Data management policies

Overview

Data management policies are very powerful tools for automated data management. Administrators can define rules that execute various actions based on customizable filtering criteria. The policies are executed by the Verba Storage Management Service and/or the Verba Import Service on either Verba Recording servers or Media Repositories.

Policy execution is turned off by default, it has to be enabled in the server configuration.

The system supports the following data management policy types:

Type	Policies	Description	Executed On	Executed By
Data Retention	Upload	Moves conversation related files (media, metadata file, etc.) from the Recording Servers to the configured storage target.	Recording Server or Media Repository / Application Server	Storage Management Service
	Archive in DB and Move Media	Moves database records to the archive table to reduce database load and moves conversation related files to the configured storage target.	Media Repository / Application Server	Storage Management Service
	Archive in DB	Moves database records to the archive table to reduce database load.	Media Repository / Application Server	Storage Management Service
	Move Media	Moves conversation related files to the configured storage target.	Media Repository / Application Server	Storage Management Service
	Copy Media	Copies conversation related files to the configured storage target and keeps the original copies. Recommended for moving data from a WORM storage target where records are still under retention and cannot be deleted (or moved) to another storage target. It can also be used to dual archive recordings.	Media Repository / Application Server	Storage Management Service
	Delete	Deletes all conversation data including database records and related files on the storage target. Generally, it is not recommended to use the delete policy for data retention, instead, the Data retention configuration should be used.	Media Repository / Application Server	Storage Management Service

	File Verification	Verifies the existence of conversation related files on the storage targets.	Media Repository / Application Server	Storage Management Service
	Increase Retention Period	Increases the data retention period for the conversations.	Media Repository / Application Server	Storage Management Service
	Delete Communication Policy Events	Deletes the communication policy events (ethical wall audit log).	Media Repository / Application Server	Storage Management Service
	Deduplicate Recordings	Deduplicates recordings for certain integrations in case of 2N recording.	Media Repository / Application Server	Storage Management Service
	Export	Exports conversations to the configured export target	Media Repository / Application Server or Recording Server (Direct Export)	Storage Management Service
	Advanced IM Export	Provides export functionality specified to Microsoft Teams Chat	Media Repository / Application Server	Storage Management Service
Data Processing	Encrypt and Sign	Encrypts and/or signs conversation related files.	Recording Server or Media Repository / Application Server	Storage Management Service
	Voice Quality Check	Checks voice quality on audio and video recordings.	Recording Server or Media Repository / Application Server	Storage Management Service
	Transcode	Transcodes audio or video files to different formats.	Media Repository / Application Server	Storage Management Service
	Transcription	Transcribes audio conversations.	Speech Analytics Server or Media Repository / Application Server	Speech Analytics Service
Data Import	Data Import	Imports different data into the system	Recording Server or Media Repository / Application Server	Import Service

Enabling data management and processing policy execution on servers

Configured data management policies have to be enabled in the Verba Storage Management Service in order to run them. Please follow the steps below to enable the feature:

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

Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

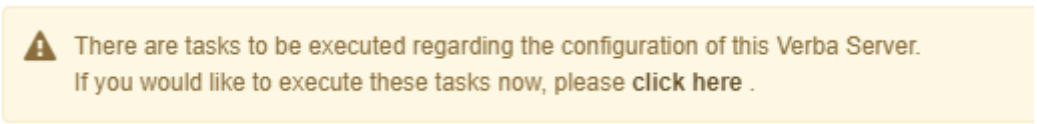
Step 3 - Click on the **Change Configuration Settings** tab and find the **Storage Management / Data Retention** section.

Step 4 - Set the **Enabled** setting to **Yes**.

Step 5 - Configure the **Schedule** setting.

Step 6 - Save the changes by clicking on the  icon.

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



For further information on the configuration settings, check Storage management settings.

