EVOIP*neo* active for SIPREC SRC

Administration manual

for system providers

10/22/2021

Product line *neo*, version 6.x

The described functions can be used with the following ASC products:

EVOIP*neo*

EVOLUTION*neo* / XXL / eco

EVO*flex* (country-specific)

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at http://www.asctechnologies.com.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

1 General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at https://www.asctechnologies.com

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

This manual describes the installation and configuration of the recording solution in the application System Configuration.

Basic information about using the application System Configuration can be found in the user manual for administrators *System Configuration - General information*.

The recording solution EVOIP*neo* active for SIPREC SRC initiated provides the functionality which is necessary for an active IP recording of unencrypted and encrypted conversations in a SIPREC environment.

This recording solution allows recording data streams either in mono or in stereo.

In mono recording, both conversation directions are saved in the same file.

In stereo recording, the conversation directions of the participants are saved in separate files. ASC recommends using stereo recordings for transcription. Transcribing the conversation directions separately renders better results. Stereo recording requires approximately twice as much storage capacity.

The audio data is transferred to the recording server by means of SIPREC. Additional data is transferred by means of SIPREC in an added XML document.

Based on the criteria configured in the Recording Planner, the Recording Control Service makes a recording decision. The EVOIP*neo* Recording Service records the corresponding conversation data and saves them on the recording server.

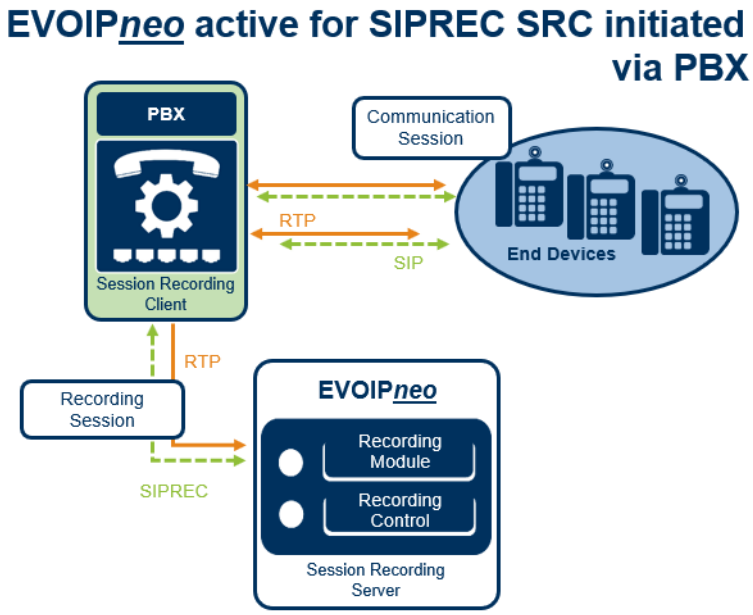


Fig. 1: Overview of the recording solution SIPREC with Session Recording Client

3 System requirements

For basic information about the necessary hardware and software components refer to the installation manual *Installation requirements.*

A list of the codecs supported in this recording solution can be found in the installation manual *Installation requirements*.

A list of the supported PBXs and end devices as well as their supported versions can be found at ASC XCHANGE (https://www.asc.de/partner) in the current *neo Integration Overview*.

3.1 Hardware components

For basic information about the necessary hardware components refer to the installation manual *Installation requirements.*

EVOIP*neo* recording software can be used on the customer's existing hardware. Alternatively, you can use ASC recorders.

3.1.1 Recorder

For the recording solution you can use the following systems:

- EVOLUTION*neo* eco
- EVOLUTION*neo*
- EVOLUTION*neo* XXL

With hybrid systems (VoIP and TDM) the required software for the recording solution has already been installed on the EVOLUTION*neo* recorder. If more performance is needed, an additional EVOLUTION*neo* recorder or EVOIP*neo* server can be added.

3.2 Software components

For the recording, you need the installation medium with the server software *neo* Suite which is installed on the ASC recording server.

3.3 External components

A list of the supported PBXs and end devices as well as their supported versions can be found at ASC XCHANGE (https://www.asc.de/partner) in the current *neo Integration Overview*.

3.3.1 PBX

Supported are PBXs end devices which use SIP as signaling protocol.

3.3.2 Supported PBXs and end devices

- RFC 4733 (DTMF) optional
- RFC 6086 (DTMF via SIP INFO) optional
- RFC 6341 (SIP-based media recording)
- RFC 7245 (SIP-based media recording)
- RFC 7865 (SIPREC recording metadata)
- RFC 7866 (SIPREC protocol)

- RFC 8068 (SIPREC protocol)

ASC gives no guarantee for the functionality of untested end devices.

3.3.3 Genesys system components (optional)

3.3.3.1 Genesys Framework

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

4 Installation requirements

For basic information about the used default ports refer to the installation manual *Installation requirements* in chapter *Communication matrix*.

If you have configured customer-specific ports, you have to open them in the firewall separately.

4.1 Licenses

ASC

License name	Number
EVOIP*neo* Base license - active	1 license per recording server
EVOIP*neo* active for SIP	1 license per concurrent recording

Tab. 1: Licenses of ASC

Sparkassen FI ISP (optional)

License name	Number
CTI*connect* for Sparkassen FI ISP	1 per recording system

Tab. 2: Licenses for Sparkassen FI ISP optional

OpenScape Contact Center (optional)

License name	Number
CTI*connect* for Unify OpenScape Contact Center	1 per recording system
SDK license for OpenScape Contact Center of Unify	1 per monitored business unit Number of the SDK licenses
Search & Replay Access software license	1 per concurrent user
Search & Replay Access system license	1 per recording system

Tab. 3: Licenses for OpenScape Contact Center optional

Genesys T-Server (optional)

License name	Number
CTI*connect* for Genesys T-Server	1 per recording system
Genesys Recording Connector	1 per monitored recording resource
Genesys Universal SDK	1 per recording server

Tab. 4: Licenses for Genesys

4.2 Information

Before you start the installation, make sure that the following information is available:

- IP address of the recording server
- SIP port of the recording server

In this recording solution, the SIP authentication methods *basic* and *auth* are supported.

5 Overview install and configure product

The following steps have to be carried out:

1. Install *neo* software
2. Configure PBX
   - Since the configuration is vendor-specific, the steps cannot be described here. The configuration is usually done by the telecommunication technician.
3. Configure System Configuration
   - Create and activate recording architectures
     - The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.
   - Configure servers
     - In the Servers module, the usage of the server is configured.

       A server can be used for archiving, import, export, replay, data storage or for audio analysis.
   - Create PBX
     - A PBX configuration can either be created via the PBX module or via the configuration in the Integrations module.
   - Configure integration
     - Configure recording architecture
       Connecting integration with the previously created recording architecture
     - Configure CTI connection data
       Configuration of CTI connection parameters and of the grammar
     - Global recording settings
       Configuration of port and transport protocol for SIP signaling
     - Configure recording servers
       Configuration of the parameters of the recording server, e. g. IP address, RTP incoming port and extensions
   - Configure add-on
     The add-on is disabled by default.
     Optionally, you can configure the following add-ons for this recording solution:

     OpenScape Contact Center

     Sparkassen FI ISP

     Genesys T-Server
   - Configure miscellaneous settings
     Optional configuration of participant information in an additional data field

6 Installation

Before installing the *neo* software, ensure that Microsoft Windows has been installed and configured according to our specifications.

For information about the installation and configuration of Microsoft Windows refer to the respective installation manual for system providers *Configuration Windows Server 2012 R2*, *Configuration Windows Server 2016* or *Configuration Windows Server 2019*.

For information about the installation of the *neo* software refer to the installation manual for system providers *Installation of the recording software of ASC*.

6.1 Install certificate for TLS encryption

For encrypted transfer between the recording server and the SIP trunk, both components must be able to match and confirm the certificate of the other participant. Therefore, both certificates must be available on both components.

To be able to establish an encrypted connection, proceed as follows:

- chapter "Import certificate to recording server", p. 11
- chapter "Import certificate to SIP client", p. 14

6.1.1 Import certificate to recording server

To enable the recording server to confirm the certificate of the SIP client, the certificate must be available on the recording server.

There are 2 possibilities to import TLS certificates:

- *Installing a customer-specific certificate, see*
  chapter "Import customer-specific certificate to the recording server", p. 11
- *Installing PBX certificate already existing on the SIP client, see*
  chapter "Import PBX certificate to recording server", p. 13

6.1.1.1 Import customer-specific certificate to the recording server

If you would like to use a customer-specific certificate, you can import it to the keystore of the recording server by means of the program *certimporter.exe*.

1. To import the TLS certificate to the recording server, change to the recording server.
2. Open the tool Certificate Import Tool in folder
   C:\Program Files (x86)\ASC\ASC Product Suite\scripts.
   ⇨ The window Certificate Import Tool appears.

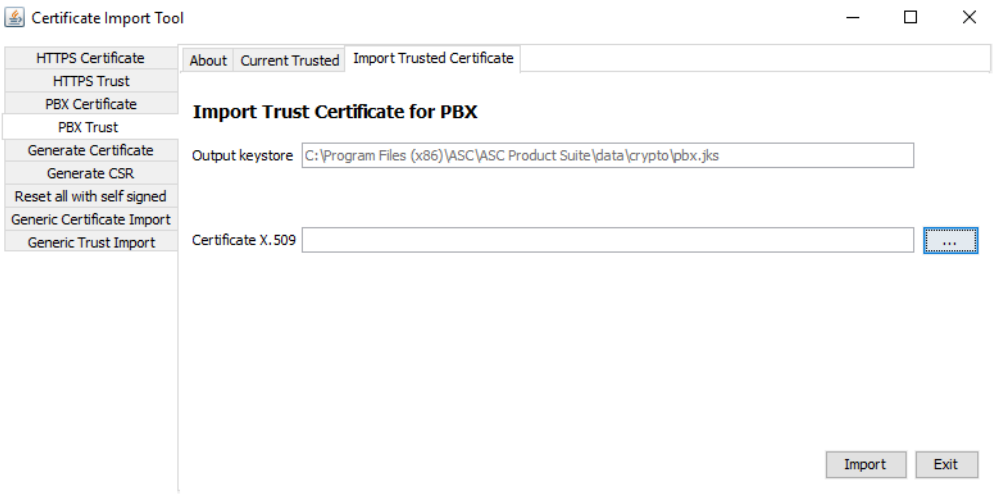


Fig. 2: Selection of the certificate

3. Select the menu item *PBX Trust* in the navigation bar.
   This function enables you to fill the keystore with the customer-specific certificate.
4. Select the tab *Import Trusted Certificate*.
5. Click on the button ··· next to the field *Certificate X.509* to select the certificate file.

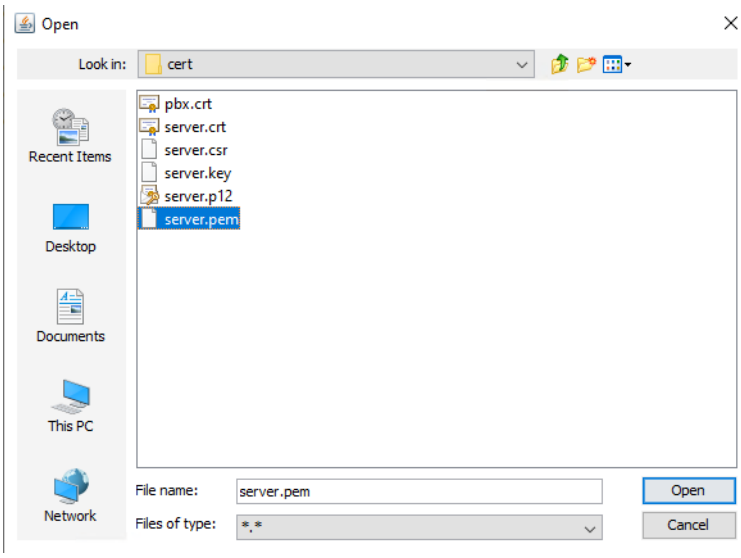


Fig. 3: Import certificate

6. Select the certificate file *server_certificate.pem* that you have copied from the SIP client.
7. Click on the button *Open*.
   ⇨ The window to enter the alias appears.

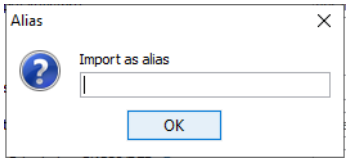


Fig. 4: Confirm alias

8. Enter the name of the SIP client.
9. Click on the button *OK* to confirm the alias.
   ⇨ A message will inform you about the successful import.

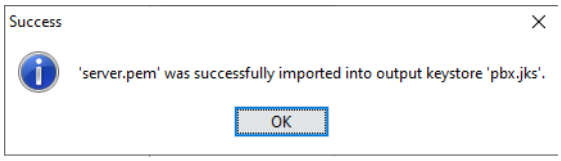


Fig. 5: Message - Successful import

10. Click on the button *OK* to confirm the success message.
11. Click on the button *Exit* to close the program Certificate Import Tool.

6.1.1.2 Import PBX certificate to recording server

By means of this function you overwrite the delivered certificate on the recording server with the certificate of the SIP client or of the PBX.

1. Copy the certificate from the SIP client or from the PBX to the recording server.
2. Open the tool *Certificate Import Tool* in the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
   ⇨ The window *Certificate Import Tool* appears.

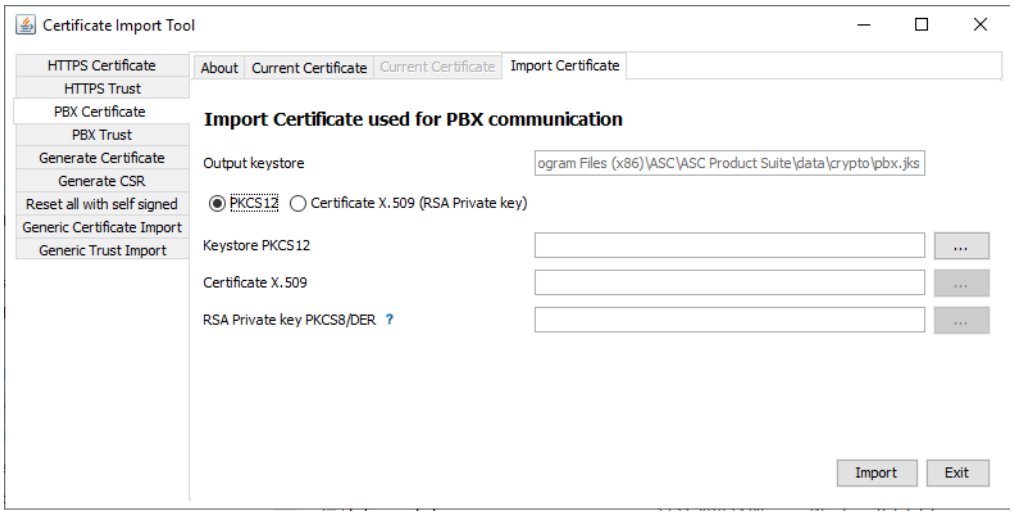


Fig. 6: Selection of the certificate

3. Select the menu item *PBX Certificate* in the navigation bar.
   By means of this function you overwrite the delivered certificate on the recording server.
4. Select the tab *Import Certificate*.
5. Select the format of the certificate.
6. Click on the button ··· next to the respective entry field to select the certificate file.
7. Select the respective certificate file that you have copied from the SIP client.
8. Click on the button *Open*.
   ⇨ The window to enter the alias appears.
9. Enter the alias of the SIP client.
10. Click on the button *OK* to confirm the alias.
    ⇨ A message will inform you about the successful import.
11. Click on the button *OK* to confirm the success message.
12. Click on the button *Exit* to close the program *Certificate Import Tool*.

6.1.2 Import certificate to SIP client

To enable the SIP client to confirm the certificate of the recording server, the certificate of the recording server must be available in the certificate management of the SIP client.

6.1.2.1 Export TLS certificate from recording server

1. To export the certificate from the recording server, change to the recording server.
2. Open the Certificate Import Tool *certimporter.exe* in the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
   ⇨ The following window appears:

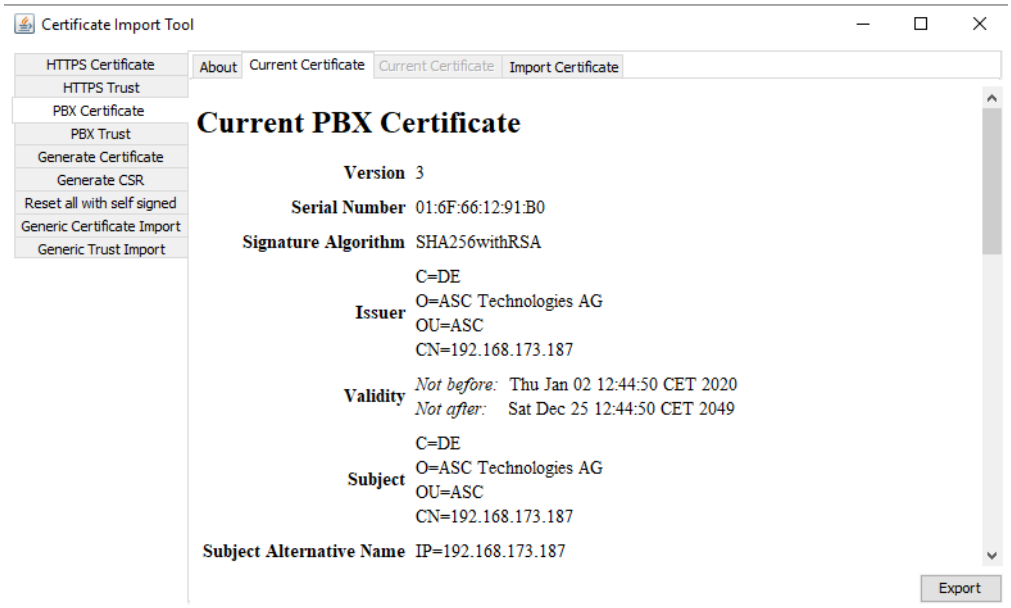
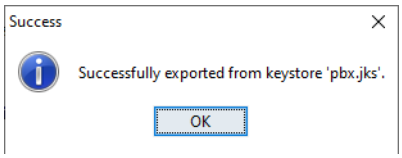


Fig. 7: Export PBX certificate from recording server

3. Select the menu item *PBX Certificate* in the navigation bar.
4. Click on the tab *Current Certificate*.
5. Click on the button *Export* to export the current certificate.
6. Select an appropriate storage location for the certificate.
7. Click on the button *Save*.
   ⇨ A success message appears.



8. Upon confirmation, you can import the certificate to the SIP client.

6.1.2.2 Import TLS certificate to SIP client

To be able to establish an encrypted connection to the recording server, you must import the certificate of the recording server to the trust store in the certificate management of the SIP client.

7 Configuration

7.1 System Configuration

Basic information about using the application System Configuration can be found in the user manual for administrators *System Configuration - General information*.

7.1.1 Start application

During the installation routine, shortcuts for the *neo* programs are created on your desktop.

1. To start the application directly on the server, double-click on the shortcut System Configuration.
   To access the application from a computer via the web, enter the following URL in the address bar:
   https://<System-IP>/SystemConfiguration.
   If you have configured customer-specific ports, you have to include the port in the URL:
   https://<System-IP>:<Port>/SystemConfiguration.

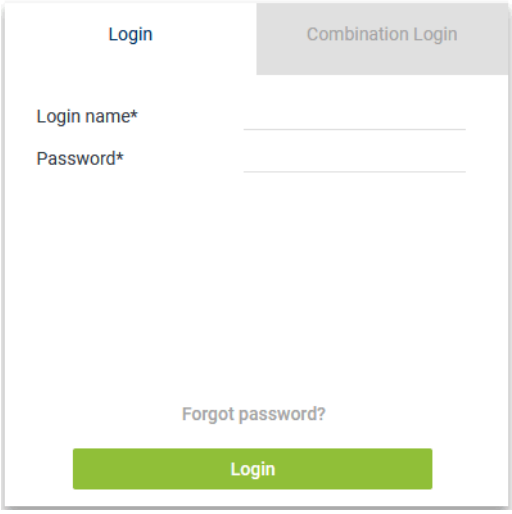


Fig. 8: System Configuration - web interface

To install and configure the recording solutions, you have to log in as system provider.

Login data for the administrator of the system provider:

User name:	*system-admin*
neo version < 6.3	
Default password:	*1* If the default password *1* has never been changed before a software update to a *neo* version ≥ 6.3, the password must be changed upon the next login or by entering it again. If the default password has already been changed before a software update to a *neo* version ≥ 6.3, the changed password remains.
neo version ≥ 6.3	
Default password:	*A$c123*

Tab. 5: Login data - system provider

2. Log in to the web interface.
   ⇨ The main window System Configuration appears.

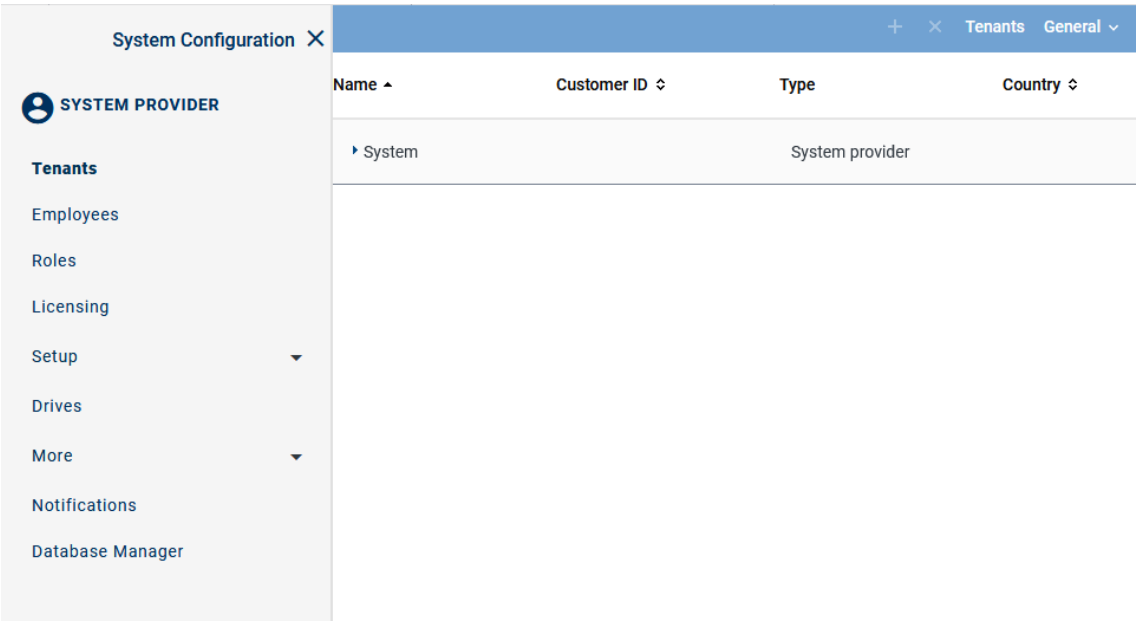


Fig. 9: System Configuration - main view:

7.1.2 Configure recording solution

Supported recording architectures

In this recording solution, the following recording architecture types are supported:

- All-in-one Basic Recording
- All-in-one Failover
- All-in-one Parallel Recording
- Multi-Server Recording
- Multi-Server Failover
- Multi-Server Parallel Recording

7.1.2.1 Configure recording solution All-in-one Basic

7.1.2.1.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

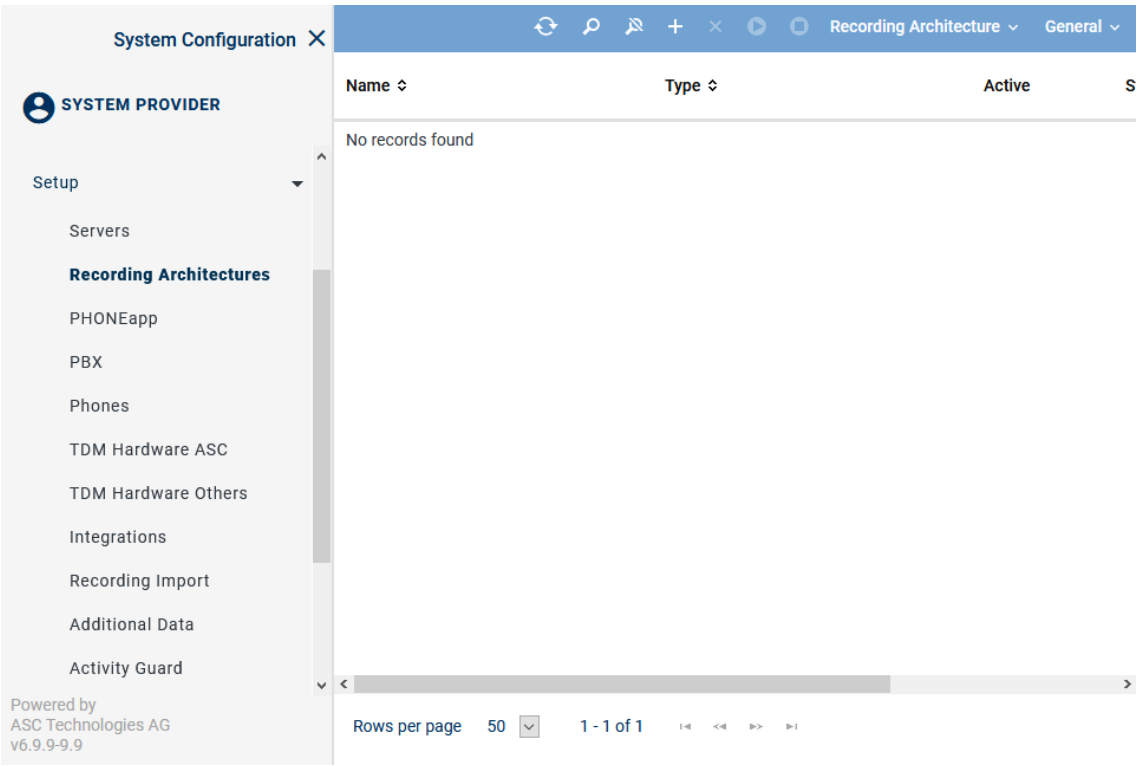


Fig. 10: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Recording Architectures module

The toolbar offers the following functions.

