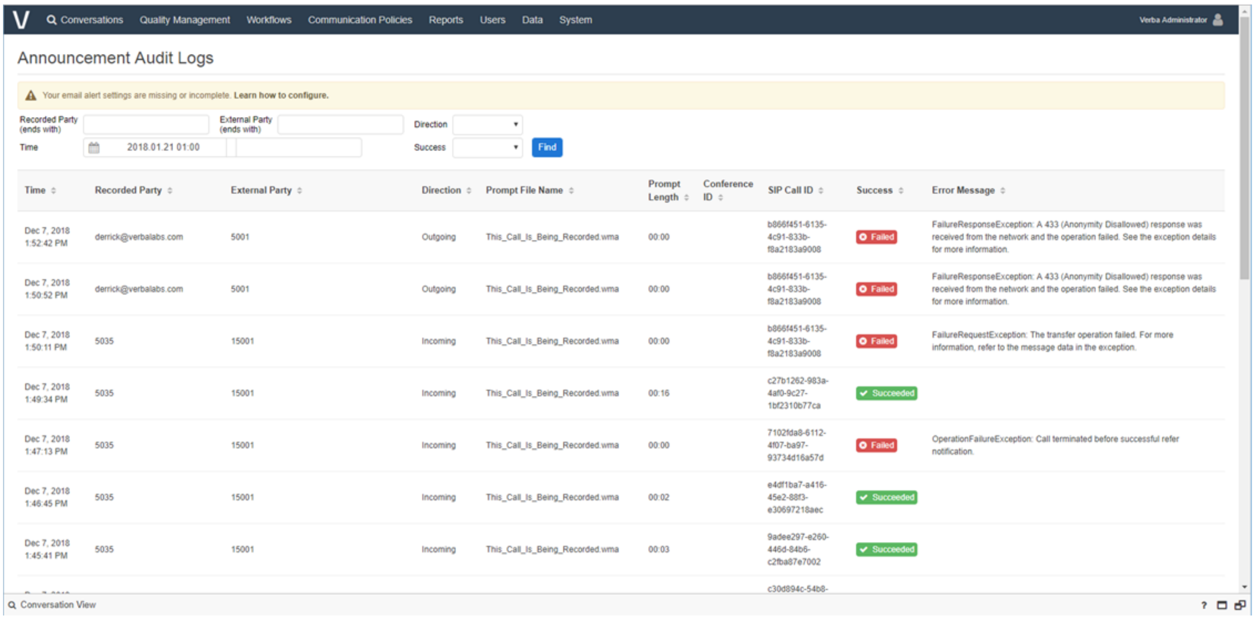
Step 2 - Select the roles you want to change.

Step 3 - Under **Administrative Permissions / Announcement**, check the **Announcement Audit Log** permission.

Step 4 - Click on **Save**. Changes will be in effect after the next login of the user(s).

Searching and viewing the announcement audit log

The announcement audit log is available under **System \ Announcement \ Audit Log**. The page is only available for users with **Announcement Audit Log** permission (see above).



Announcement Audit Logs

Your email alert settings are missing or incomplete. **Learn how to configure.**

Recorded Party (ends with):
External Party (ends with):
Direction:
Time: 2018.01.21 01:00
Success:

Time	Recorded Party	External Party	Direction	Prompt File Name	Prompt Length	Conference ID	SIP Call ID	Success	Error Message
Dec 7, 2018 1:52:42 PM	derrick@verbalabs.com	5001	Outgoing	This_Call_Is_Being_Recorded.wma	00:00		b866f451-6135-4c91-833b-f8a2183a9008	Failed	FailureResponseException: A 433 (Anonymity Disallowed) response was received from the network and the operation failed. See the exception details for more information.
Dec 7, 2018 1:50:52 PM	derrick@verbalabs.com	5001	Outgoing	This_Call_Is_Being_Recorded.wma	00:00		b866f451-6135-4c91-833b-f8a2183a9008	Failed	FailureResponseException: A 433 (Anonymity Disallowed) response was received from the network and the operation failed. See the exception details for more information.
Dec 7, 2018 1:50:11 PM	5035	15001	Incoming	This_Call_Is_Being_Recorded.wma	00:00		b866f451-6135-4c91-833b-f8a2183a9008	Failed	FailureRequestException: The transfer operation failed. For more information, refer to the message data in the exception.
Dec 7, 2018 1:49:34 PM	5035	15001	Incoming	This_Call_Is_Being_Recorded.wma	00:16		c27b1262-983a-4af0-9c27-1bf2310b77ca	Succeeded	
Dec 7, 2018 1:47:13 PM	5035	15001	Incoming	This_Call_Is_Being_Recorded.wma	00:00		7102fda8-6112-4f07-ba97-93734d16a57d	Failed	OperationFailureException: Call terminated before successful refer notification.
Dec 7, 2018 1:46:45 PM	5035	15001	Incoming	This_Call_Is_Being_Recorded.wma	00:02		e4df1ba7-a416-45e2-88f3-e30697218aec	Succeeded	
Dec 7, 2018 1:45:41 PM	5035	15001	Incoming	This_Call_Is_Being_Recorded.wma	00:03		9adee297-e260-446d-84b6-c2fba87e7002	Succeeded	
							c30d894c-54b8-		