Enabling data import policy execution on servers

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

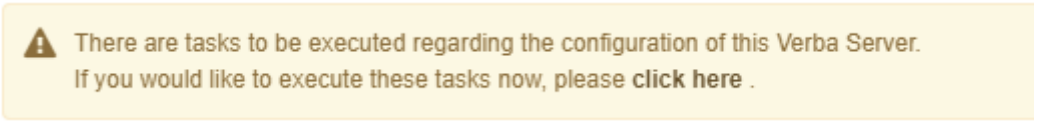
Step 2 - Navigate to the **Configuration / Servers** menu item and select the Media Repository server (or Single server) from the list.

Step 3 - Go to the **Service Activation** tab, then activate the **Verba Import Service** by clicking on the  icon.

Step 4 - Go to the **Change Configuration Settings** tab, configure the schedule settings under the **CDR and Archived Content Importer \ CDR Import** and **Archive Import** nodes.

Step 5 - Save the changes by clicking on the  icon.

Step 6 - A notification banner will appear on the top. Click on the **click here** link, so you will be redirected to the **Configuration Tasks** tab. Click on the **Execute** button in order to execute the changes.



Step 7 - Click on the **Service Control** tab.

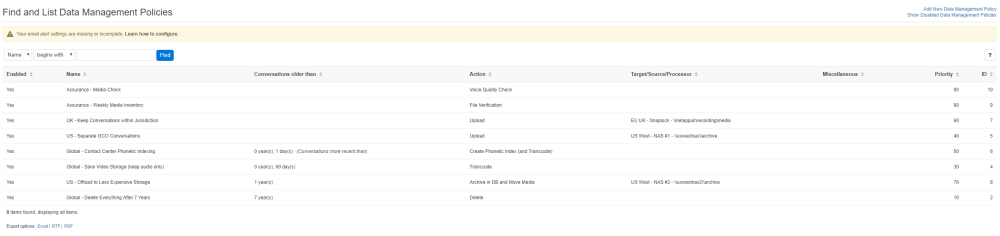
Step 8 - Start the **Verba Import Service** by clicking on the  icon.

For further information on the configuration settings, check CDR and Archived Content Importer settings.

Configuring data management policies

Find and list data management policies

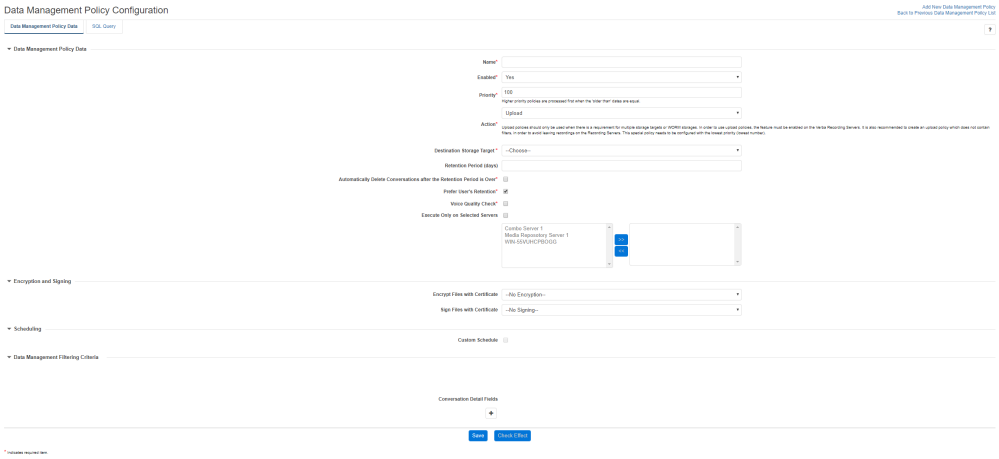
Select the **Data management / Data Management Policies** menu item. You can use the search form below the title, to filter data retention policies: just select your filter and click **Find**.



When you click on a policy (or the **Add New Data Management Policy** button to create a new one), the Data Management Policy Configuration page opens.