Fig. 11: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.

		The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Create	Creates a new recording architecture.
	Delete	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. **NOTICE!** You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	Activate	Activates the selected recording architecture.
	Deactivate	Deactivates the selected recording architecture. **NOTICE!** You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
Recording Architecture	*Standby Management*	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create recording architecture All-in-one Basic

If the entire *neo* software has been installed on one server, you must create a recording architecture of the type *All-in-one Basic Recording*.

Depending on the selected recording architecture type, the following configuration steps vary.

The following configuration steps are exemplary for the recording architecture *All-in-one Basic Recording*.

1. To create a new recording architecture, click on the icon *(Create)* in the toolbar of the main view.

   ⇨ The window *New Recording Architecture* appears.

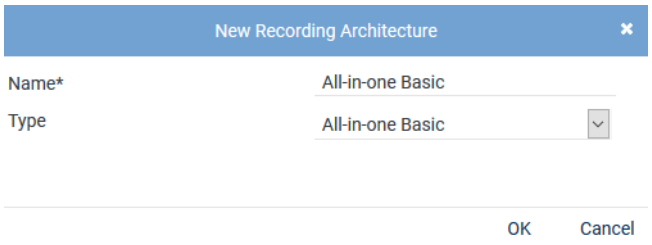


Fig. 12: Create recording architecture - All-in-one Basic Recording

2. In the entry field *Name*, enter a descriptive name for the recording architecture.
3. From the drop-down list *Type*, select the recording architecture type *All-in-one Basic Recording*.
   NOTICE! The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.
   ⇨ Your entries now appear in the detail view.

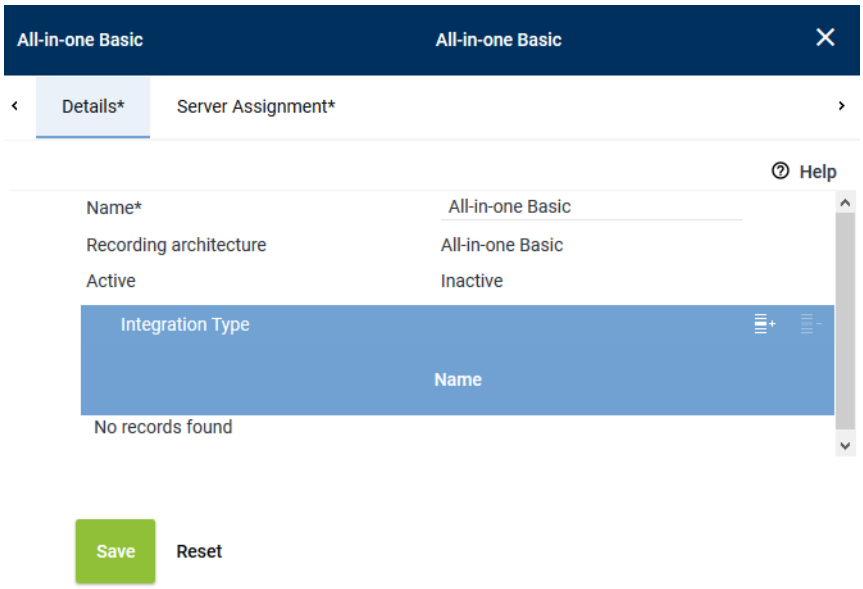


Fig. 13: Recording architecture - tab Details

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 14: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for All-in-one Basic

1. Click on the tab *Server Assignment* to assign a recording server to the recording architecture..

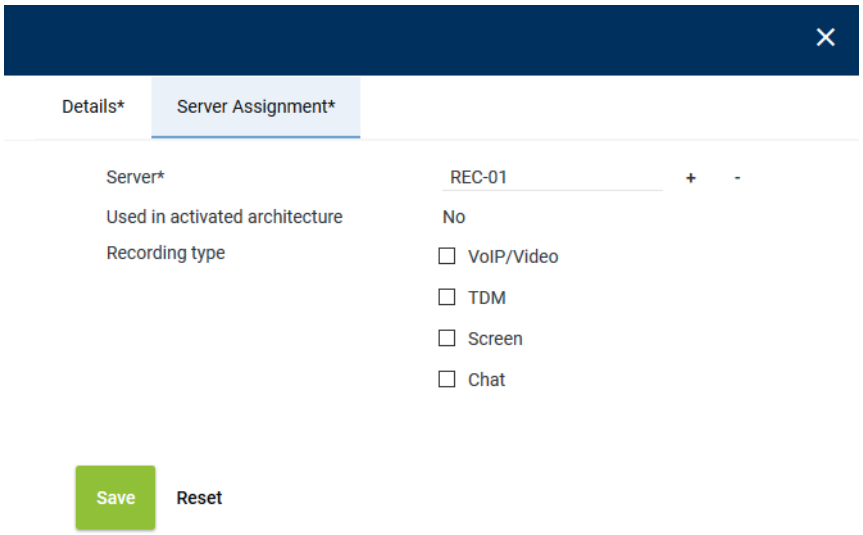


Fig. 15: Recording architecture - tab Server Assignment

2. Click on the button + next to the entry field *Server*.
   ⇨ The window *Servers* appears.

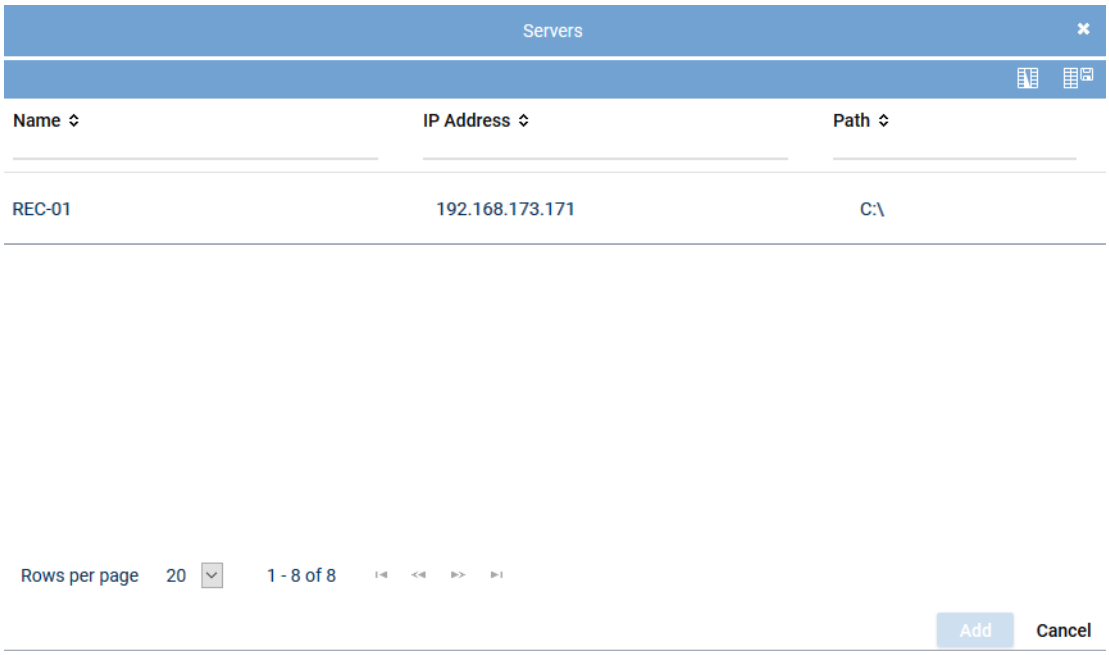


Fig. 16: Recording architecture - assign server

3. Select the respective server.

A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

4. Click on the button *Add*.
   ⇨ The name of the server appears in the detail view.
5. Activate the check boxes in front of the recording variants that you would like to use this server for.

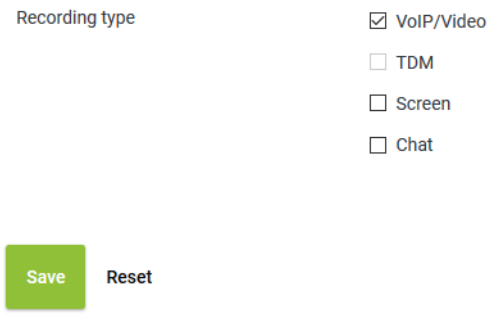


Fig. 17: Recording architecture - activate recording variant

You can activate several recording types if the integration has been designed for this and if you have installed the respective licenses.

Activate recording architecture

1. Click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the toolbar becomes active.

3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

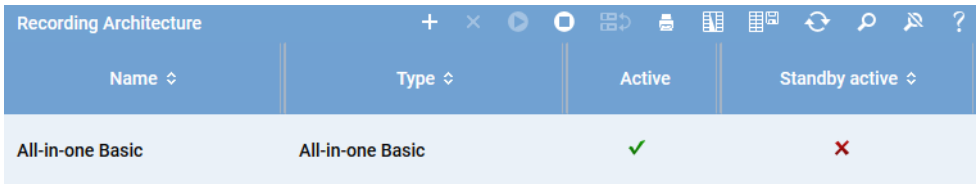


Fig. 18: Recording architecture - activate recording architecture

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✗ *(Inactive)* appears.

ⓘ The recording architecture must have been activated so that the integration can be configured.

ⓘ If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.1.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

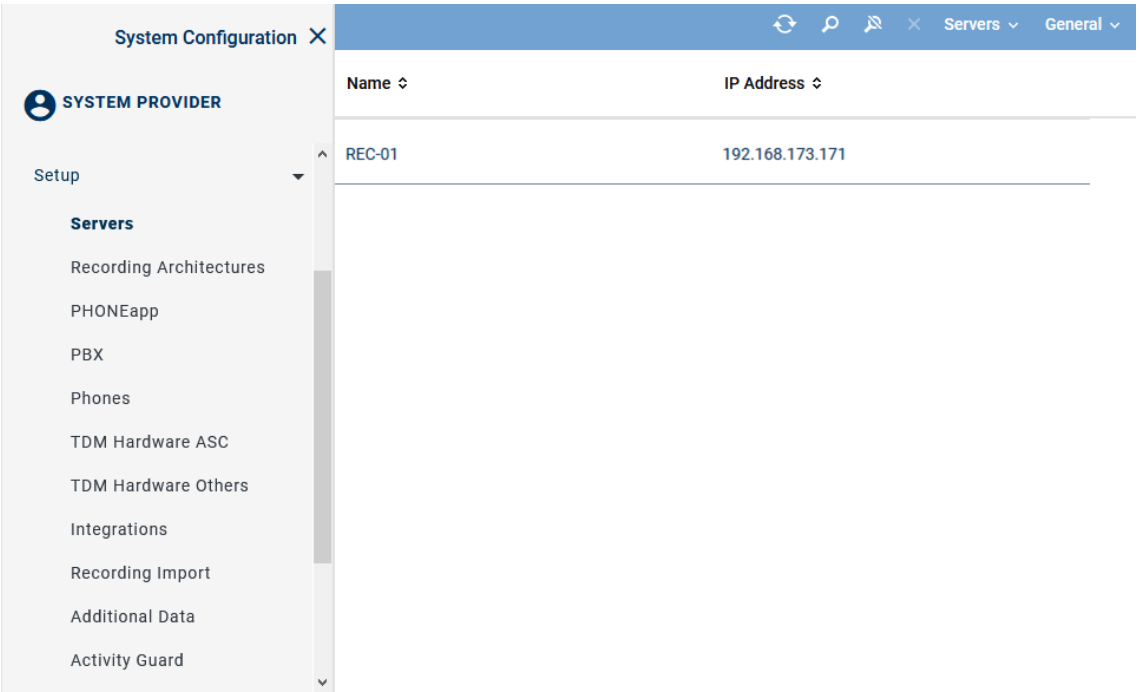


Fig. 19: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.
Path	Shows the path of the server.

Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 20: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.
Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 23.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.

⇨ The window *Server Locations* appears.

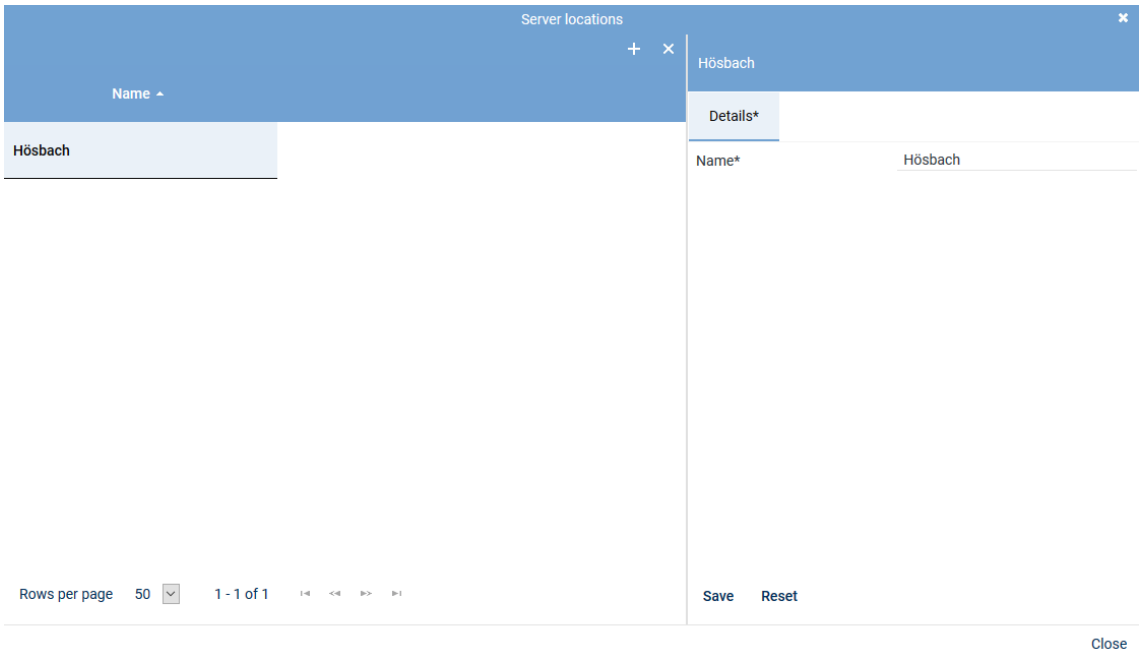


Fig. 21: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

ⓘ A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

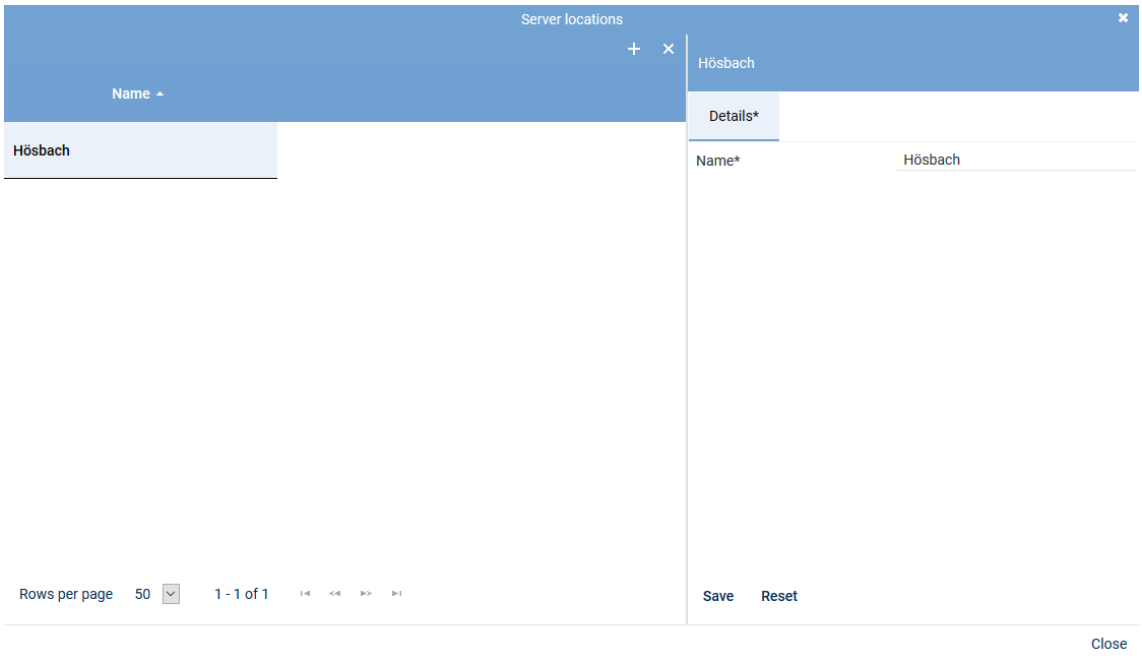


Fig. 22: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

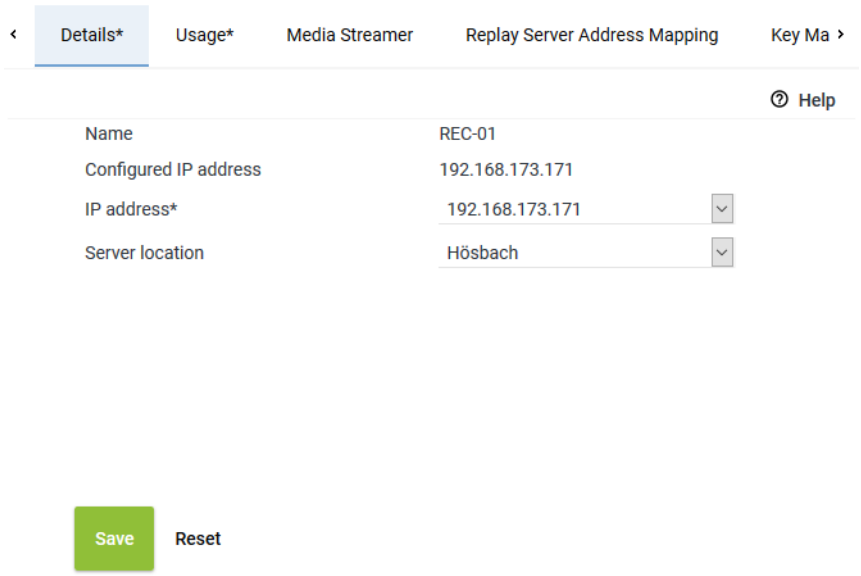


Fig. 23: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.

4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

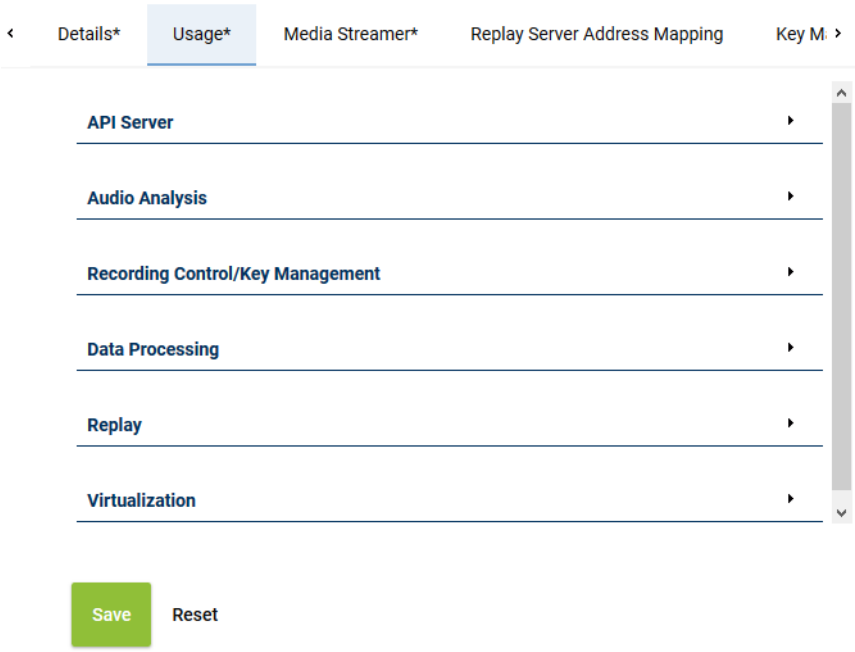


Fig. 24: Servers - tab usage

Group field API Server

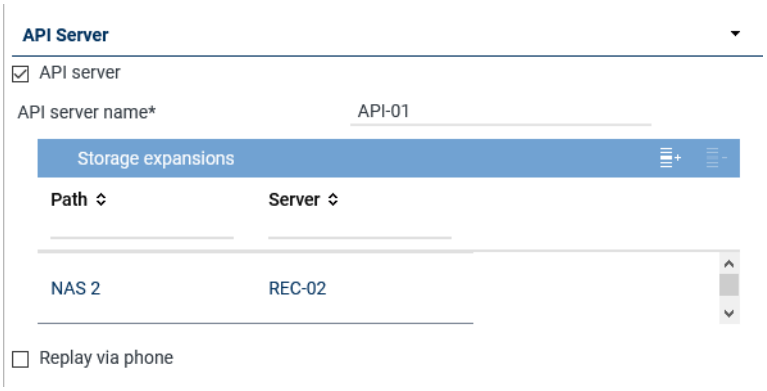


Fig. 25: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server.