The audit log contains the following information:

Field	Description
Time	Date and time of the announcement (start)
Recorded Party	The party which is configured for recording and announcement
External Party	The external party to whom the announcement is played
Direction	The direction of the announcement: • Incoming: the announcement is played for the caller party in an inbound call • Outgoing: the announcement is played for the called party in an outbound call • Conference: the announcement is played for a conference participant
Prompt File Name	The name of the prompt file used for the announcement
Prompt Length	The length of the announcement call leg. It does not necessarily match the length of the prompt file, it could be longer than that. For Microsoft Teams, the length is always 00:00, because the Microsoft SDK cannot provide the information.
Conference ID	The unique identifier of the conference call. Applies to Skype for Business conference announcements only.
SIP Call ID	The unique SIP call ID of the announcement call leg. For Microsoft Teams, this is the Technical Call ID of the recorded call.

Success	Indicates if the announcement was successfully played or not. The system is not able to create an entry for all announcement failers. There could be cases when there is no entry at all.
Error Message	The error message received when the announcement is failed

The audit log page allows searching for audit log entries based on the following criteria:

- Time
- Recorded Party
- External Party
- Direction
- Success

There are multiple ways to find the audit log entries for a specific recorded conversation. The system is

- Users can find the audit log entry using the search screen by entering filters for time and recorder and/or external party.
- On the conversation details screen, there is a link in the top right corner, called **View Announcement Audit Log** link, which redirects the user to the audit log search screen pre-populated with the right search criteria.

Exporting the announcement audit log

The announcement audit log can be exported on the audit log search page which is available under **System \ Announcement \ Audit Log**. The page is only available for users with **Announcement Audit Log** permission (see above). On the page, once the audit log entries are displayed, the log can be exported to XLS or PDF by clicking on the corresponding link at the bottom of the page. The page by default only retrieves up to 1000 records, which can be changed as a system-wide configuration.

Announcement whitelist

The announcement white list allows excluding phone numbers and SIP URIs from an announcement. If a phone number is added to the whitelist, the system will not play the recording announcement for that number.
Multiple whitelists can be added and maintained through the user interface as a global configuration in a Verba instance. Whitelists can contain:

- SIP URI (john.doe@contoso.com)
- Number (+3617005555)
- Number Range (12001-12150)
- Regular Expression (^.*\@contoso\.com)
- DOS Wildcard (*, ?)

Supported for all types of voice recording announcements:

- Cisco: PSTN In, PSTN Out
- Skype for Business: PSTN In, PSTN Out, Conference, Federated In, Federated Out

The whitelist is applied by the corresponding services:

- Verba Cisco Announcement Service
- Verba Lync/SfB Call Filter Service (on the SfB Front-End Servers)

Creating and configuring an announcement whitelist

To add a new whitelist follow the steps below:

Step 1 - Open the Web Interface and go to the **System \ Announcement \ Whitelist**.

Step 2 - Click on the **Add New Announcement Whitelist** link on the top right corner.

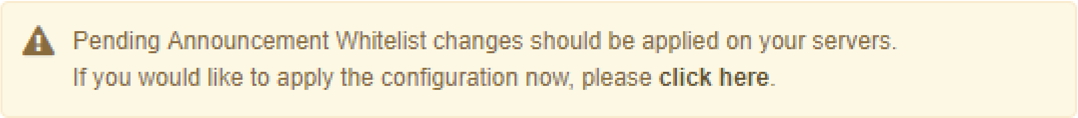
Step 3 - On the new page, define the **Name** of the whitelist.