Creating a data management policy

You can create a new data retention policy by clicking on the **Add New Data Management Policy** link on the **Administration / Data Management Policies** page. After selecting the link, the following page is opened.



The following table describes the policy settings that are common for all types of policies:

Setting	Description	Requirements
Name	The name of the data management policy.	Required field. Minimum length: 3 Maximum length: 256 Must be unique in the system.
Enabled	Indicates whether the policy is enabled or disabled. Only enabled policies are executed.	Required field.
Priority	Defines the execution order of the policies. This should be an integer number. Higher priority policies are processed first if multiple policies apply to the same call.	Required field.
Action	Defines the policy action. Some of the configuration options are only available with certain actions. The layout of the configuration page changes based on the selected action. For more information on each of the actions and their specific configuration options refer to the individual description pages.	Required field.

Next, by adding filtering criteria, you will need to define the calls the policy should apply to.

Adding Data Management Filtering criteria

You can configure a filter that defines what calls should be included in your data management policy.

- **Conversations Older than** (not available for upload and phonetic index related policy actions): This filtering option defines the age of the calls. Only calls older than the defined value will be handled for the policy during execution.
- **Conversations more recent than** (only available for phonetic index related actions): This filtering option defines the age of the calls. Only calls more recent than the defined value will be handled for the policy during execution.

Click on the + icon to add a new filtering option. You can add as many policies as you want. Multiple field filters are used with 'AND' operator.

The rest of the filtering options are based on various metadata or CDR (Call Detail Record) information that is stored in the database for each conversation. The table below contains a list of potentially available filtering options including custom metadata fields.

Category	Field	Description
Participants	From	The number of the caller party in the conversation

	From Info	The number of the called party in the conversation
	From (digits)	The number of digits in the phone number of the initiator of the conversation
	From Device ID	The Device ID of the initiator of the conversation
	From IP	The IP address of the caller party in the conversation
	To	The name of the caller party in the conversation
	To Info	The name of the called party in the conversation
	To (digits)	The number of digits in the phone number of the target of the conversation
	To Device ID	The Device ID of the target of the conversation
	To IP	The IP address of the called party in the conversation
	Both To or From	The number of any party participating in the conversation
	Both To or From Info	The name of any party participating in the conversation
	Dialed Number	The original dialed number
	User	The user associated with the conversation based on the extension configuration
	User Location	The location of the user, defined in the user configuration
	Extension	The extension numbers in a conversation, a selection list of the configured extensions, otherwise similar to the 'Any party number' field below
	Group	The group where a conversation belongs to based on the users associated with the conversations
	User ID	The User/Agent/Trader ID obtained from the recorded platform
	Participating User	The user that participated in the conversation. (advanced instant message data only)
	Participating User Location	The location of the user that participated in the conversation. (advanced instant message data only)
	Participating Group	The group of the user that participated in the conversation. (advanced instant message data only)
	Other Participant	Other users participated in the conversation. (advanced instant message data only)
Details	Start Time (UTC)	The start time of the conversation in UTC timezone

	Recent Than	Only conversations selected where the start time is recent than the defined value. Make sure it is not used with a recurring schedule, otherwise conversations can be skipped if the defined value is close to the recurring period.
	Direction	The direction of the conversation (e.g. internal, inbound, outbound, etc.)
	End Cause	The end cause of the conversation (e.g. normal, hold, transfer, etc.)
	Duration Interval	The length of the conversation
	Conversation Type	The type of conversation. Available options: • Voice • Video • Instant Messaging • SMS • Desktop Screen • Screen & Application Share (Lync/SfB) • Whiteboard (Lync/SfB) • Poll / Q&A (Lync/SfB) • File Share (Lync/SfB)
	Instant Message Type	The type of IM conversation (Microsoft Teams only). Available options: • Chat • Channel
	Forward Reason	The forward reason for the conversation (e. g. forwarded, transferred, team call, delegated, etc.)
	On-demand	Defines whether a call was recorded as on-demand
	Marked for recording	Defines whether an on-demand conversation was marked for recording
	Protected	Defines whether the conversation is protected
	Label	The labels added to the conversation
	Case	The cases containing the conversation
	Encrypted with Certificate	The certificate used to encrypt the conversation
	Signed with Certificate	The certificate used to sign the conversation
	Quality Management Scorecard exits	Checks if there is a Quality Management Scorecard assigned to the conversation
Analytics	Silence Ratio	The silence ratio in a conversation
	Talkover Ratio	The talkover ratio of the conversation
	Longest Silence	The longest silence present in a conversation
Technical	Recording Server	The hostname of the server that recorded the conversation
	Media File Name	The name of the stored media file