Parameter	Value/Description
	☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 37.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List *Storage expansions*	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 28. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list. If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 35. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

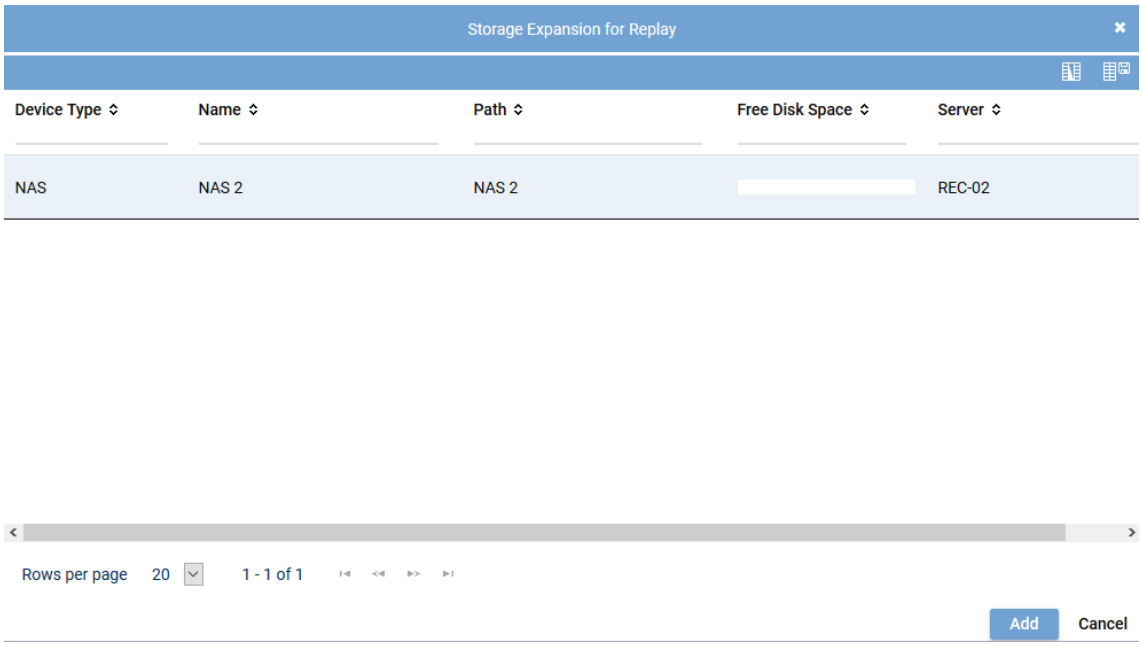


Fig. 26: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

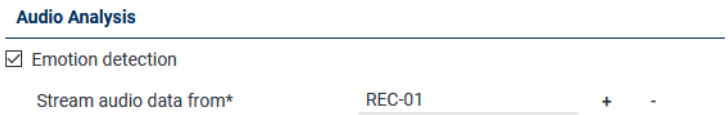


Fig. 27: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 6: Configure audio analysis

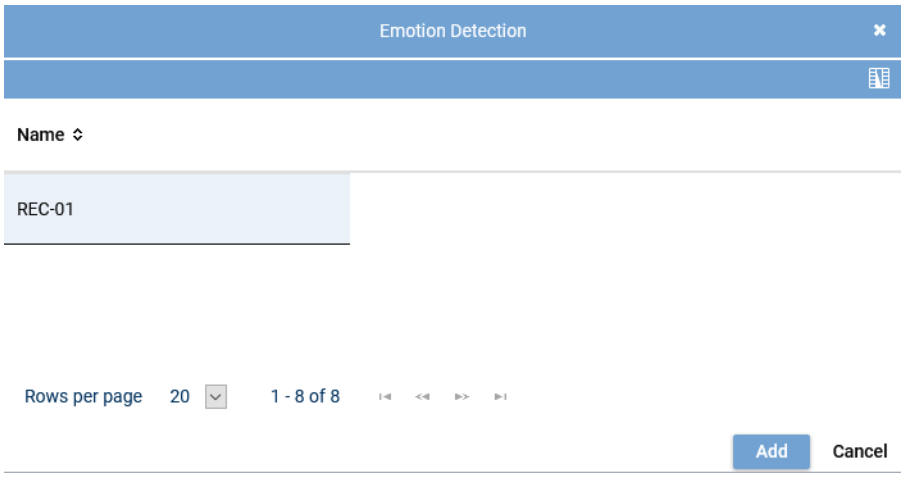


Fig. 28: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

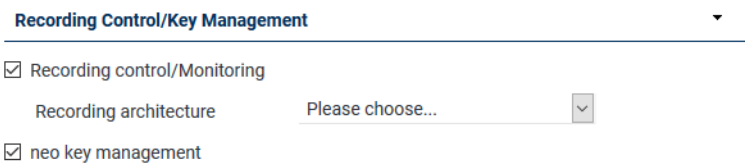


Fig. 29: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 7: Configure recording control/key management

Group field Data Processing

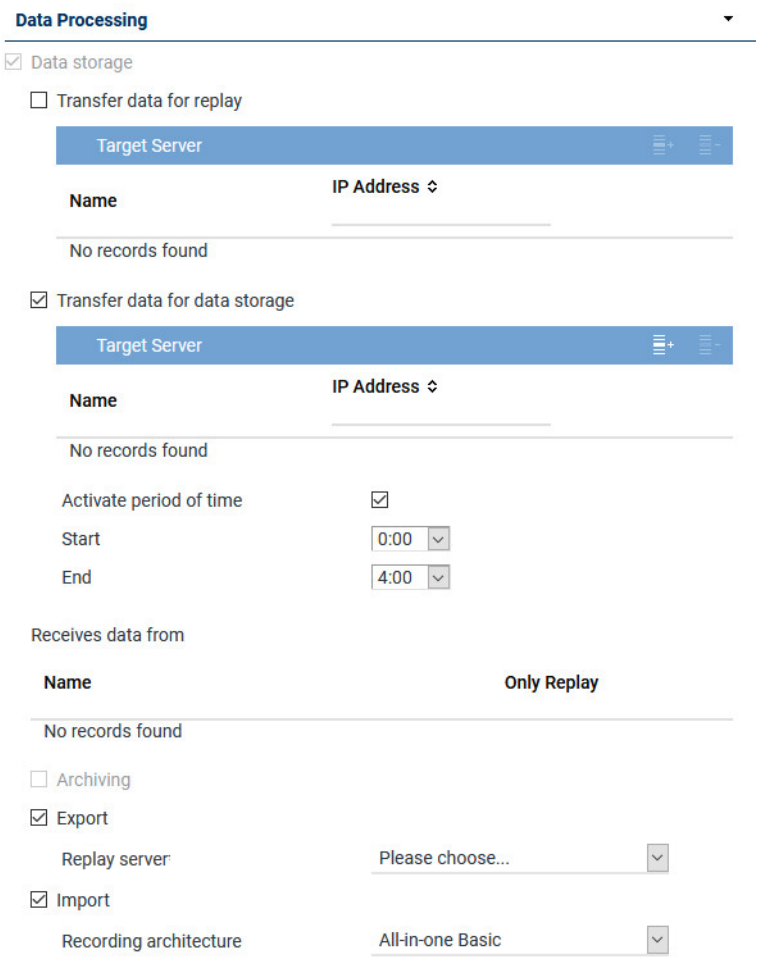


Fig. 30: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 32. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be trans-

Parameter	Value/Description
	ferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 32. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.

Parameter	Value/Description
	NOTICE! If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 8: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 31: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

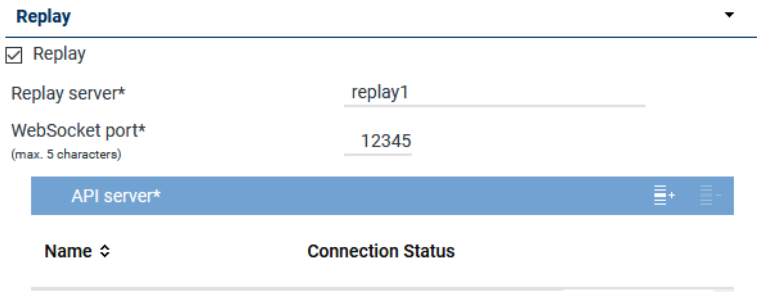


Fig. 32: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 33. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 9: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.

- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

Fig. 33: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 26.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 34: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management.

Parameter	Value/Description
	• *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 10: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

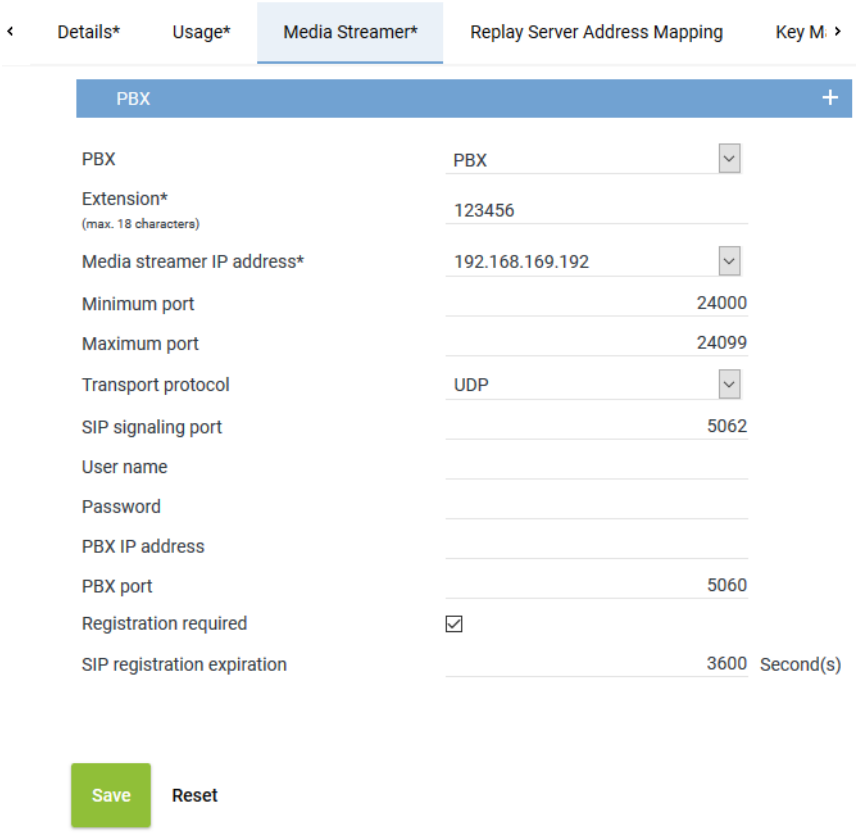


Fig. 35: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.

	If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 41.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number. A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

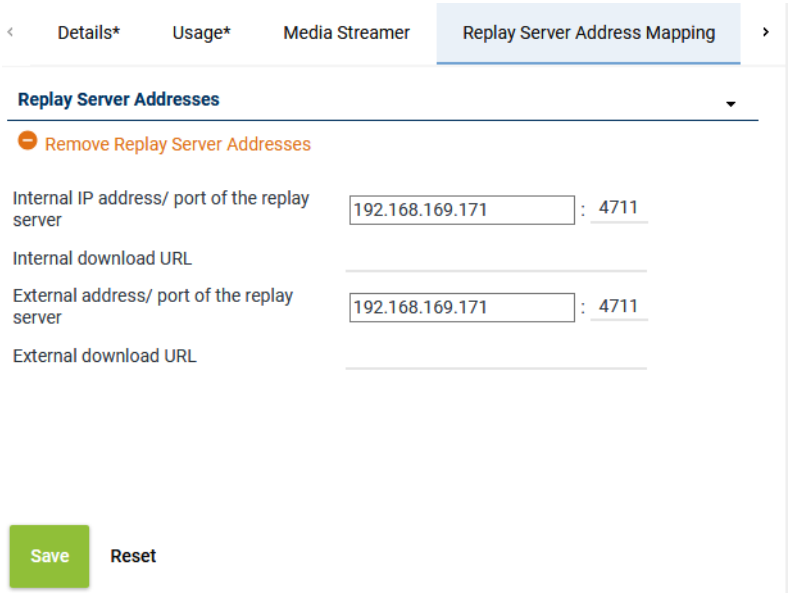


Fig. 36: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

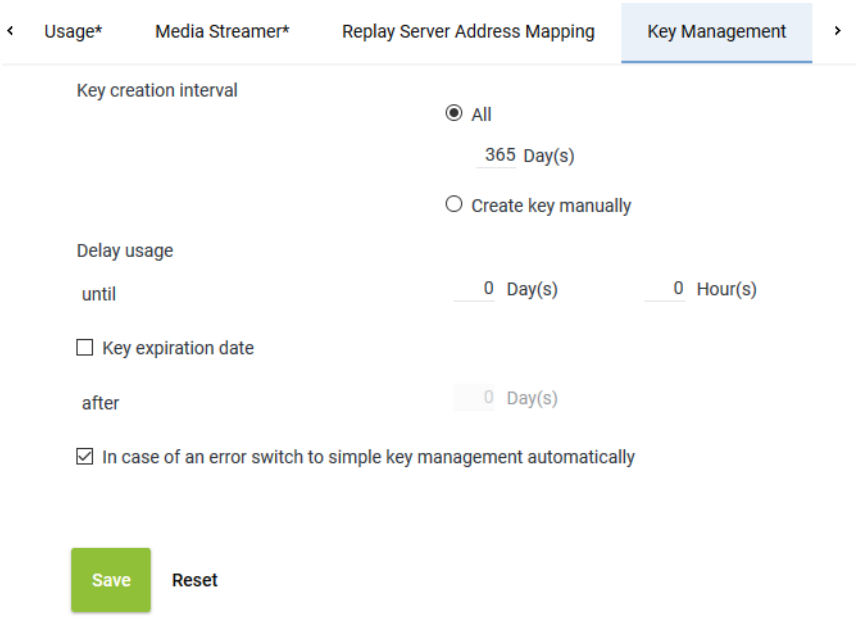


Fig. 37: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.

Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid. ☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

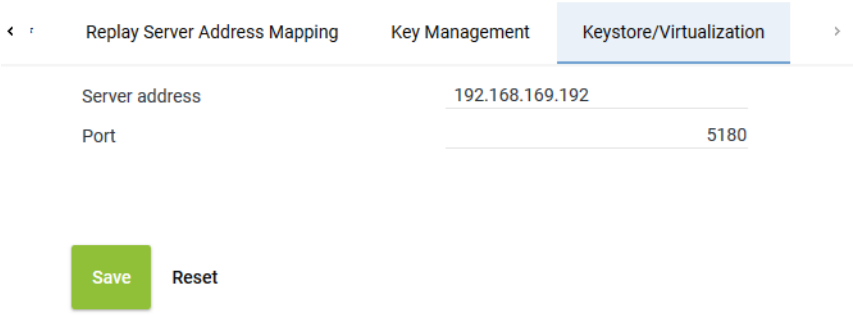


Fig. 38: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management:

	IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.1.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

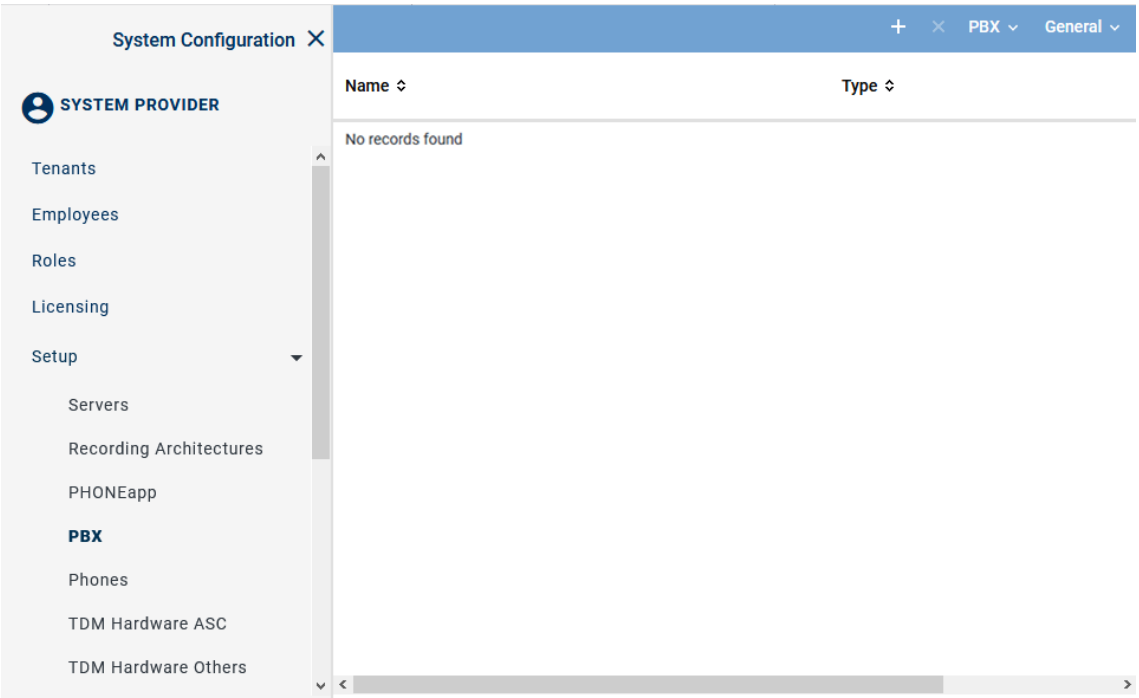


Fig. 39: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 40: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.

PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

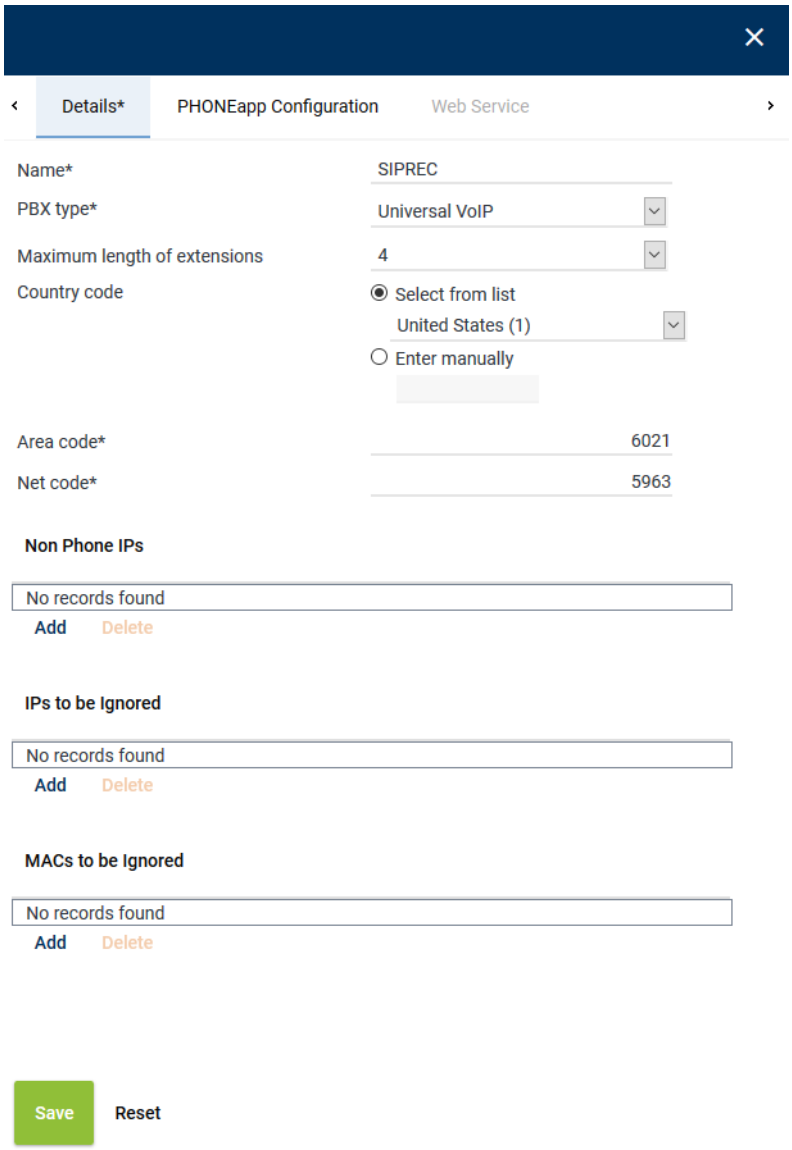


Fig. 41: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list* Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 11: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 12: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.1.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

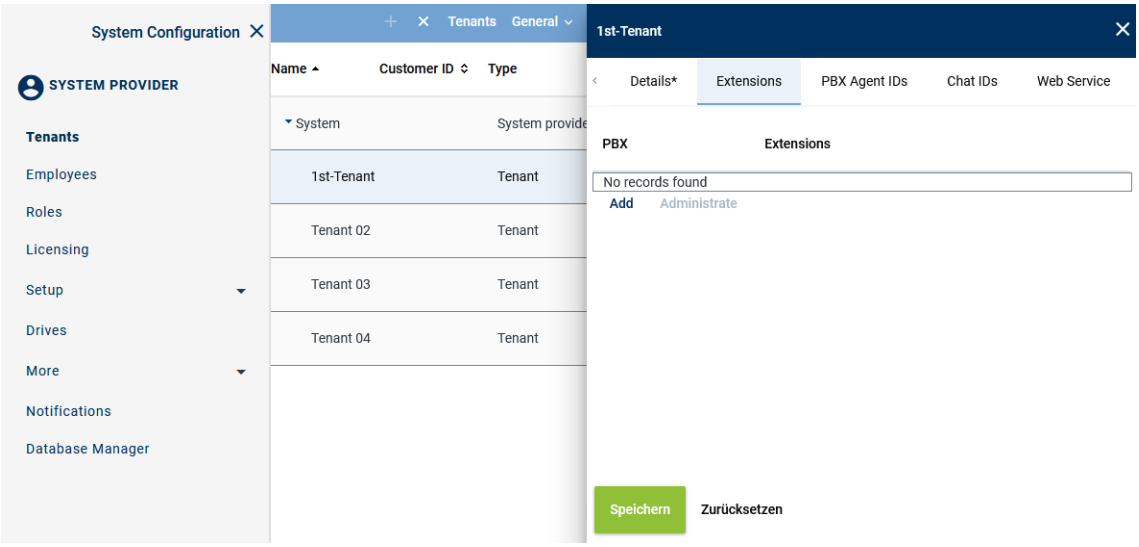


Fig. 42: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.

⇨ The following window appears:

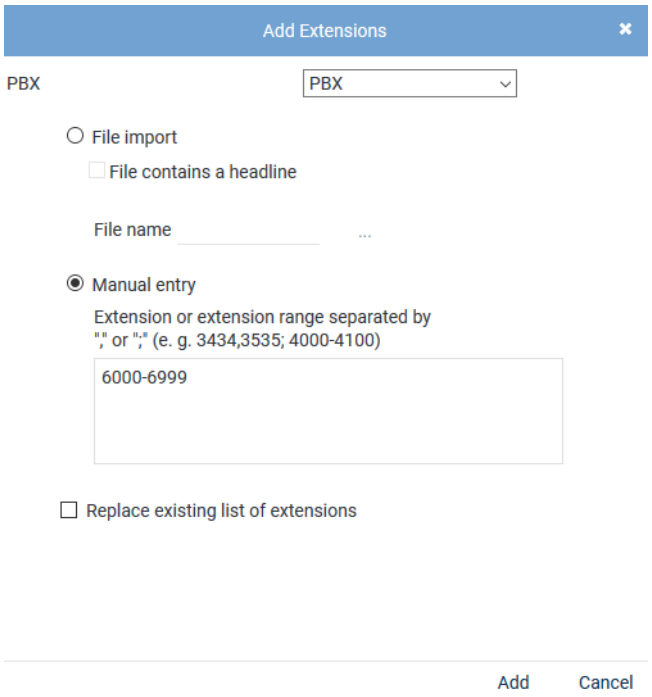


Fig. 43: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT* • *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually.

	To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

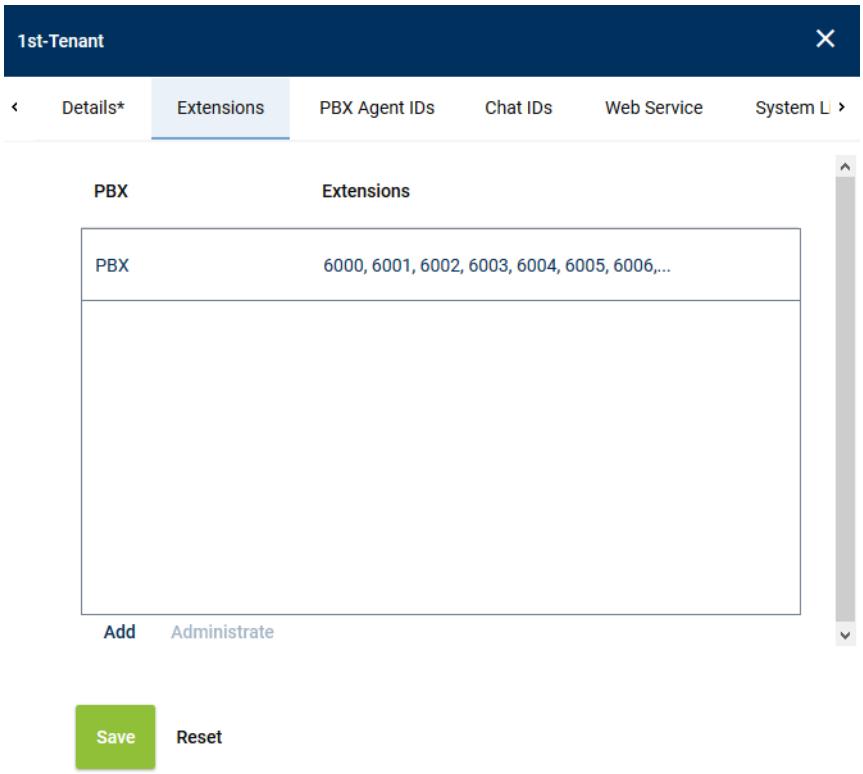


Fig. 44: Remove extensions

2. Click the button *Administrate*.

3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 45: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