Step 4 - Add entries to the list manually by clicking on the ✚ icon then select the type of entry and finally add the entry using the input box. You can use the 🗑 icon to remove an entry from the list

Step 5 - Alternatively, you can bulk upload a list by copying and pasting the entire list into the text area under **Bulk Upload**. Press the **Upload** button to import the list. The system will try to automatically recognize the type of entries.

Step 6 - If you are finished with adding entries to the list, press the **Save** button.

Step 7 - A notification banner will appear on the top. Click on the **click here** link, and you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the update on all servers which can run the announcement services. Changes to any whitelist will trigger the configuration update on all related servers. The system applies the whitelist configuration as one combined /merged configuration.



⚠ Pending Announcement Whitelist changes should be applied on your servers.
If you would like to apply the configuration now, please **click here**.

The table below shows the available entry types in the whitelists:

Type	Description	Example
SIP URI	A SIP URI in the format of john.doe@contoso.com	john.doe@contoso.com
Number	A phone number	+3617005555 3617005555 The numbers cannot contain spaces or '-' (dash) characters and can include a single '+' (plus) character in the beginning.
Number Range	A number range separated by the '-' (dash) character	12001-12150 Any number between 12001 and 12150 (inclusive).
Regular Expression	A regular expression	^.*\@contoso\.com Any SIP URI from the @contoso.com domain.
DOS Wildcard	A DOS wildcard such as '*' (asterisk) representing any number of characters and '?' (question mark) representing a single character	
Contains String	A string of characters to match any substring	@contoso.com Any SIP URI containing the '@contoso.com' string.

Call Blocking on Recording Failure

Call blocking is available on Lync 2010 and 2013 and Skype for Business 2015 and 2019 platforms. When the 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.

- Voice, video, screen and application share calls, instant messages, and P2P file transfers can be blocked.
- 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 (SfB/Lync Call and IM Filter Service, Proxy Service) are logging details of each call that has been blocked into an audit log file (lync_im_filter_auditlog.csv, lync_call_filter_auditlog.csv).
- 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

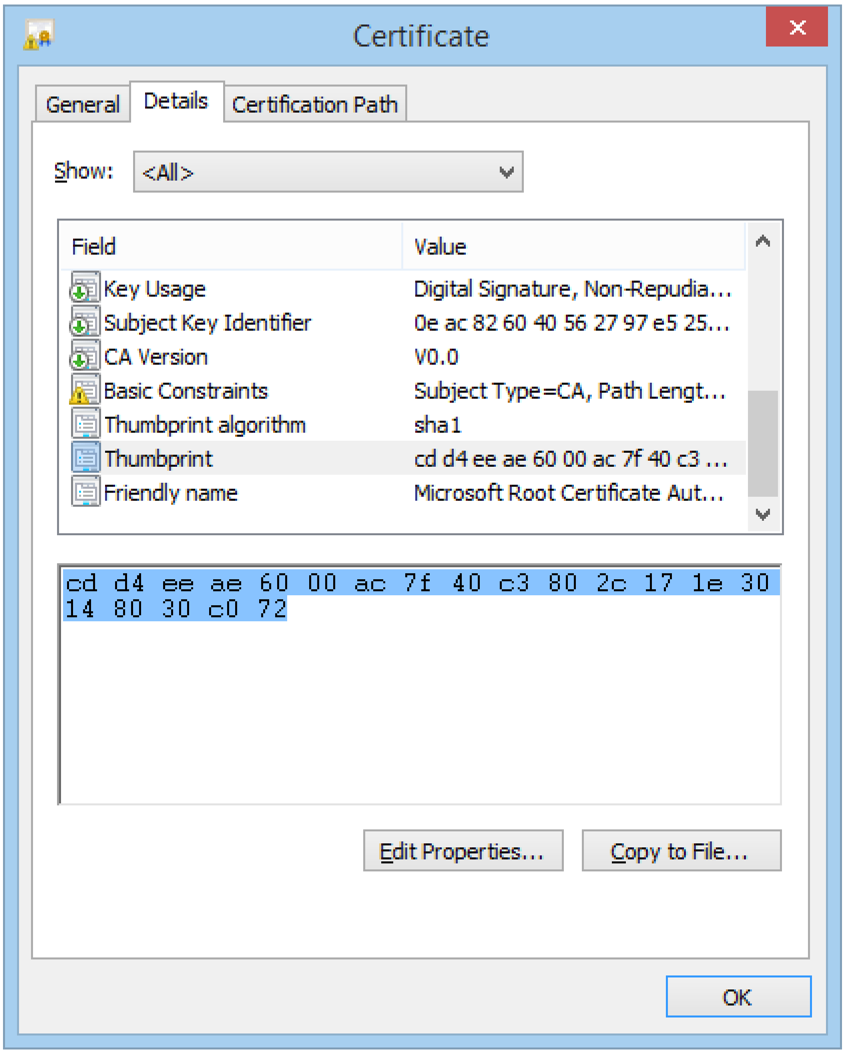
Follow the steps below to configure certificates:

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.



Field	Value
Key Usage	Digital Signature, Non-Repudia...
Subject Key Identifier	0e ac 82 60 40 56 27 97 e5 25...
CA Version	V0.0
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1
Thumbprint	cd d4 ee ae 60 00 ac 7f 40 c3 ...
Friendly name	Microsoft Root Certificate Aut...

```
cd d4 ee ae 60 00 ac 7f 40 c3 80 2c 17 1e 30
14 80 30 c0 72
```

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.

Please note that encryption policies will skip recordings which are under Retention Period.

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.

Please note that signing policies will skip recordings which are under Retention Period.

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 Encryption 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 the system 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 system database. The CDR reconciliation offers the following functions:

- Periodically matches the original CDRs with the database records. If a conversation cannot be found in the Verba system, the service creates a database record in the system and flags it.
- During the process, the service also compares the duration of the conversation to the length of the 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 that were not completed, such as not answered or busy, are also imported optionally and flagged (for Skype for Business and Cisco only).
- 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 that 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
  - Microsoft Skype for Business 2015, 2019
  - Cisco Unified Communications Manager 8.5 and later
  - Symphony XML
  - Zoom Meeting
  - Zoom Phone
- 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 that 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.

Configuring CDR reconcilaition

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.
- For Symphony CDR reconciliation, refer to Symphony Instant Messages - Files - CDRs.
- For Zoom Meeting and Zoom Phone CDR reconciliation, refer to Zoom Meeting and Phone.

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: • Canceled • 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.

Alerting on not recorded or incorrect conversations

When the system is running the reconciliation policy and it finds out that certain calls were not recorded (missing from the Verba database), an alert is raised showing the missing recordings. For more information on the alert, see CDR Importer Service: RecordFailure Alert.

Reporting not recorded or incorrect conversations

If you want to create reports periodically and send them in an 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
- CDR Reconciliation for Skype for Business Summary

Understanding why recording failed

There can be various reasons why a conversation was not recorded or imported. It is recommended to establish a process to investigate the issues after recognizing missing recordings (e.g. receiving the alerts). Refer to Troubleshooting voice recording or import failures for more information.

AVAILABLE IN 9.7.5 AND ABOVE

In order to help the investigation process for Skype for Business integrations, the CDR reconciliation process automatically retrieves Skype for Business diagnostics data from the Skype for Business CDR tables and stores the information in the Skype for Business CDR metadata template fields for missing calls and for calls which were not recorded properly (there were recording errors during the recording process). You can find more information about the Skype for Business CDR table fields at https://docs.microsoft.com/en-us/skypeforbusiness/schema-reference/call-detail-recording-cdr-database-schema/call-detail-recording-cdr-database-schema.

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**

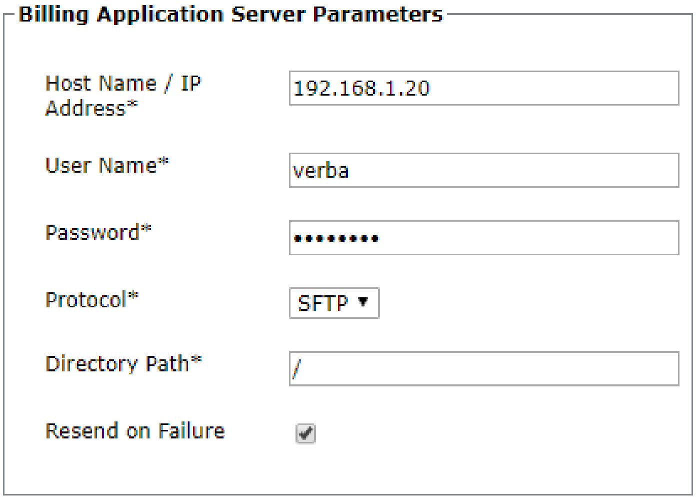
Stage 3: Configure the CDR Management

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.