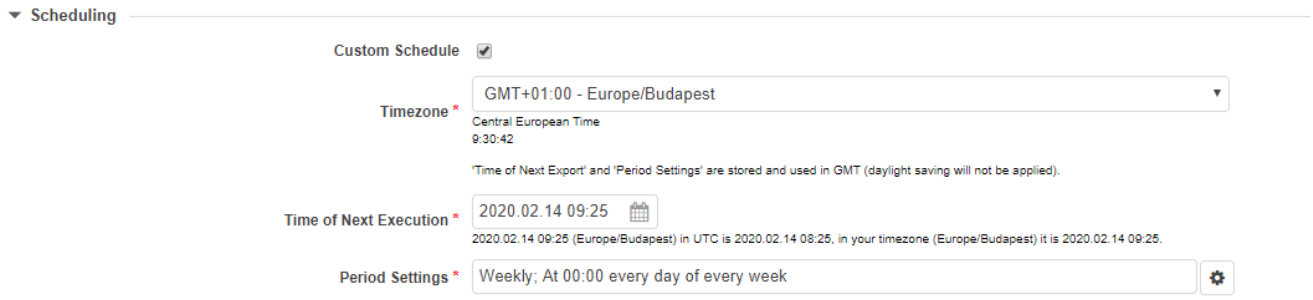
	Storage Target	The current storage location of the media file(s)
	2nd Storage Target	The second storage location of the media file(s) in the case of dual archiving is enabled
	Source Platform	Defines which telephony / unified communications system the conversation was recorded on (Cisco, Sfb, Avaya, etc.)
	Secondary	Defines whether the conversation is recorded on a server marked as secondary (using 2N / duplicate recording)
	CDR/Media Record	Defines whether the conversation is a Standard, CDR-Only or Media-Only record. CDR-Only and Media-Only records are used for trader voice recording.
	Elapsed Time Since Transcoding (UTC)	The time elapsed since transcoding in UTC timezone
	Time of Transcode (UTC)	The date and time of transcoding in UTC timezone
Metadata Fields	Custom Metadata Fields	Custom metadata fields configured in the system, the list of available fields might vary depending on the integration configured and the metadata templates added

If you do not want a Delete policy to delete protected conversations, you have to **explicitly add a 'Protected' = 'No' filter**.

After filling out the form, click the **Save** button to save the data retention policy into the database.

Custom Schedules

You can set up a custom schedule for each policy.



Under *Period Settings* you can configure the frequency, by clicking on the  button at the end of the line.
The Configuration Wizard will appear, here you can set the desired value.

If you leave the *Custom Schedule* option unchecked, then the central settings will take effect.
By setting a custom schedule, you overwrite the central configuration for this policy.

Modifying and deleting data management policies

To edit a data retention entry, you have to click on the desired row of the list showing registered data management policies. After clicking on the row, a new page opens automatically.

To make changes effective, push the **Save** button. All conditions, which are described in the previous part, have to be met.

You can delete the data management policy by clicking on the **Delete** button.

Alerts

The system raises alerts related to data management policies in the following cases:

- policy execution failed
- policy execution finished
- data management policy is created, updated or deleted.

For more information, see Alerts.

Audit log

The system automatically creates audit logs during policy execution which contains record-level information about the executed action. For more information, see Data management policy audit log.