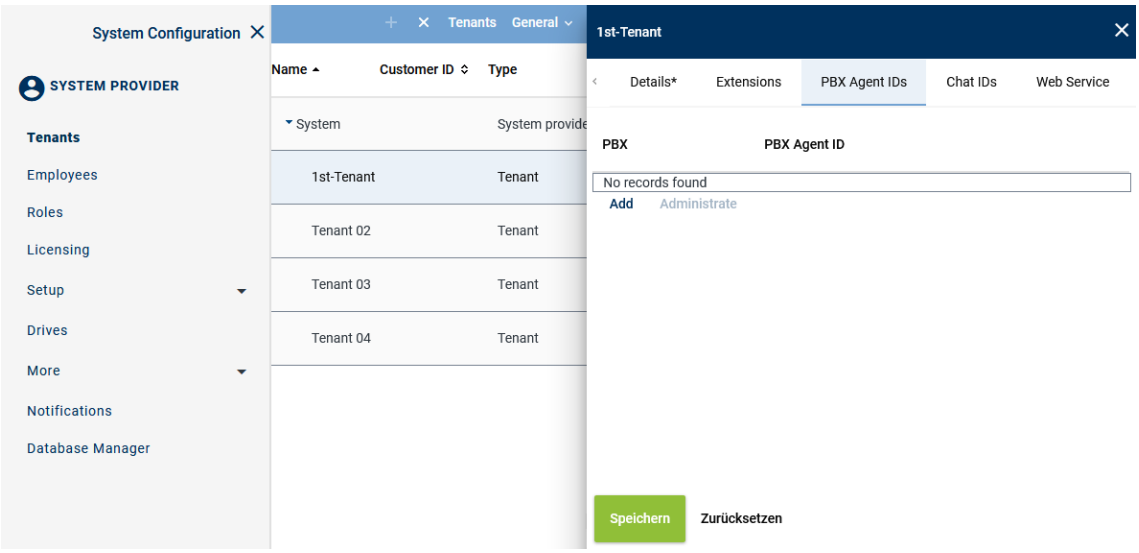


Fig. 46: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

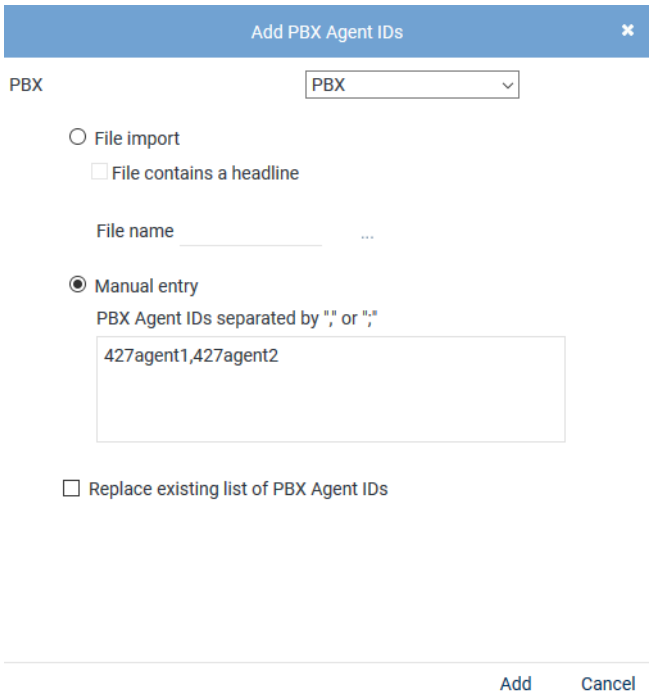


Fig. 47: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline

	Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

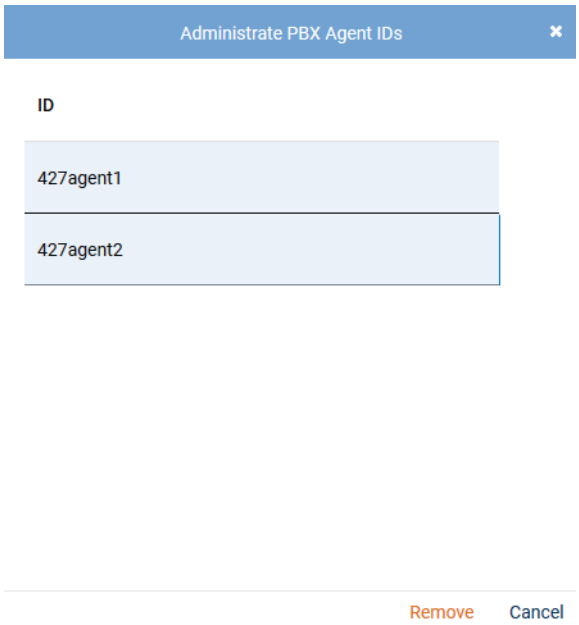


Fig. 48: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.1.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

> In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

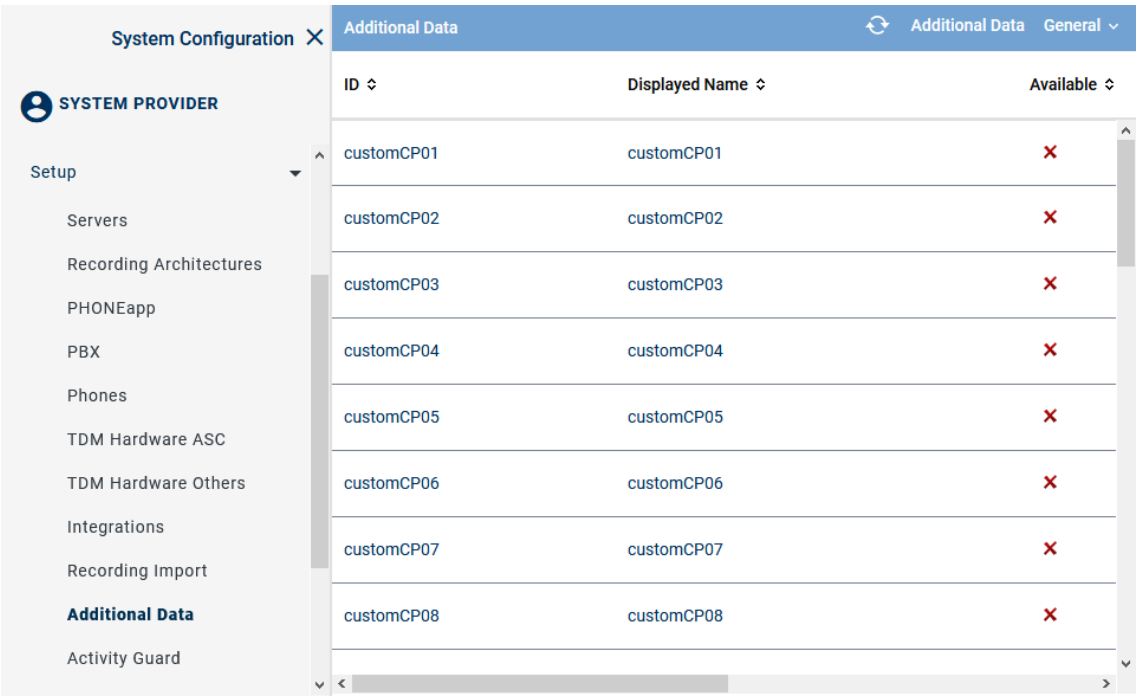


Fig. 49: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

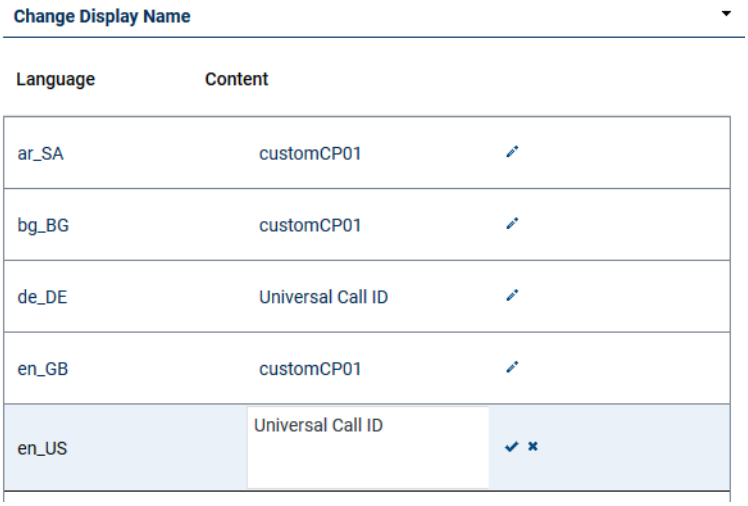


Fig. 50: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 51: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.1.6 Create integration for All-in-one Basic

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

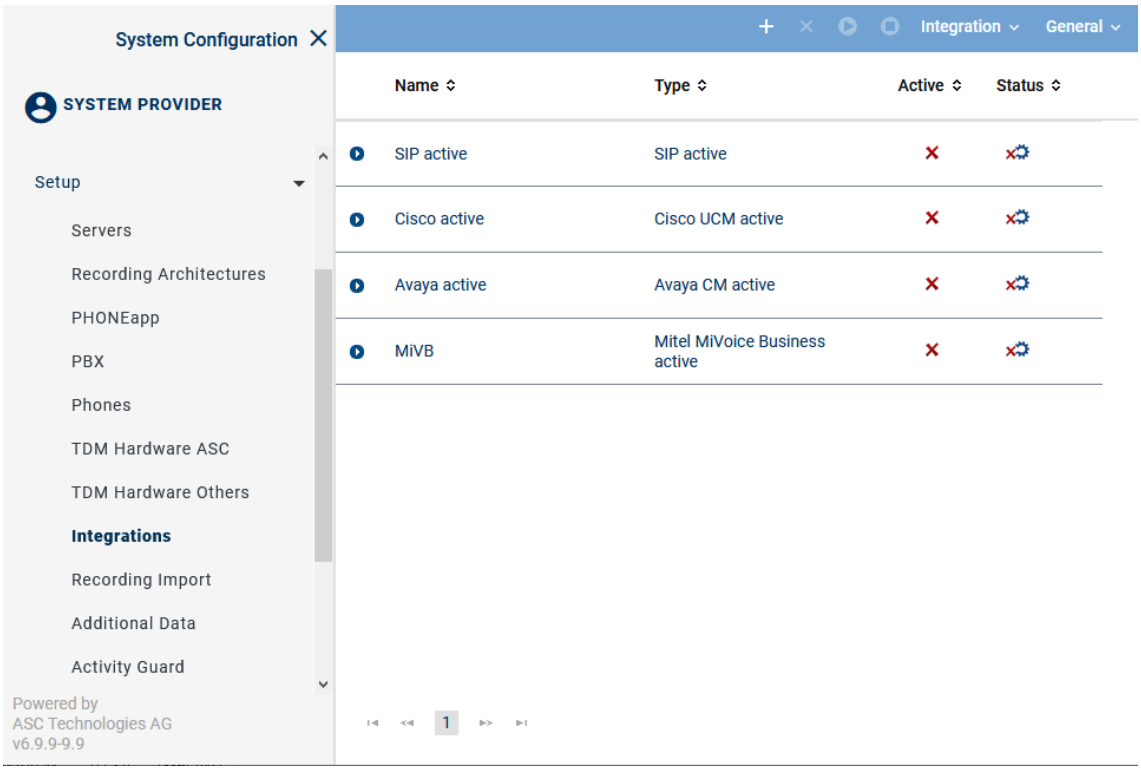


Fig. 52: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 53: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

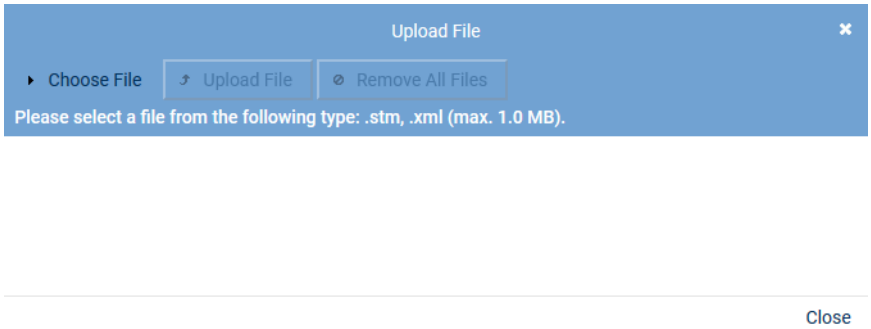


Fig. 54: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

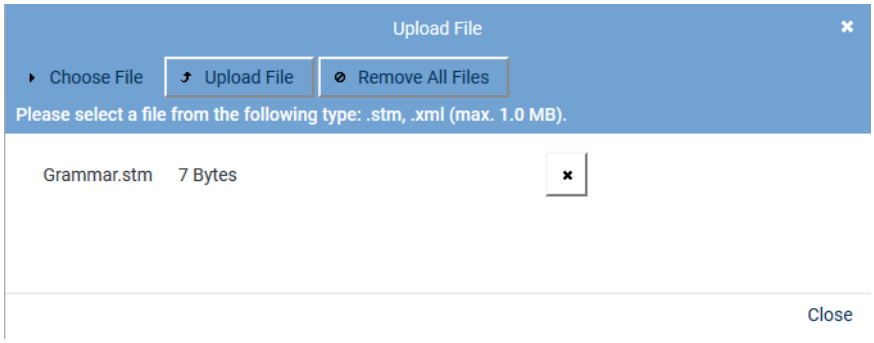


Fig. 55: Upload grammar

5. To remove a selected file from the list, click on the button × *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 56: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 13: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 57: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for All-in-one Basic

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

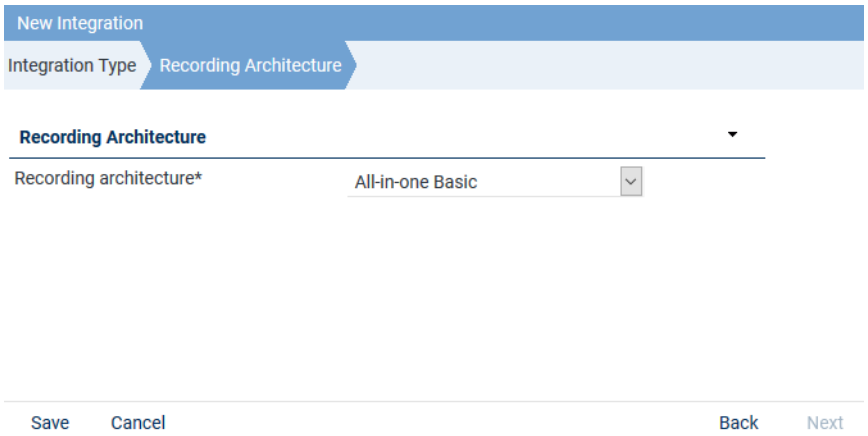


Fig. 58: Assign recording architecture - All-in-one Basic

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

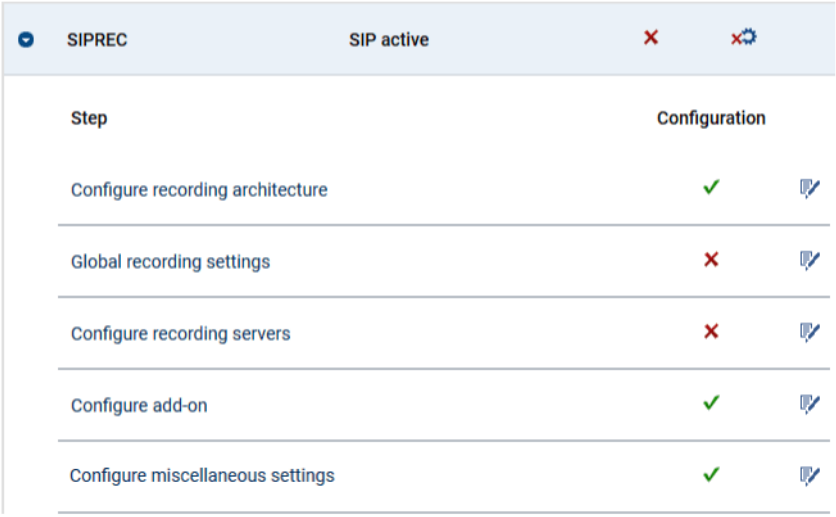


Fig. 59: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

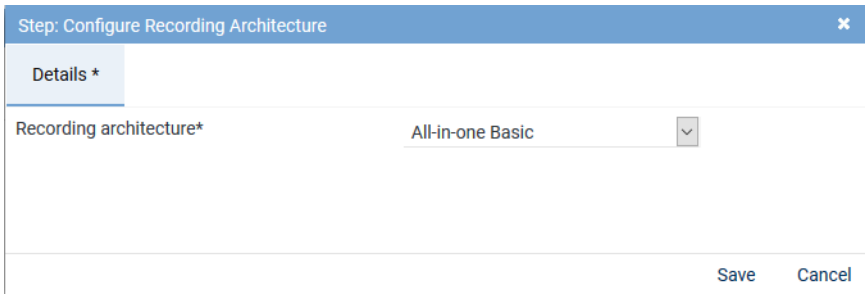


Fig. 60: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for All-in-one Basic

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.

   ⇨ The window *Step: Global Recording Settings* appears.

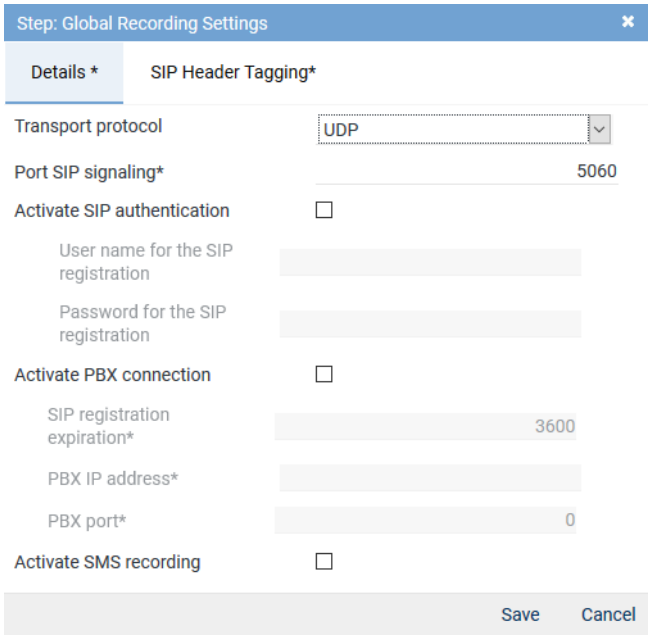


Fig. 61: Configuration step - Global Recording Settings - All-in-one Basic Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*

Parameter	Value/Description
Activate SIP authentication	Deactivate this option for this recording solution.
Activate PBX connection	Deactivate this check box for this recording solution.
Activate SMS recording	Activate the check box if you would like to use SMS recording.

Tab. 14: Global recording settings

3. To save the entries, click on the button *Save*.
   To discard entries, click on the button *Cancel*.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

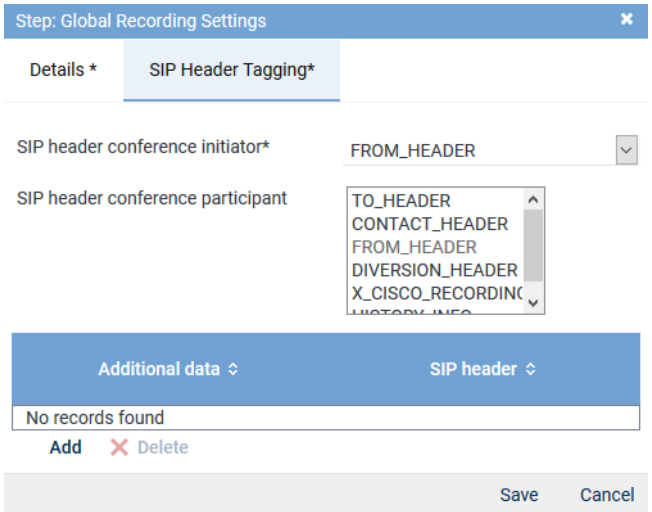


Fig. 62: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.
   ⇨ The window *SIP Additional Data* appears.

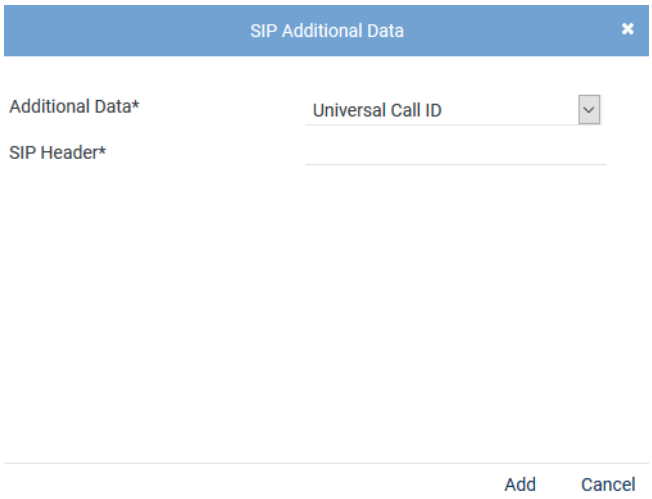


Fig. 63: SIP Additional Data

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted. To have ASC configure the mapping file, contact your distribution partner.

Tab. 15: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for All-in-one Basic

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

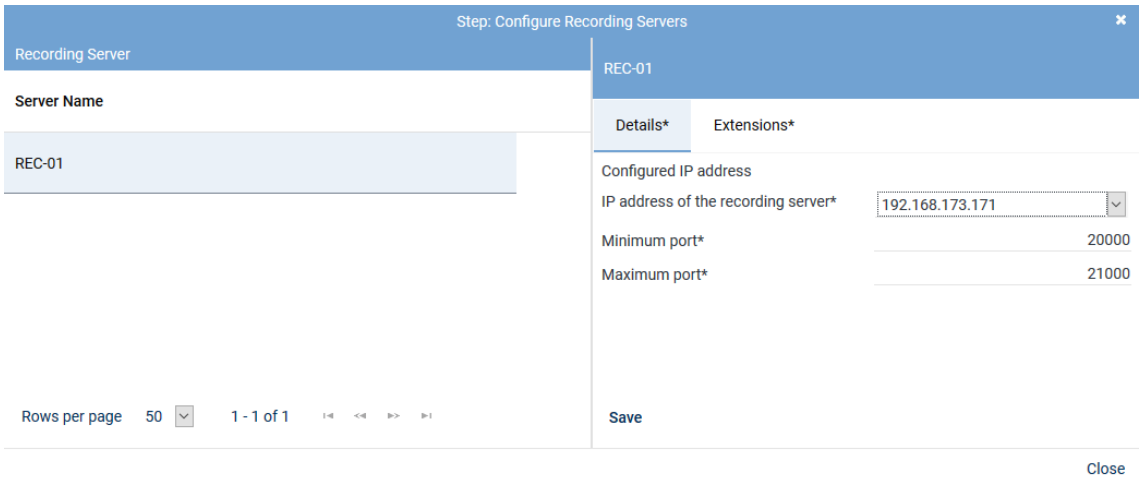


Fig. 64: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 16: Configure recording servers

For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.

In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Configure add-on

The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

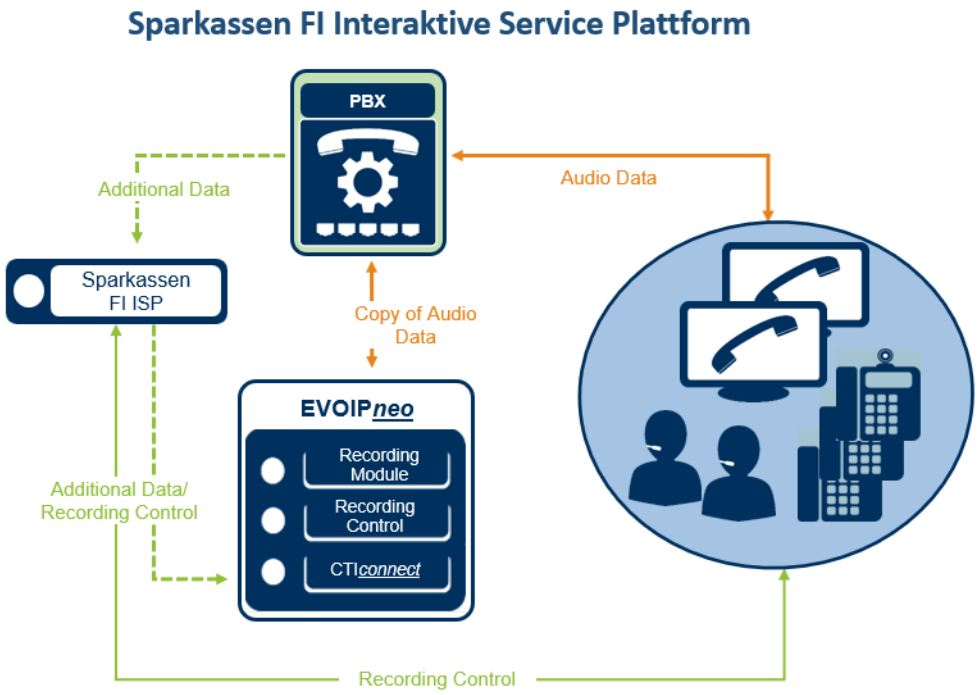


Fig. 65: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

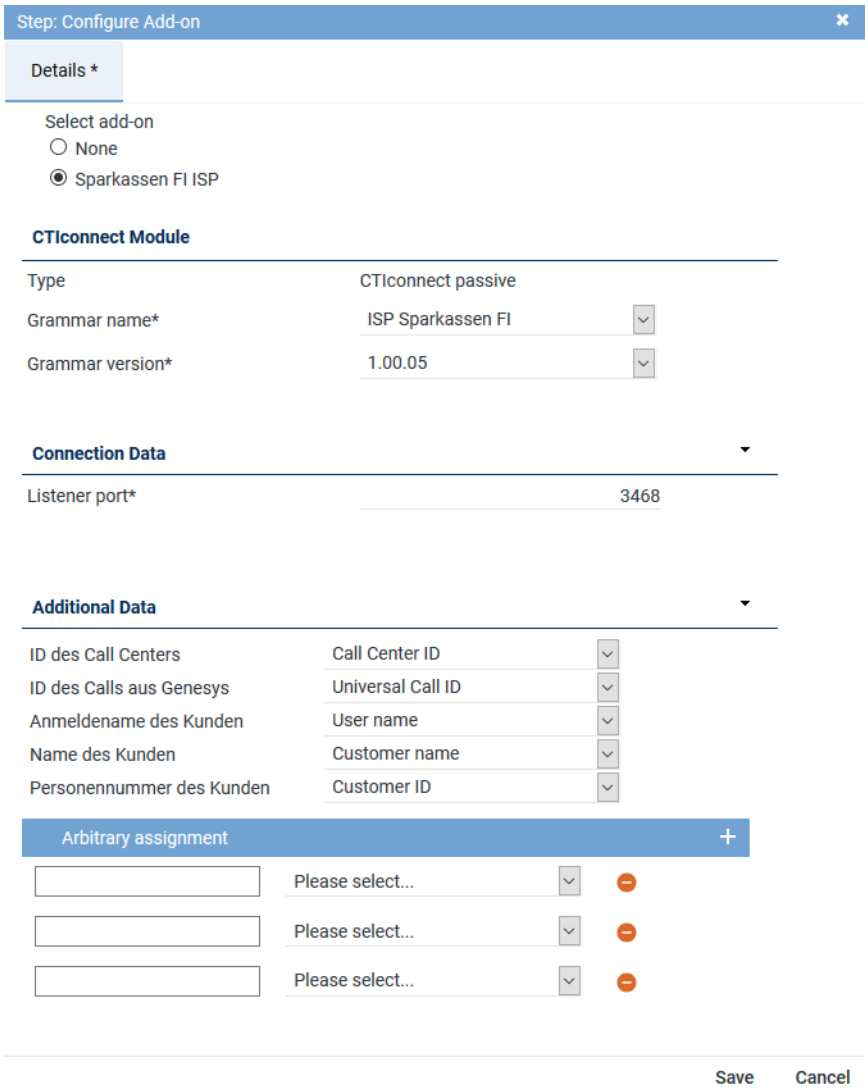


Fig. 66: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 17: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 54.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 18: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