Billing Application Server Parameters

Host Name / IP Address*	192.168.1.20
User Name*	verba
Password*	••••••••
Protocol*	SFTP ▼
Directory Path*	/
Resend on Failure	☑

ⓘ 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

Customer Identification Data Masking

Verba provides the ability to mask customer identification data (CID) in the service logs and on the user interface. If CID masking is used, the technical staff can access the GUI and the logs without accessing sensitive information. In the case of the service log masking, it means a 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

⚠ Service log masking can increase the CPU load on the servers due to the pattern matching algorithms used by the regular expressions. In the case of complex expressions, it is recommended to test the effect on the CPU load before rolling out the setting to production systems.

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.

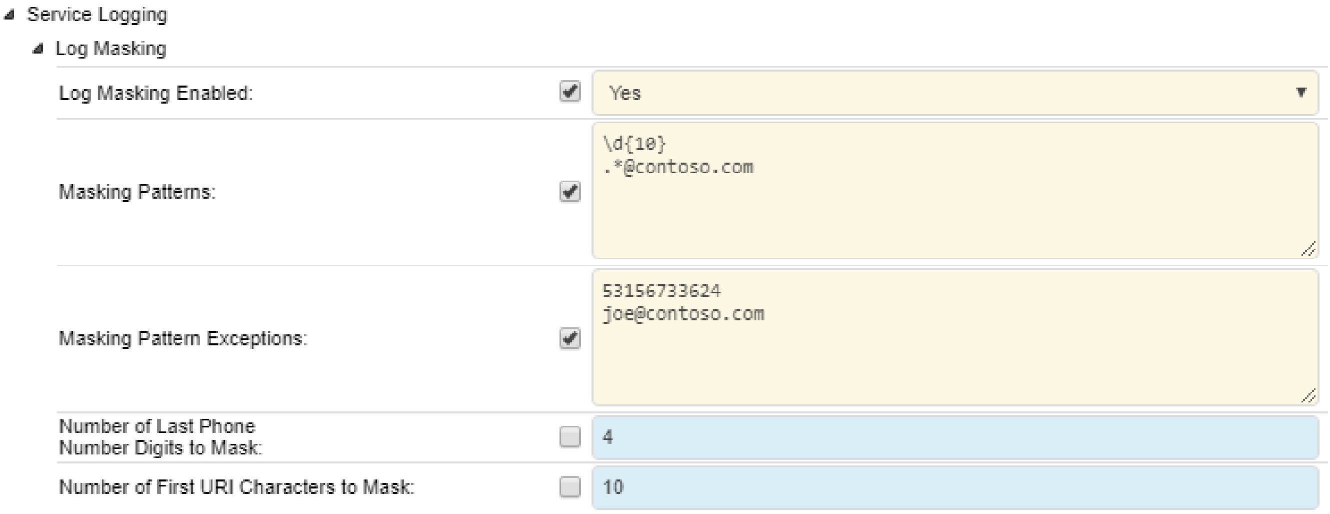
Step 3 - Go to the **Change Configuration Settings** tab.

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.



◢ Service Logging

◢ Log Masking

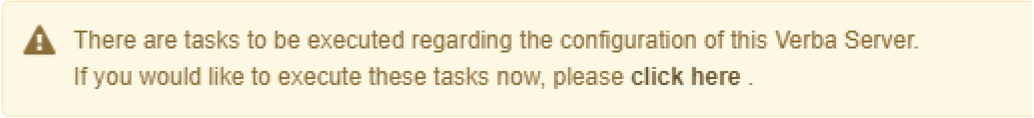
Log Masking Enabled:	☑	Yes ▾
Masking Patterns:	☑	\d{10} .*@contoso.com
Masking Pattern Exceptions:	☑	53156733624 joe@contoso.com
Number of Last Phone Number Digits to Mask:	□	4
Number of First URI Characters to Mask:	□	10

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.



⚠ 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** .