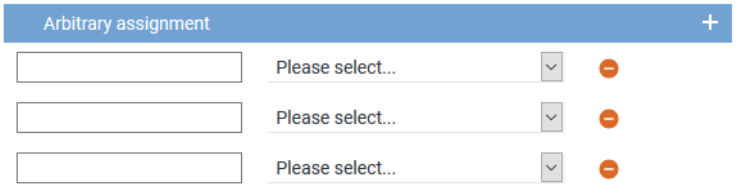


Fig. 67: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*

- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

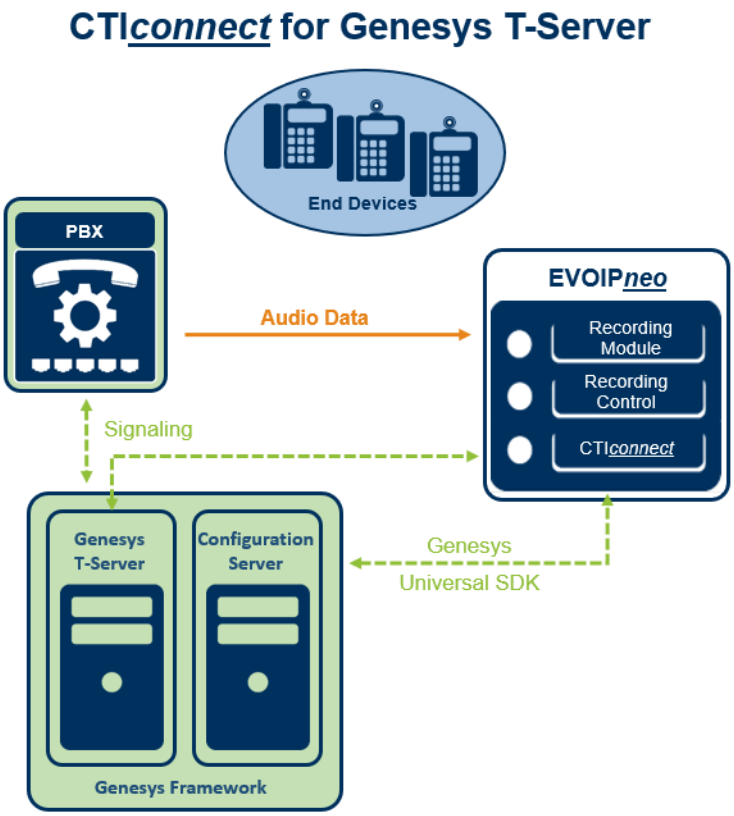


Fig. 68: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

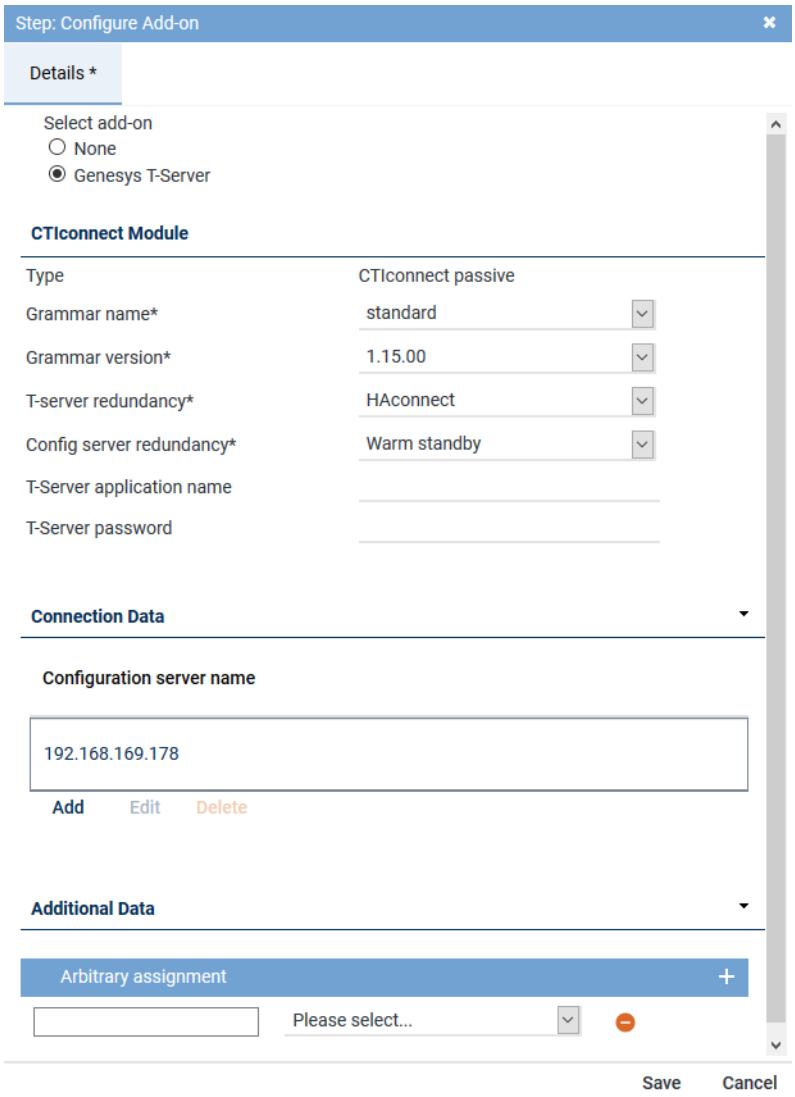


Fig. 69: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 19: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

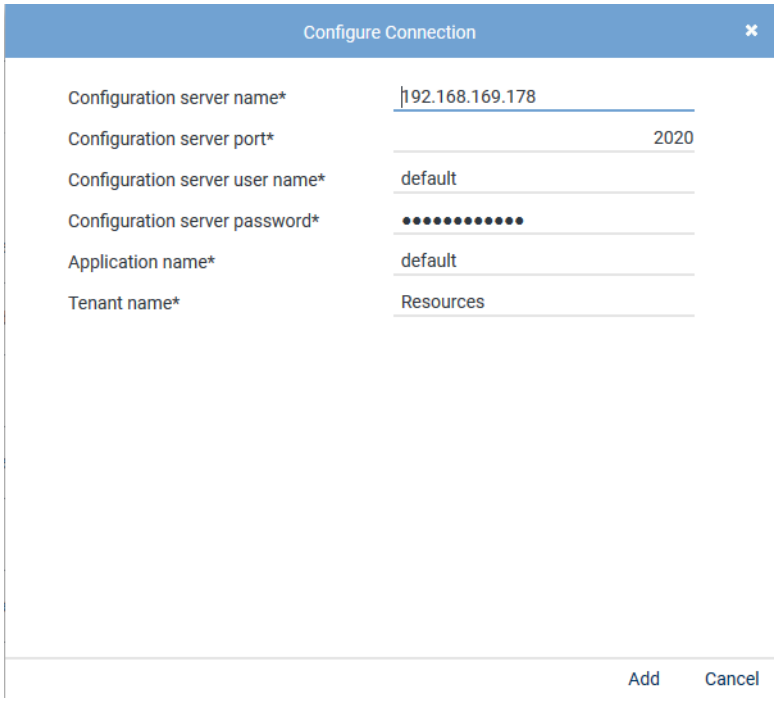


Fig. 70: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 20: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

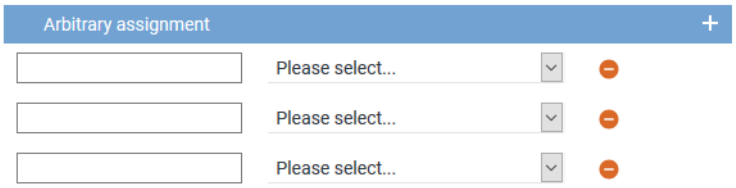


Fig. 71: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

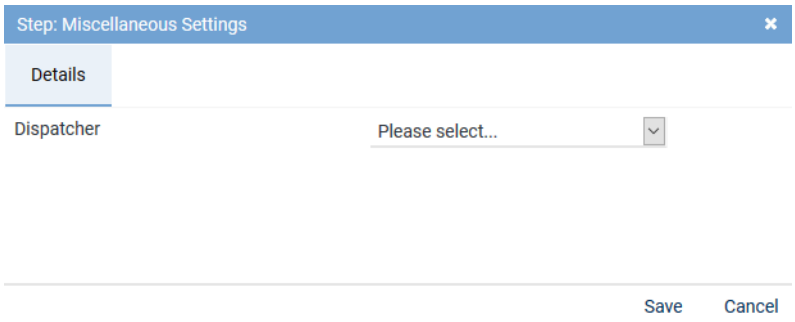


Fig. 72: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

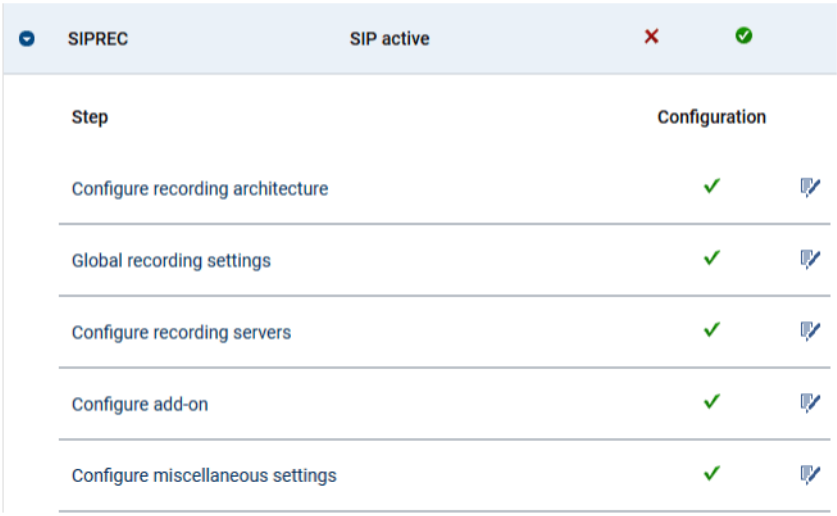


Fig. 73: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

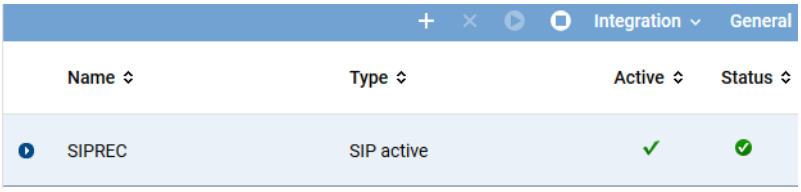


Fig. 74: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

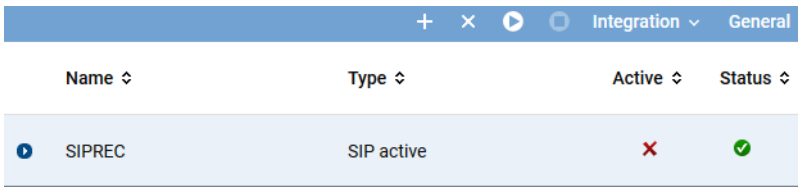


Fig. 75: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.2.2 Configure recording solution All-in-one Failover

7.1.2.2.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

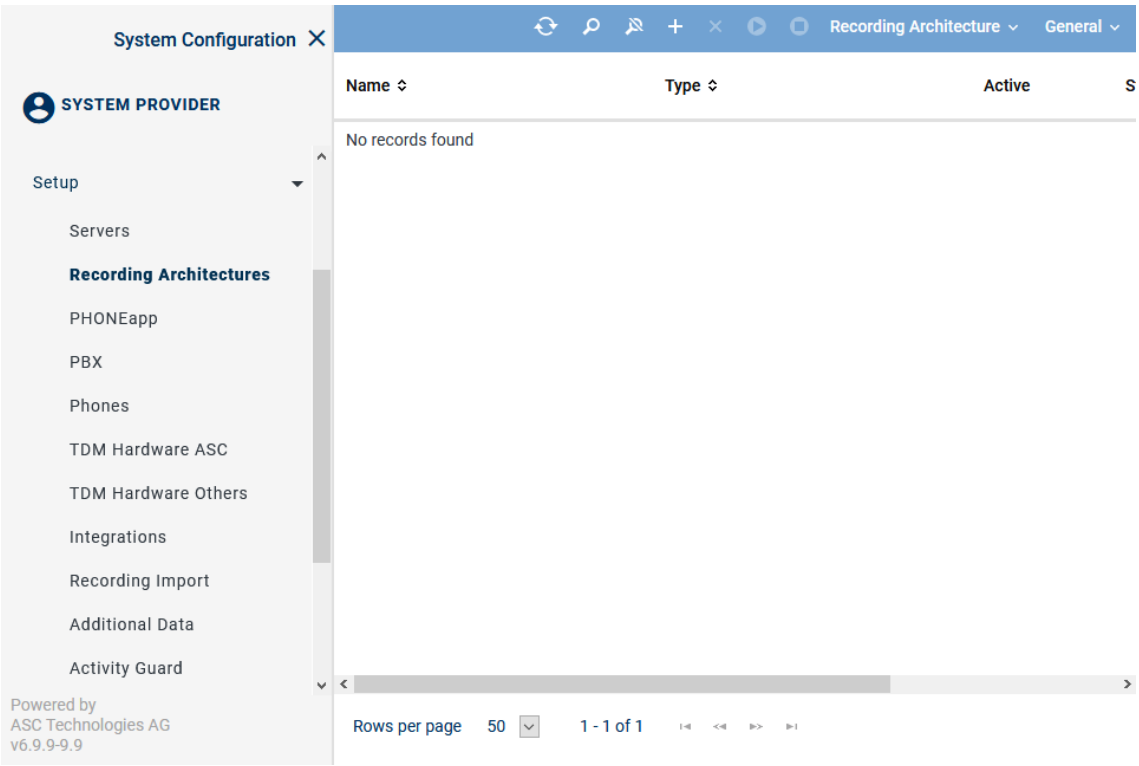


Fig. 76: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Recording Architectures module

The toolbar offers the following functions.

Fig. 77: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.

		The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Create	Creates a new recording architecture.
	Delete	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. **NOTICE!** You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	Activate	Activates the selected recording architecture.
	Deactivate	Deactivates the selected recording architecture. **NOTICE!** You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
Recording Architecture	*Standby Management*	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create recording architecture All-in-one Failover

If a standby recording server is supposed to take over recording in case of an error, you have to create a recording architecture of the type *All-in-one Failover*.

1. To create a new recording architecture, click on the icon *(Create)* in the toolbar of the main view.
   ⇨ The window *New Recording Architecture* appears.

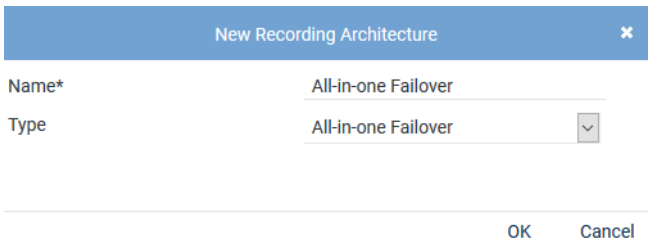


Fig. 78: Create recording architecture - All-in-one Failover

2. In the entry field *Name*, enter a descriptive name for the recording architecture.

3. From the drop-down list *Type*, select the recording architecture type *All-in-one Failover*.
   NOTICE! The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.
   ⇨ Your entries now appear in the detail view.

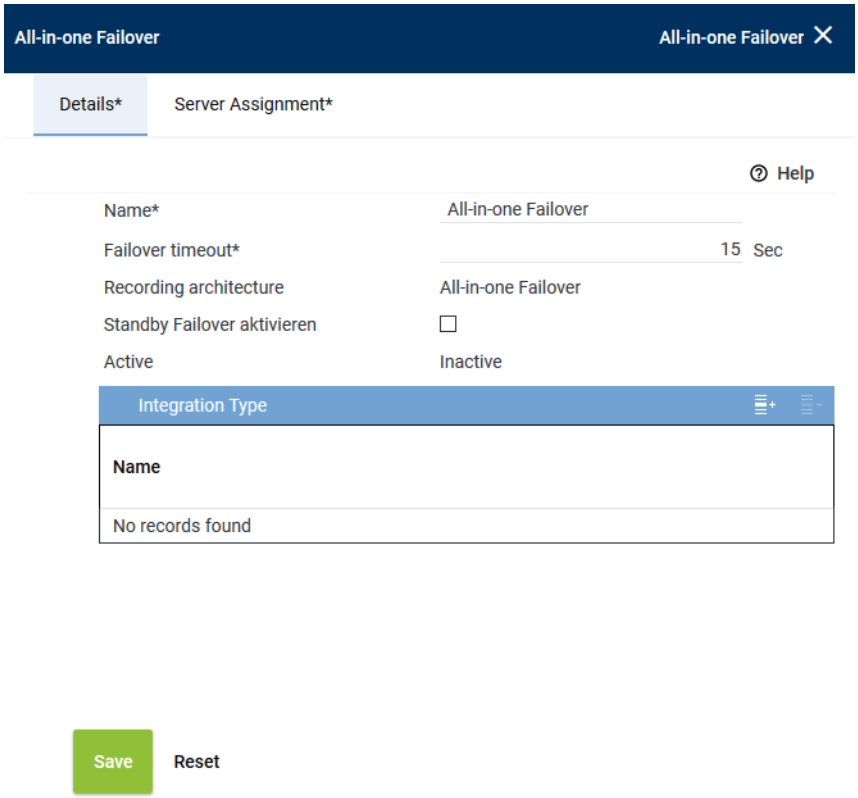


Fig. 79: Recording architecture - tab Details - All-in-one Failover

As standby components may have been configured for the active recording server, a failover timeout may be configured in this recording architecture. For further information about failover architectures, see chapter "Standby management for failover architectures", p. 373.

Failover timeout	Enter a timeout of a minimum of 15 seconds after which the failover process is supposed to start. Depending on the system architecture it may make sense to configure a longer timeout period. The timeout defines the elapse time until the failover process starts. If the status returns to *OK* within this time, then the failover process is not triggered. **NOTICE!** Check these parameters after an update and set the timeout to 15 seconds, if required.
Activate standby failover	Activate this option if you would like to ensure that the system switches back to the primary server in case of an error of the standby server. **NOTICE!** There is no check whether the primary database is working properly before switching back. As a result it is possible that both databases are in an undefined state. **NOTICE!** After switching back to the original primary server from the standby server, this option is deactivated. If the switching process is supposed to be carried out automatically in the event of a new error, you must activate this option again.
Active	Shows the status of the recording architecture.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 80: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for All-in-one Failover Recording

1. Click on the tab *Server Assignment* to assign the recording servers to the recording architecture *All-in-one Failover Recording*.

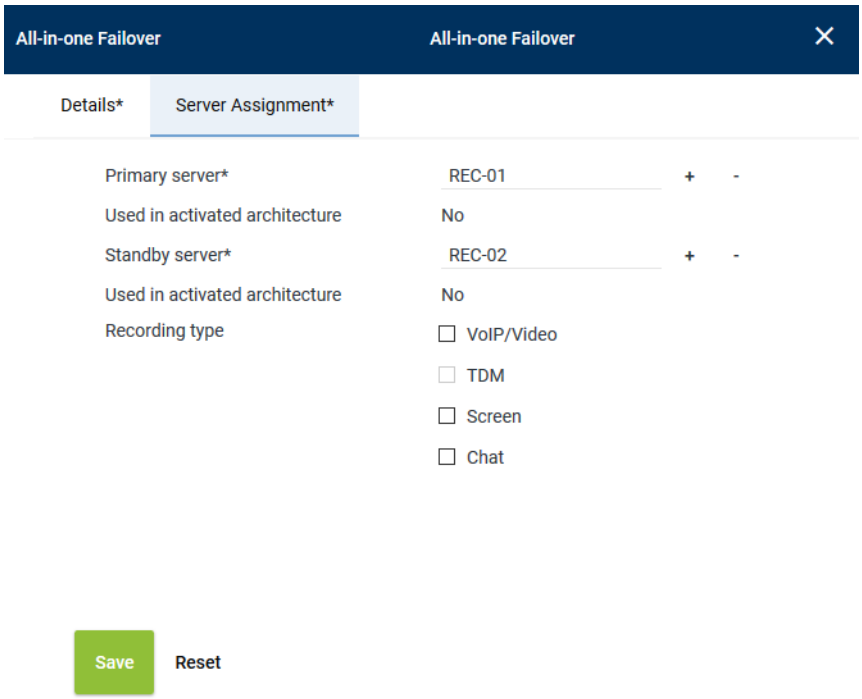


Fig. 81: Recording Architecture - tab Server Assignment

2. Click on the button + behind the entry field *Primary server*.
   ⇨ The window *Servers* appears.

Fig. 82: Recording Architecture - assign server - example

3. Select the *primary server*.

ⓘ A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

4. Click on the button *Add*.
   ⇨ The name of the server now appears in the detail view.

5. To delete an assignment, click on the button .
6. Repeat the steps and select the server which is supposed to be use in case of an error failover operation in the entry field *Standby server*.
7. Select the recording type you would like to use for these servers by activating the check box.

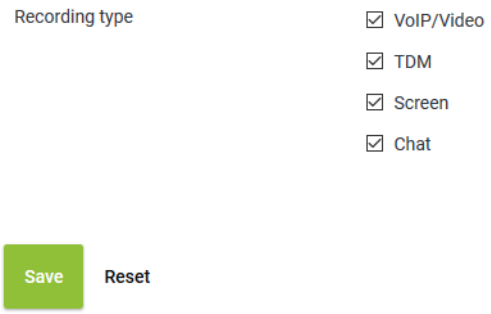


Fig. 83: Recording Architecture - activate recording type

You can activate several recording types if the integration has been designed for this and if you have installed the respective licenses.

8. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the toolbar becomes active.
3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

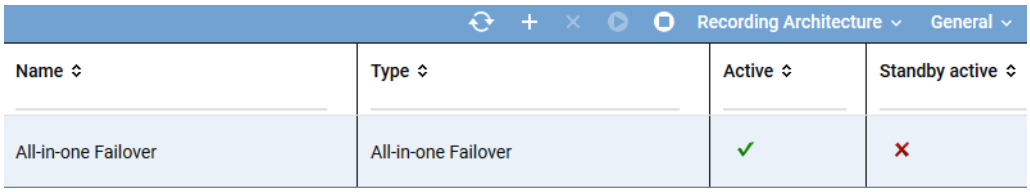


Fig. 84: Recording architecture - activate recording architecture

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✗ *(Inactive)* appears.

The recording architecture must have been activated so that the integration can be configured.

For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See chapter "Standby management for failover architectures", p. 373.

If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.2.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

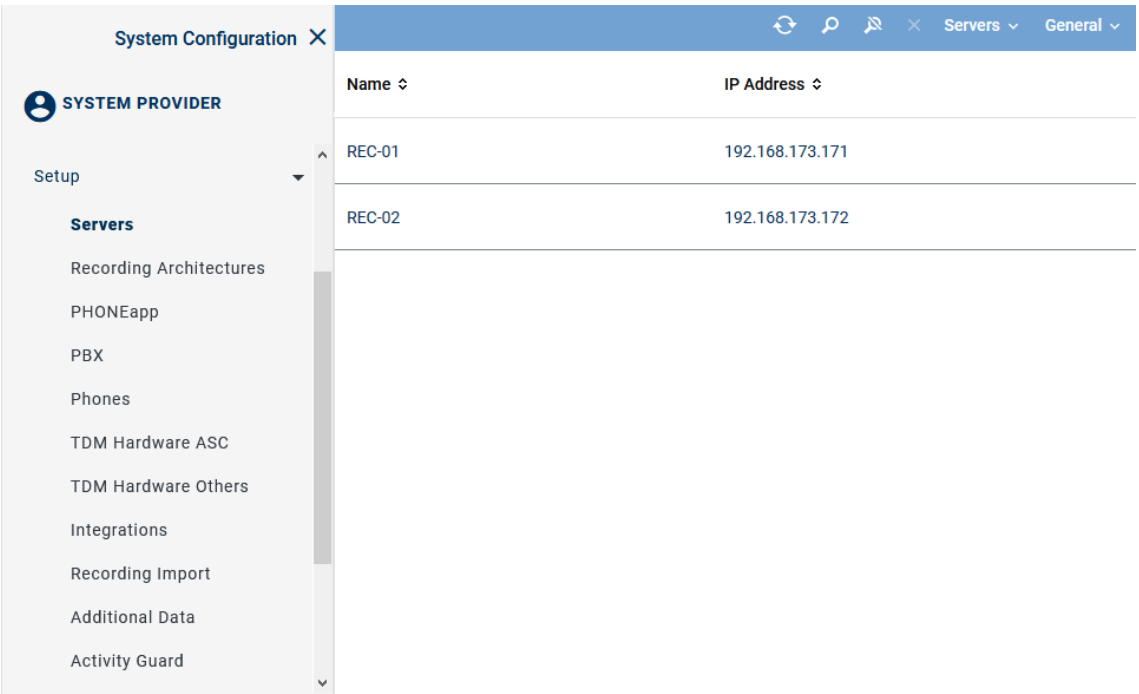


Fig. 85: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.
Path	Shows the path of the server.
Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 86: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.

	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.
Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 79.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.

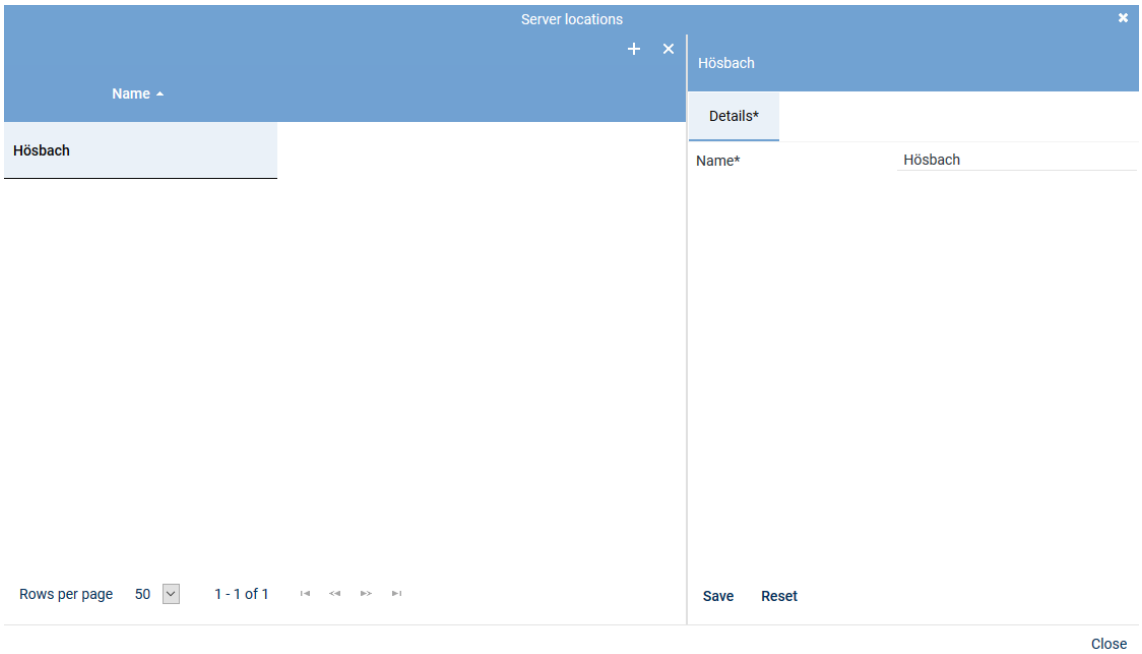


Fig. 87: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

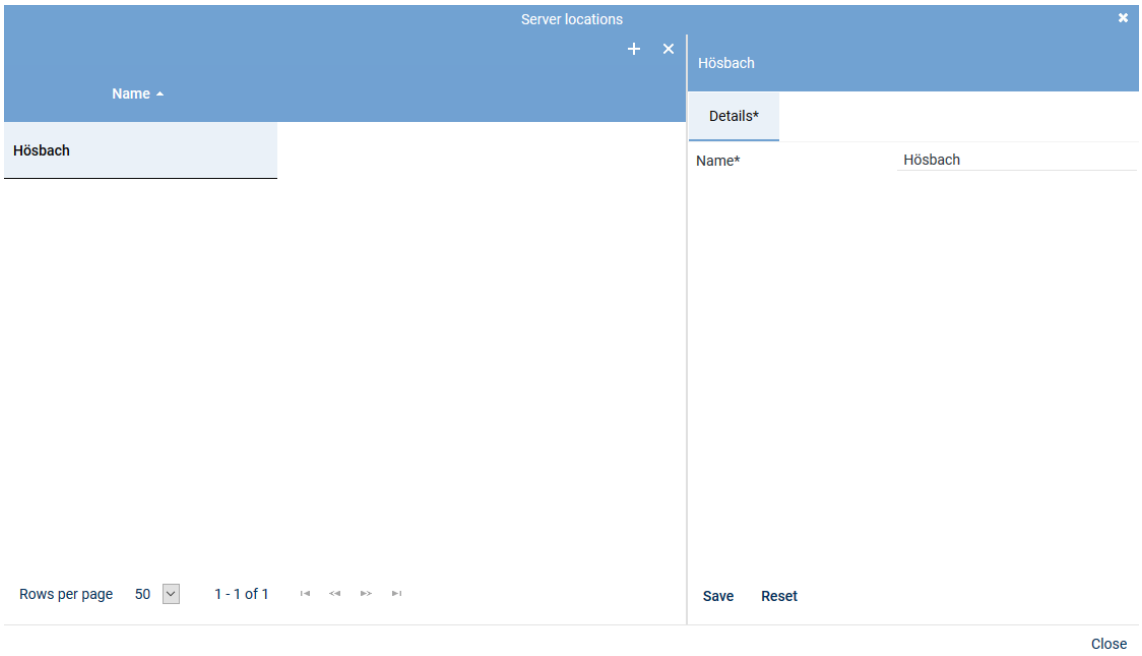


Fig. 88: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

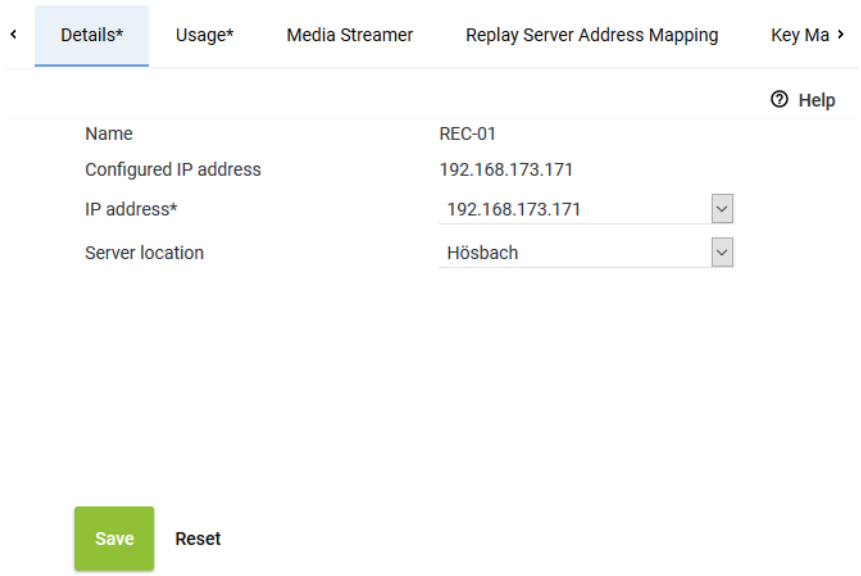


Fig. 89: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.

4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

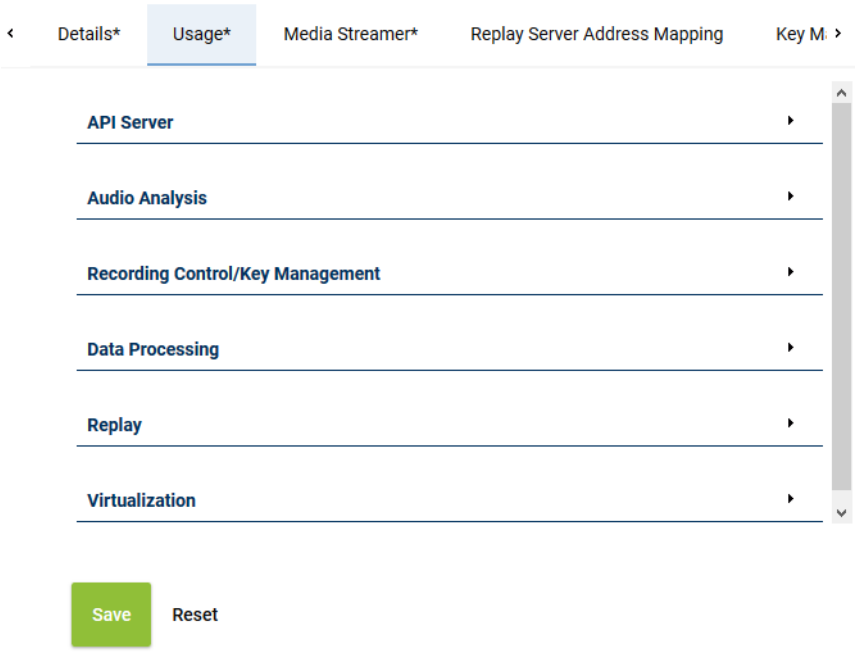


Fig. 90: Servers - tab usage

Group field API Server

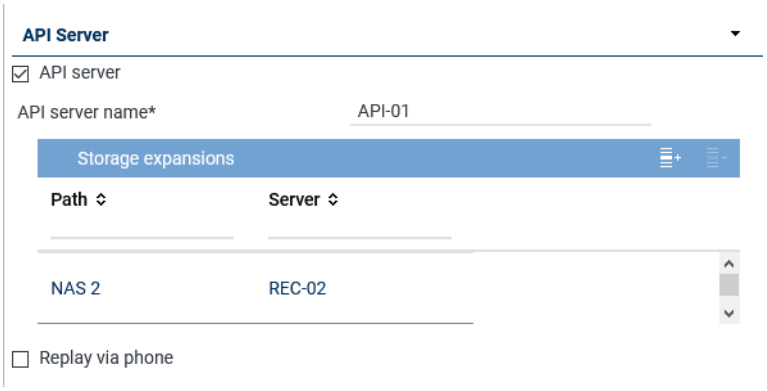


Fig. 91: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server.

Parameter	Value/Description
	☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 93.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List *Storage expansions*	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 84. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list. If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 91. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

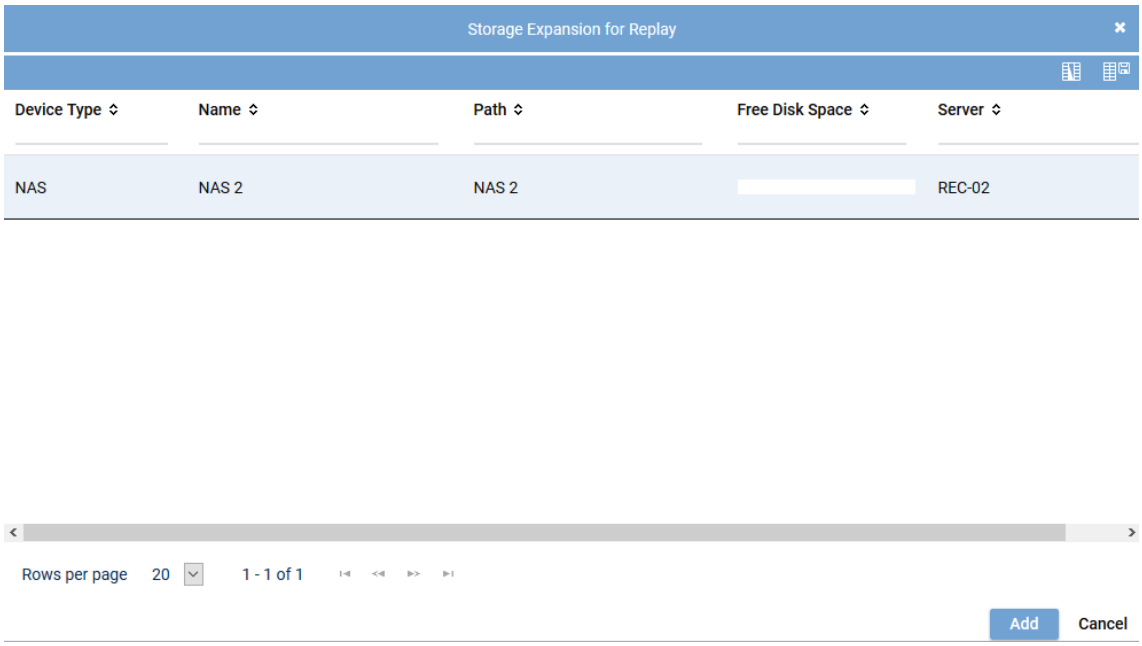


Fig. 92: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

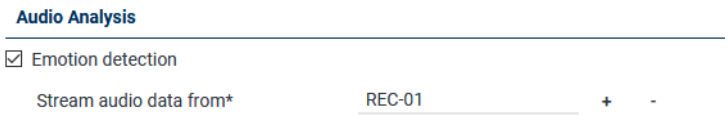


Fig. 93: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 21: Configure audio analysis

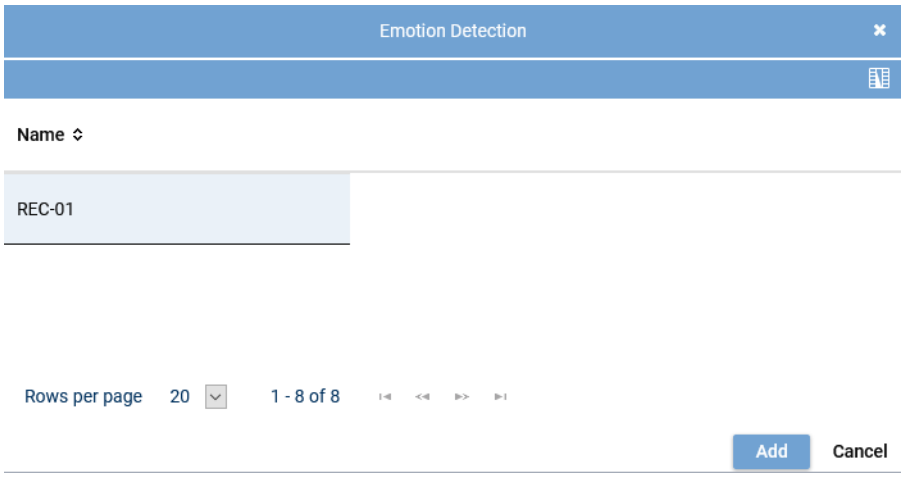


Fig. 94: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

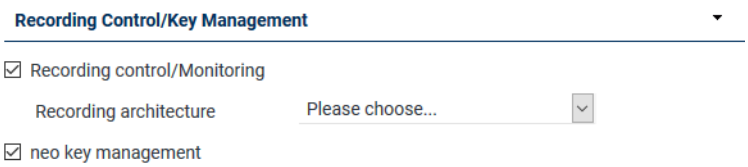


Fig. 95: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 22: Configure recording control/key management

Group field Data Processing

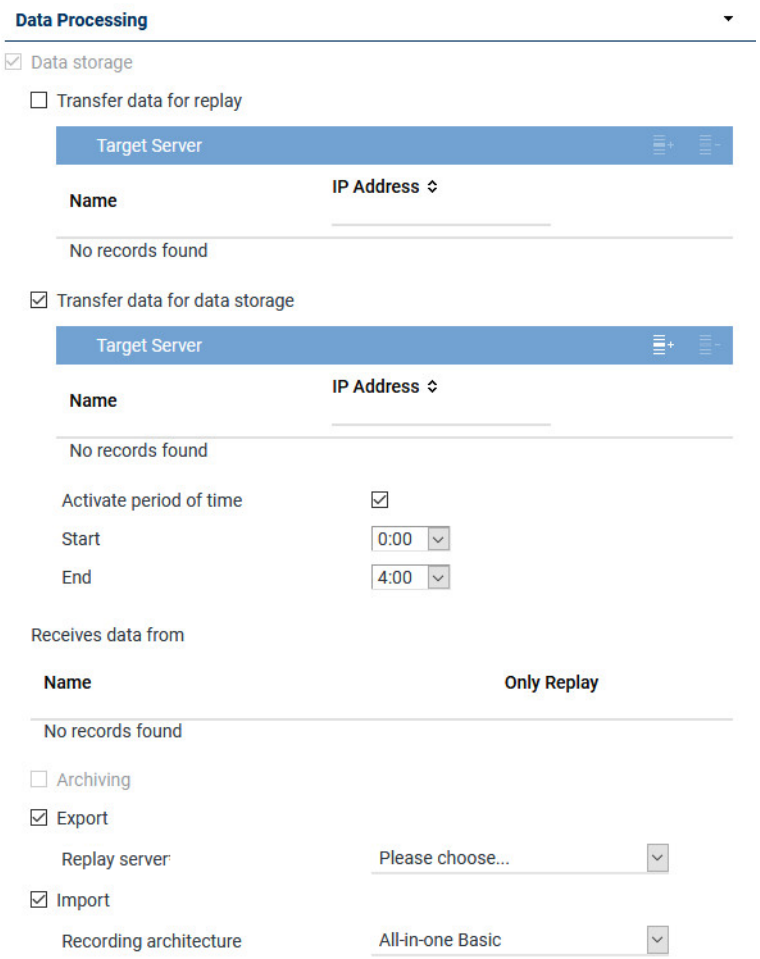


Fig. 96: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 88. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be trans-

Parameter	Value/Description
	ferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 88. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.

Parameter	Value/Description
	NOTICE! If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 23: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 97: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

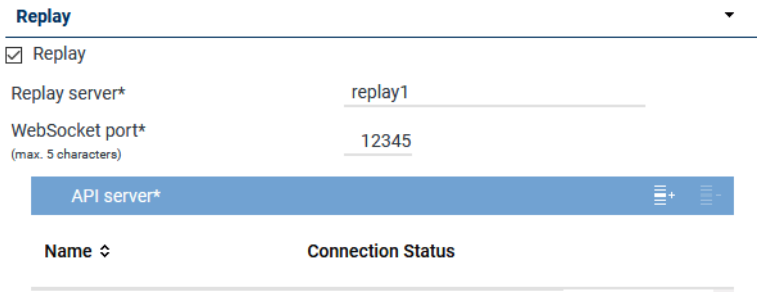


Fig. 98: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 89. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 24: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.

- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

Fig. 99: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 82.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 100: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management.

Parameter	Value/Description
	• *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 25: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

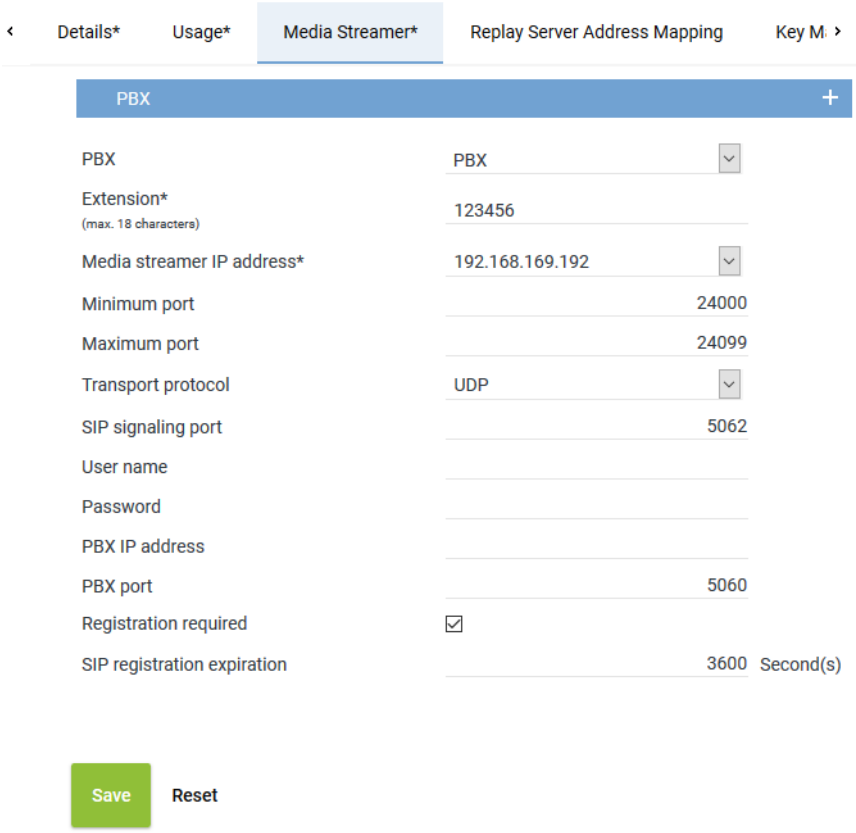


Fig. 101: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.

	If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 97.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number. A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

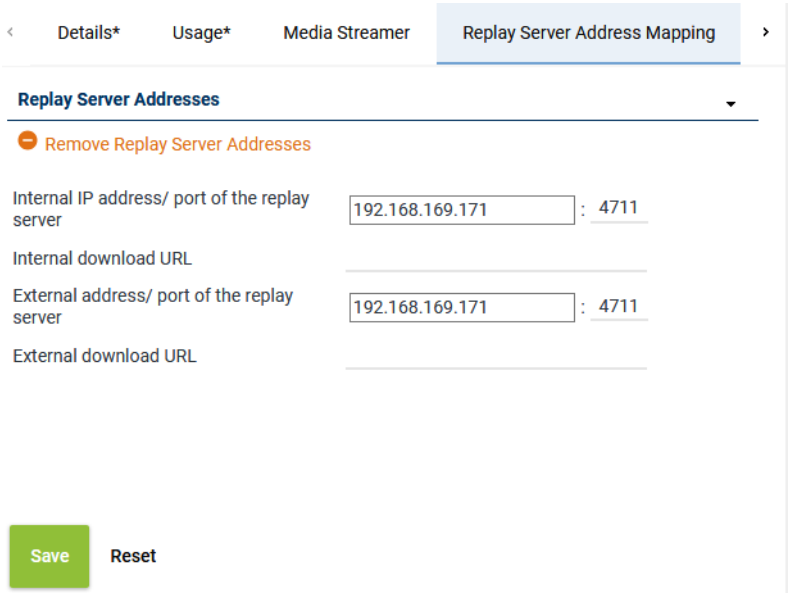


Fig. 102: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

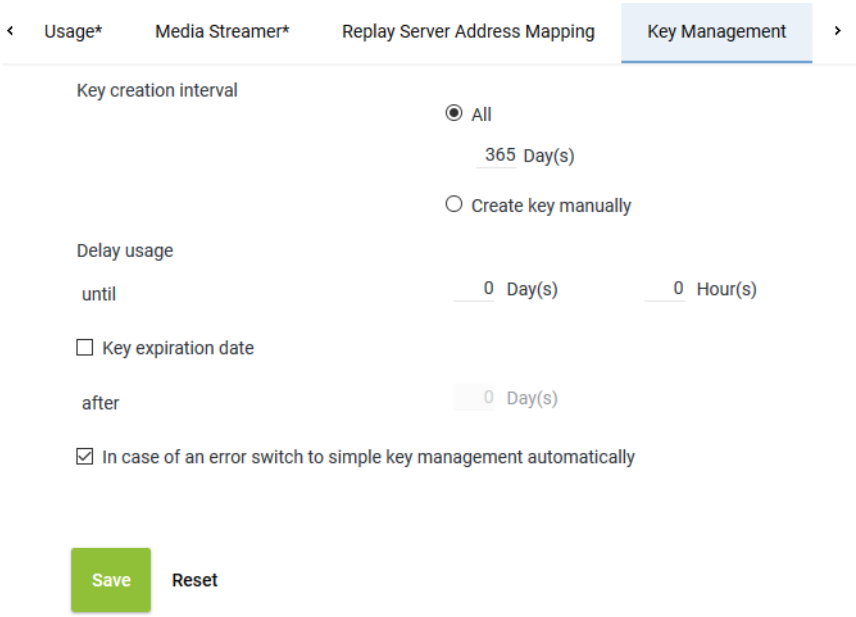


Fig. 103: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.

Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid. ☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

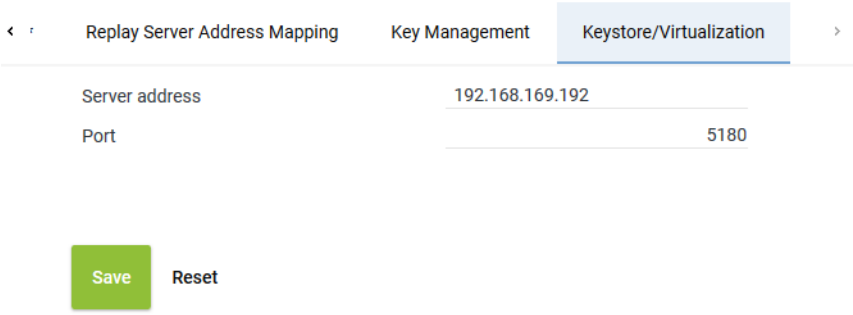


Fig. 104: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management:

	IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.2.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

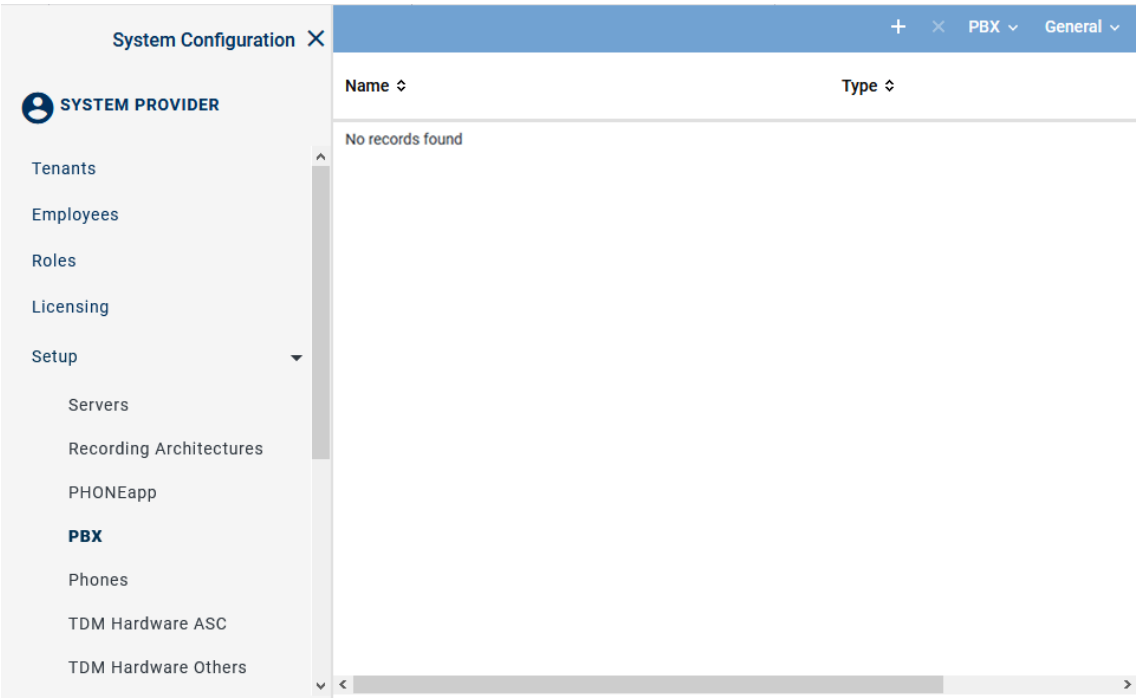


Fig. 105: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 106: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.

PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

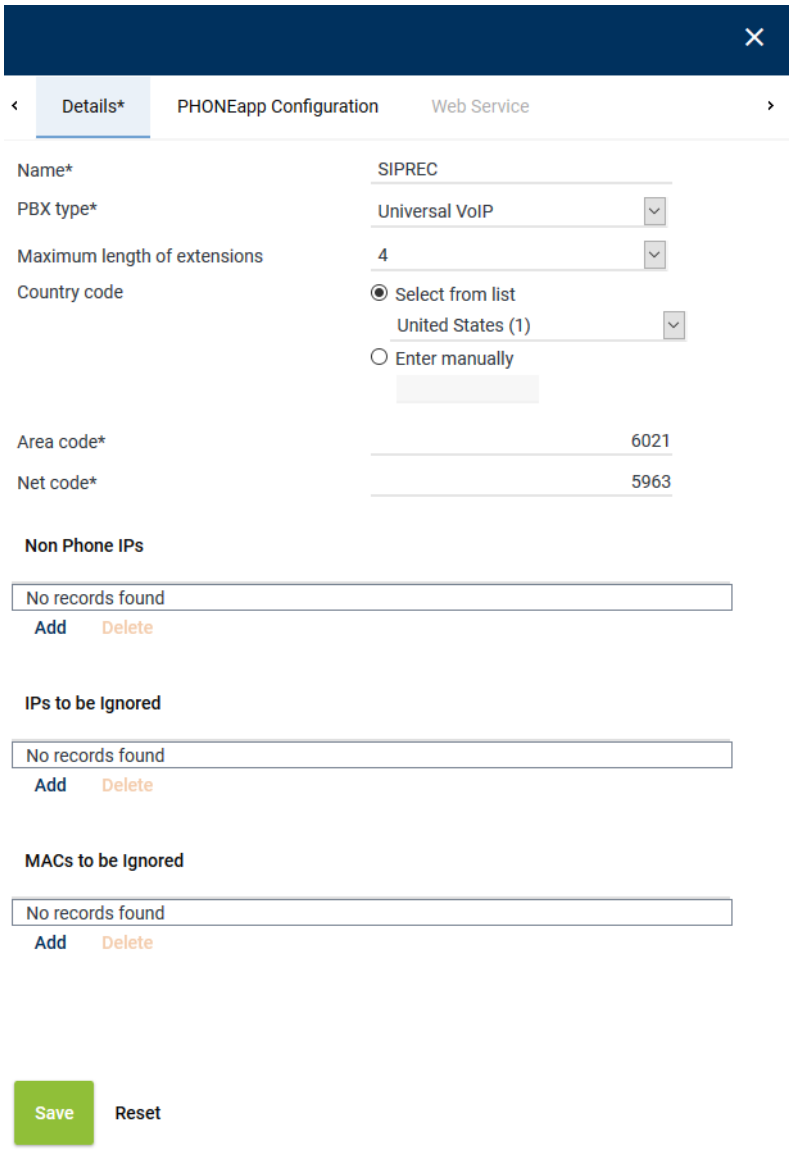


Fig. 107: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list* Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 26: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 27: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.2.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

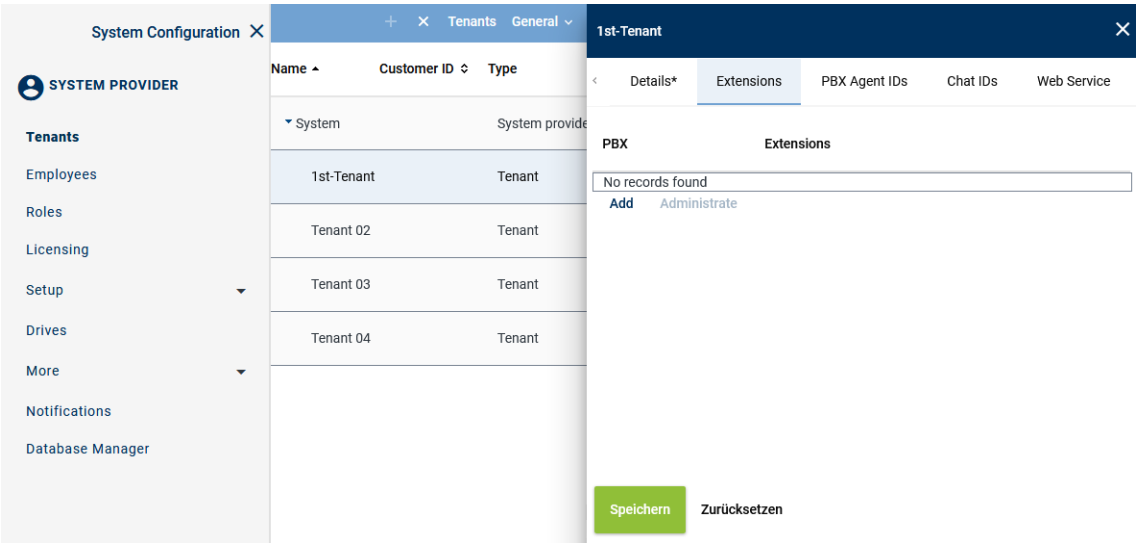


Fig. 108: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.

⇨ The following window appears:

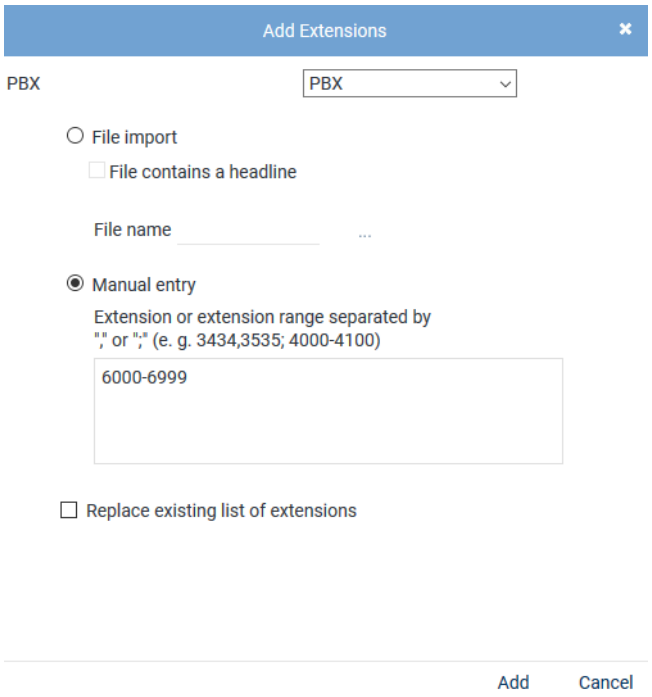


Fig. 109: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT* • *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually.

	To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

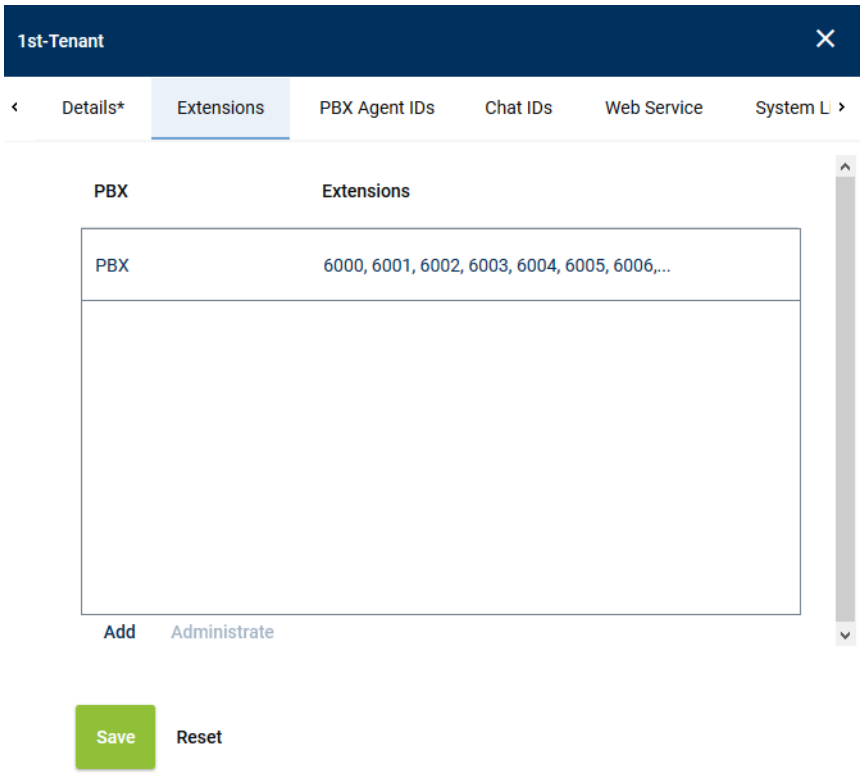


Fig. 110: Remove extensions

2. Click the button *Administrate*.

3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 111: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

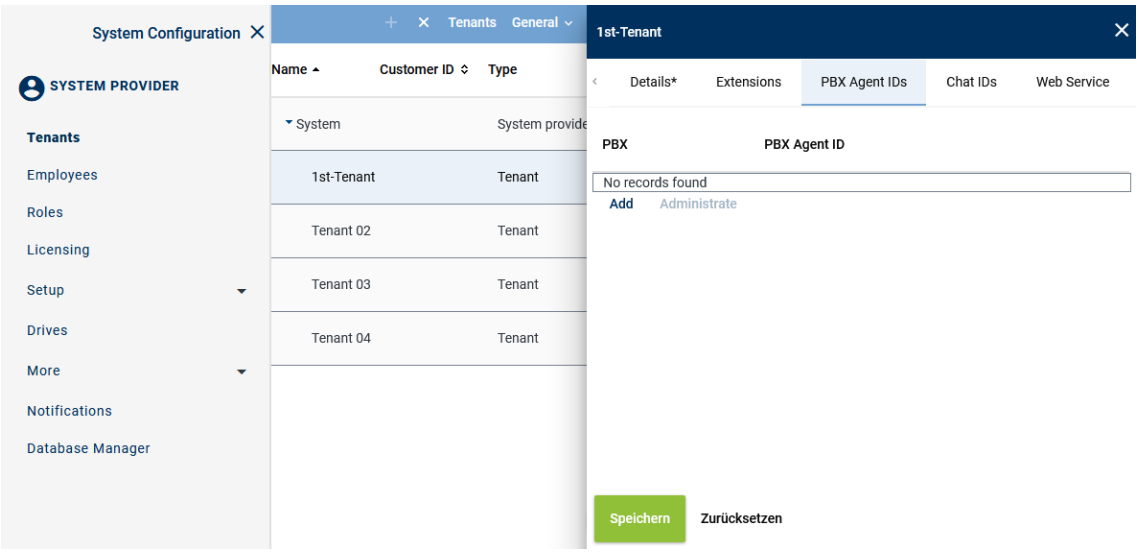


Fig. 112: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

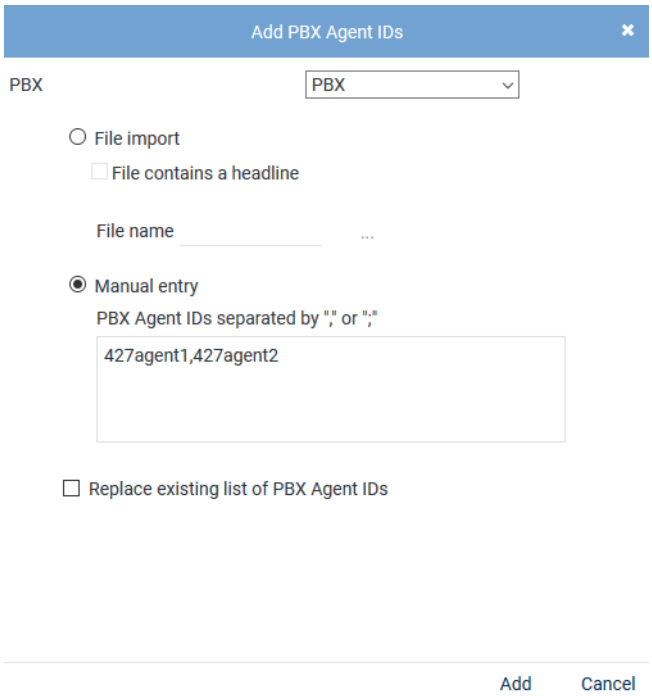


Fig. 113: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline

	Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

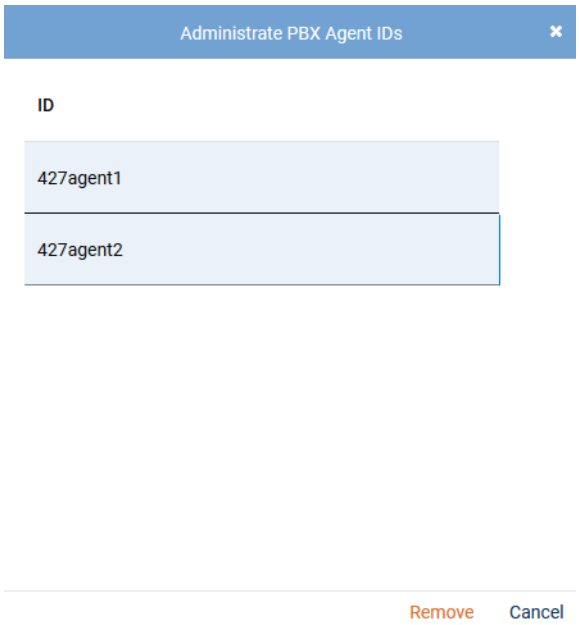


Fig. 114: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.2.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

> In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

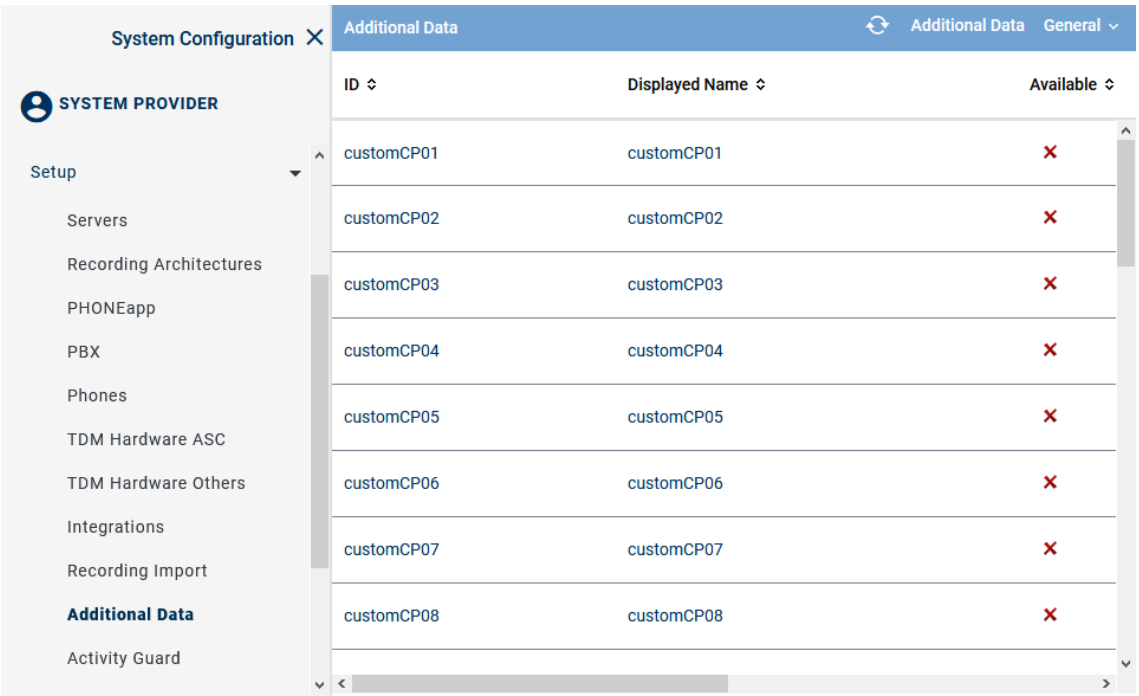


Fig. 115: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

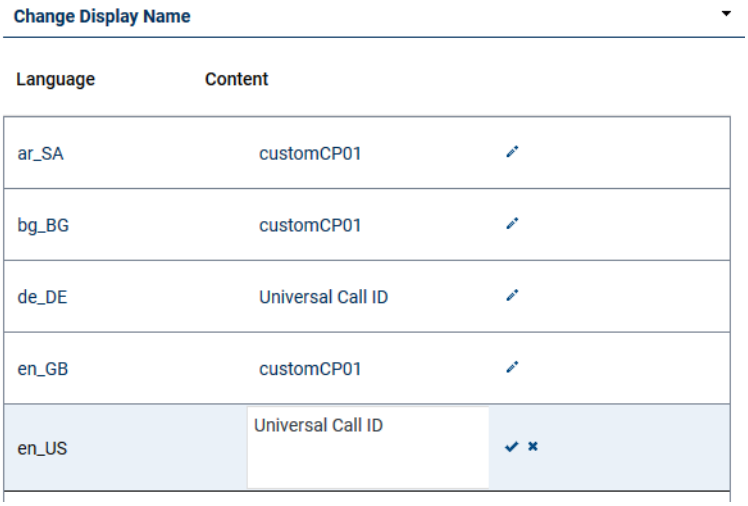


Fig. 116: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 117: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.2.6 Create integration for All-in-one Failover

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

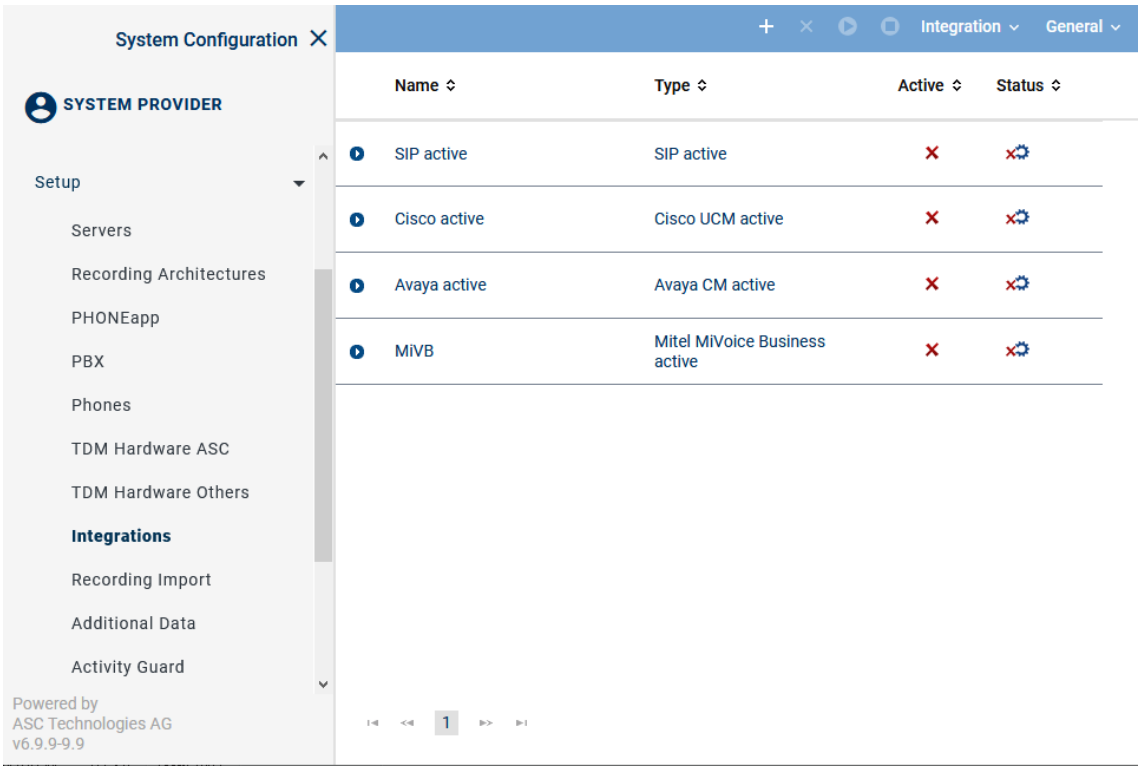


Fig. 118: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 119: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

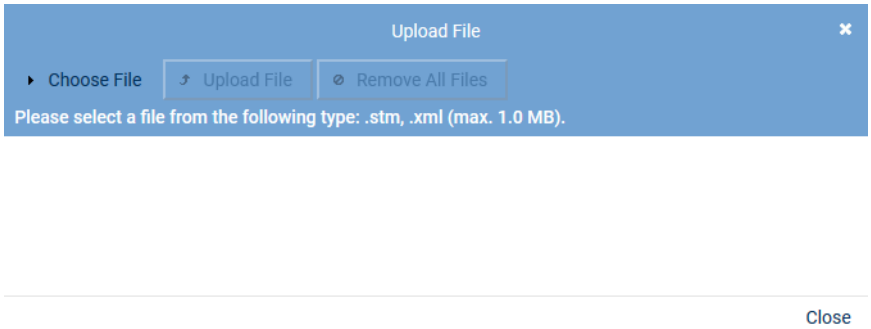


Fig. 120: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

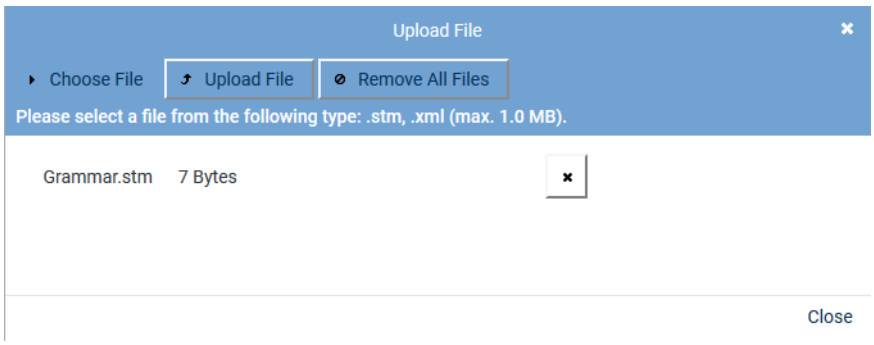


Fig. 121: Upload grammar

5. To remove a selected file from the list, click on the button × *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 122: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 28: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 123: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for All-in-one Failover

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

Fig. 124: Assign recording architecture - All-in-one Failover

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

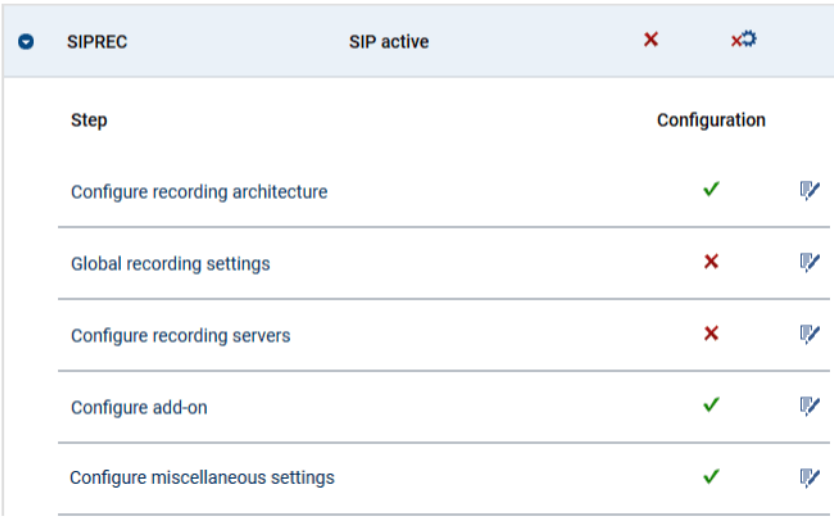


Fig. 125: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

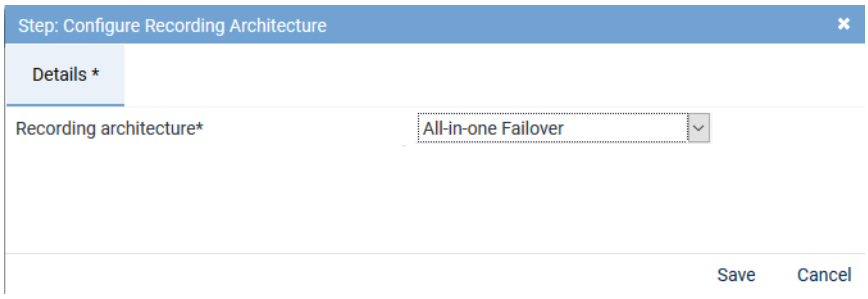


Fig. 126: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for All-in-one Failover

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.