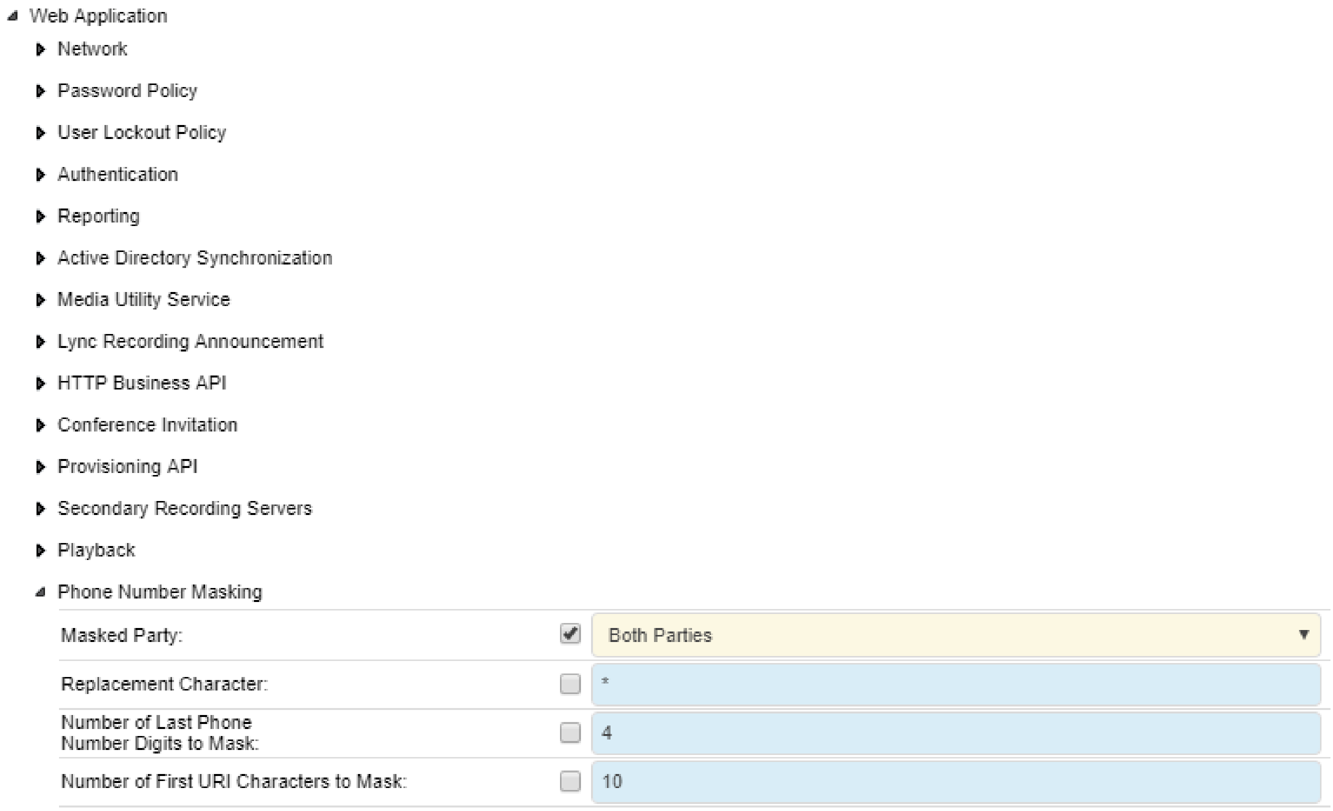
Configuring CID Masking for the GUI

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.



- Web Application
  - Network
  - Password Policy
  - User Lockout Policy
  - Authentication
  - Reporting
  - Active Directory Synchronization
  - Media Utility Service
  - Lync Recording Announcement
  - HTTP Business API
  - Conference Invitation
  - Provisioning API
  - Secondary Recording Servers
  - Playback
  - Phone Number Masking

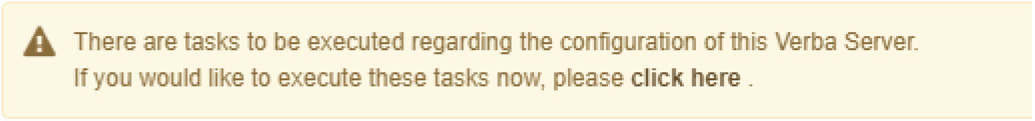
Masked Party:	☑	Both Parties ▼
Replacement Character:	□	*
Number of Last Phone Number Digits to Mask:	□	4
Number of First URI Characters to Mask:	□	10

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** 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 - Configure Phone Number Masking for the users under role configuration, enable **Phone Number Masking in Search** permission. The new permission setting will take effect after the next login of the user.