   ⇨ The window *Step: Global Recording Settings* appears.

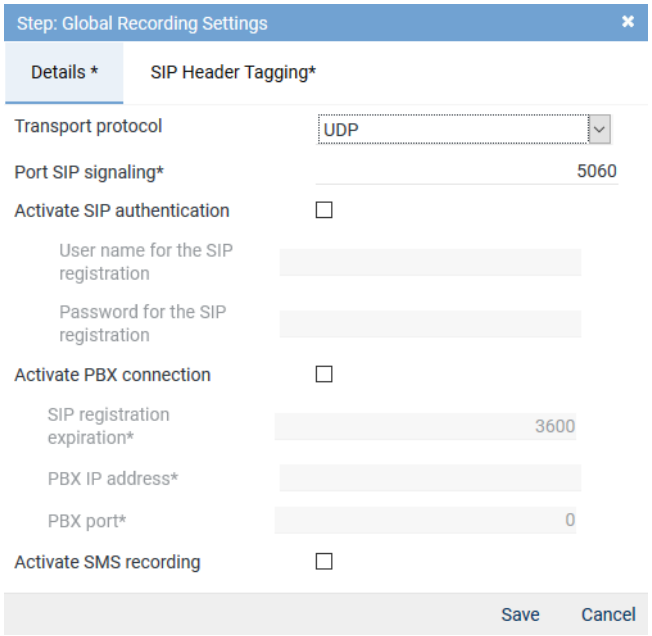


Fig. 127: Configuration step - Global Recording Settings - All-in-one Basic Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*

Parameter	Value/Description
Activate SIP authentication	Deactivate this option for this recording solution.
Activate PBX connection	Deactivate this check box for this recording solution.
Activate SMS recording	Activate the check box if you would like to use SMS recording.

Tab. 29: Global recording settings

3. Click on the button *Save*.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

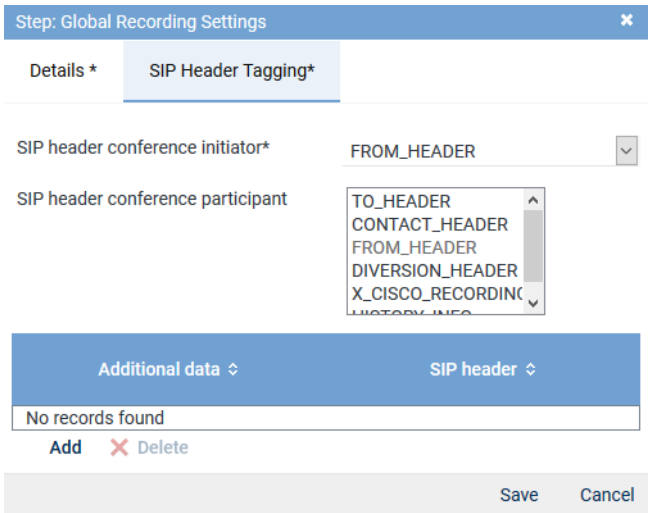


Fig. 128: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.
   ⇨ The window *SIP Additional Data* appears.

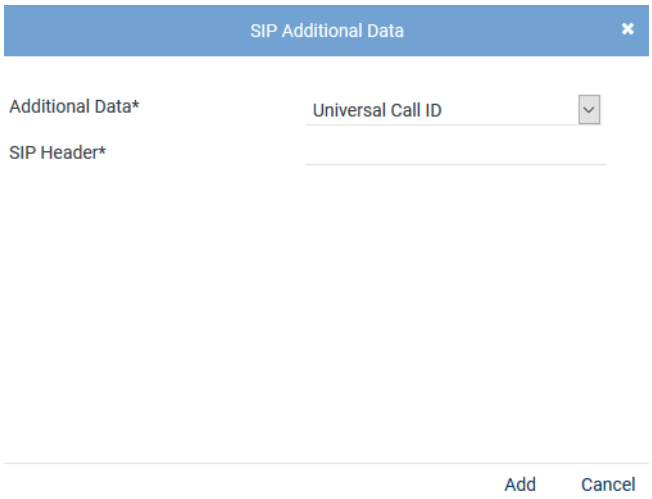


Fig. 129: SIP Additional Data

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted. To have ASC configure the mapping file, contact your distribution partner.

Tab. 30: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for All-in-one Failover

To guarantee that switching servers in case of failover runs smoothly, you must configure a port range for both recording servers. The range may be the same for both recording servers. Make sure, though, that the port range lies within the range of ports activated in the firewall, refer to the installation manual Installation requirements in chapter Communication matrix.

This configuration takes place in the configuration step *Configure recording servers*.

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

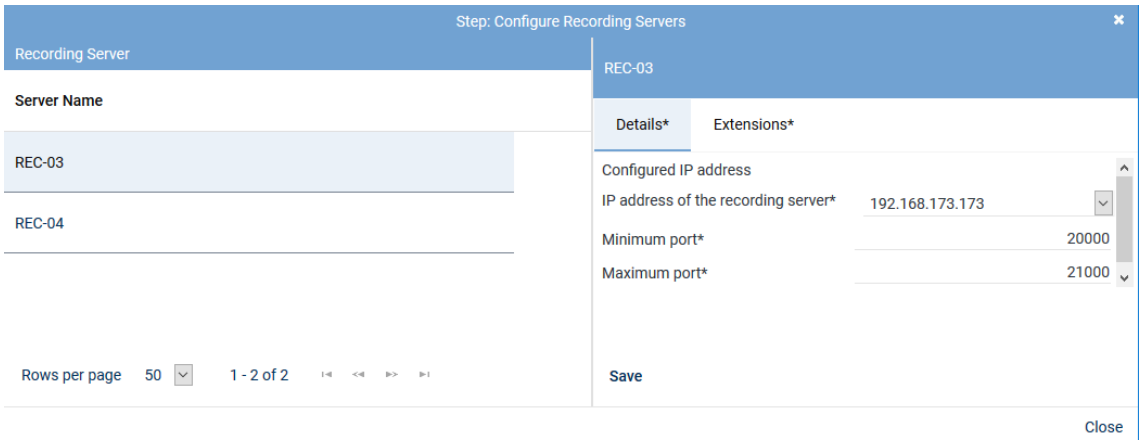


Fig. 130: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 31: Configure recording servers

For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.

In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Tab Extensions

1. Click on the tab *Extensions*.

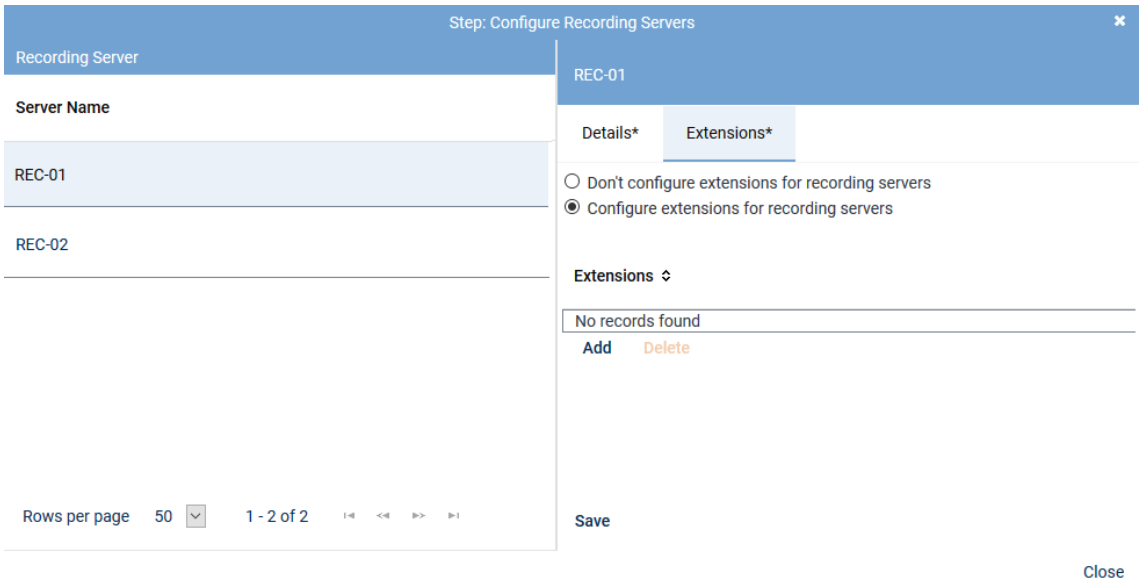


Fig. 131: Tab Extensions

The following options are available:

Configure no extensions for recording servers	Activate this option if you have not configured the extensions for the recording server in the PBX.
Configure extensions of the recording server	Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

2. To add extensions, click on the button *Add* in the table *Extensions*.
   ⇨ The window *Add Extensions* appears.

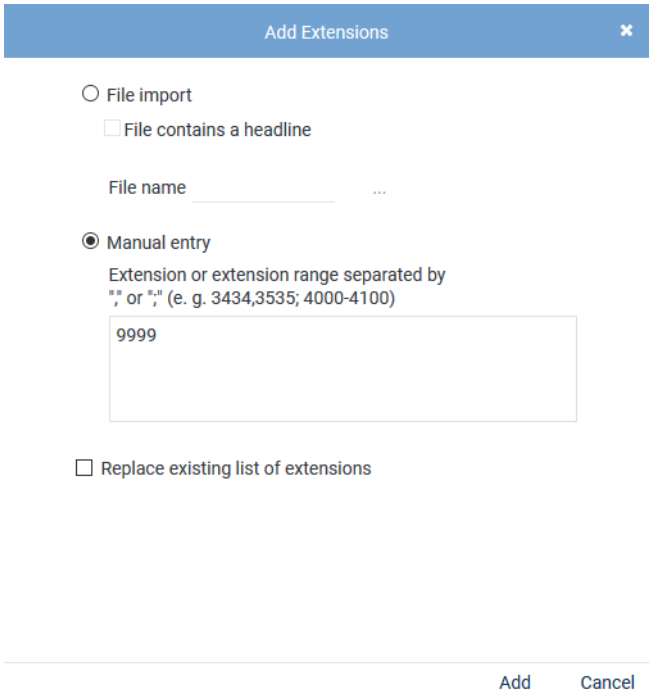


Fig. 132: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.

5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

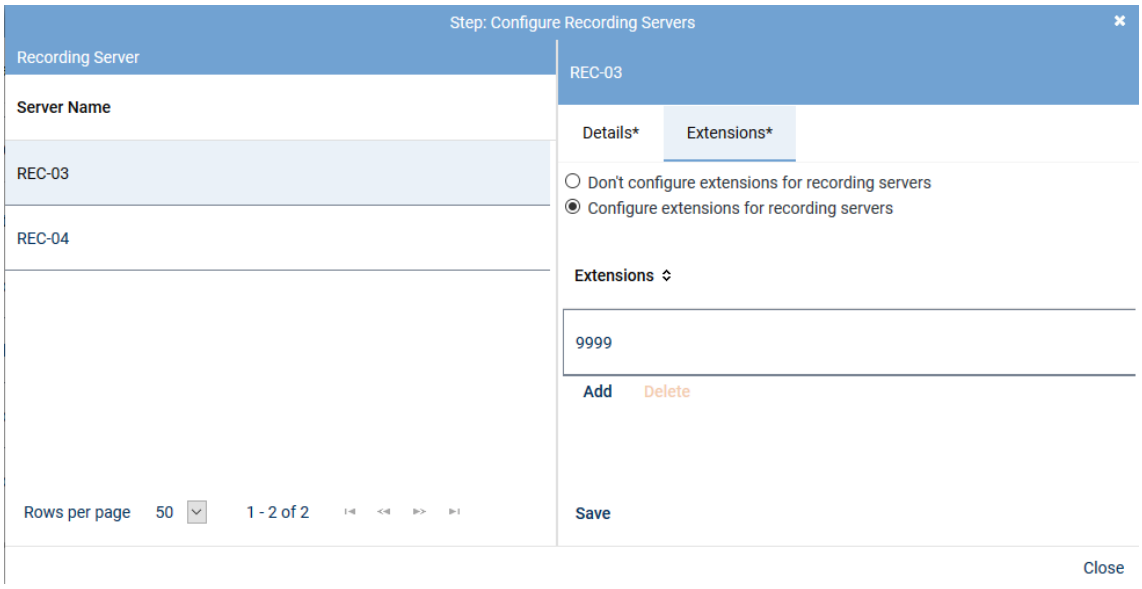


Fig. 133: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.
8. Click on the button *Save*.
9. Click on the button *Close* to finish this configuration step.

Configure add-on

ⓘ The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

ⓘ The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

ⓘ Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

ⓘ The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

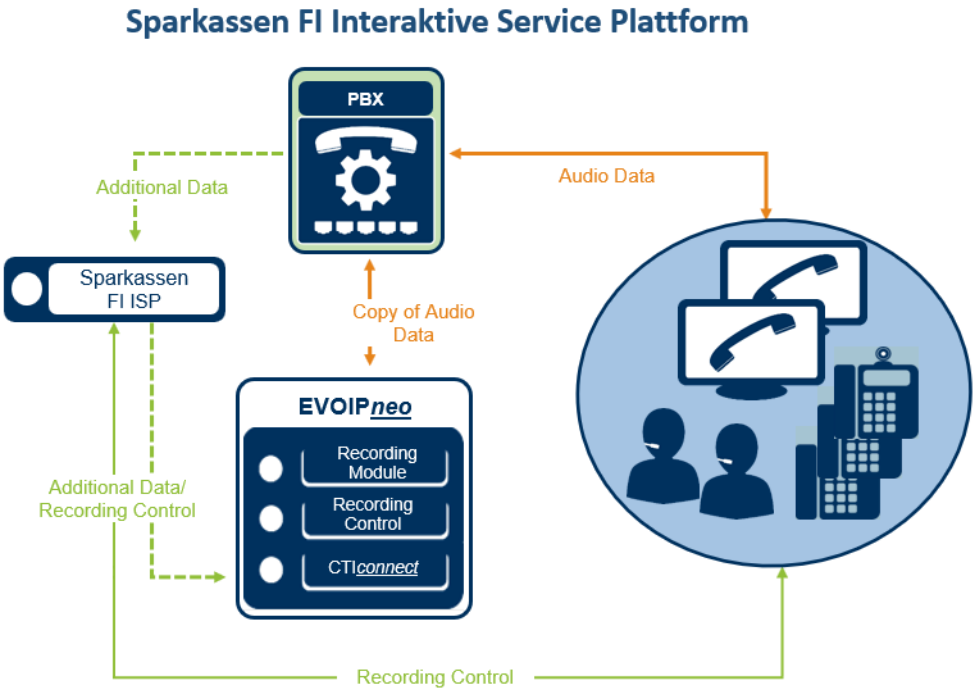


Fig. 134: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

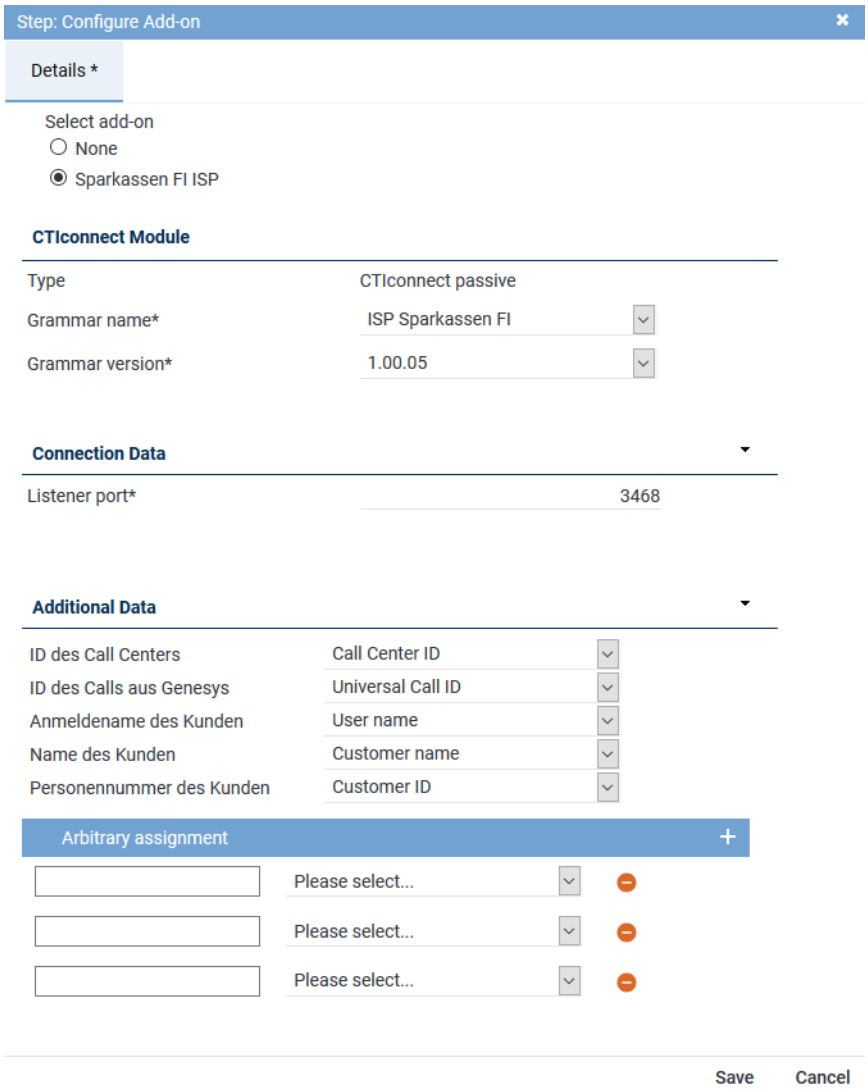


Fig. 135: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 32: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 110.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 33: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

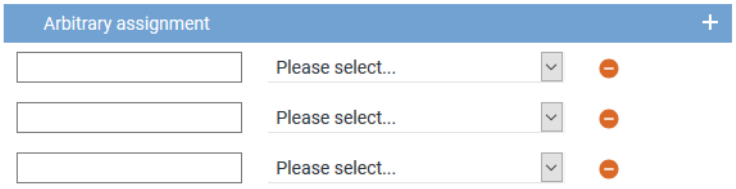


Fig. 136: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*

- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

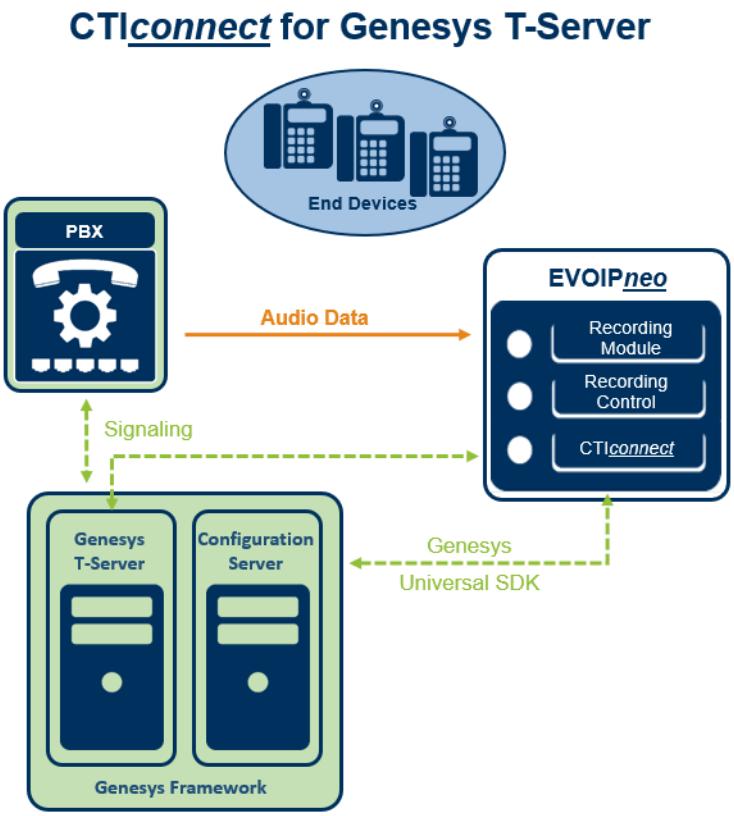


Fig. 137: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

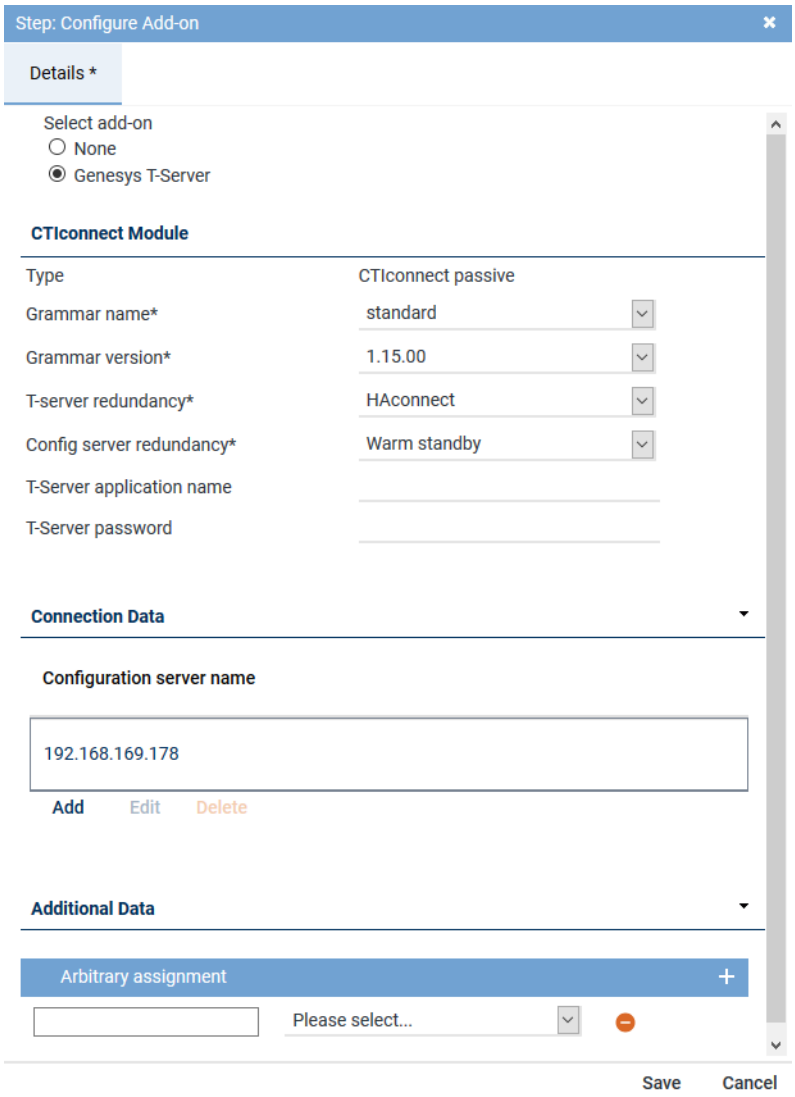


Fig. 138: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 34: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

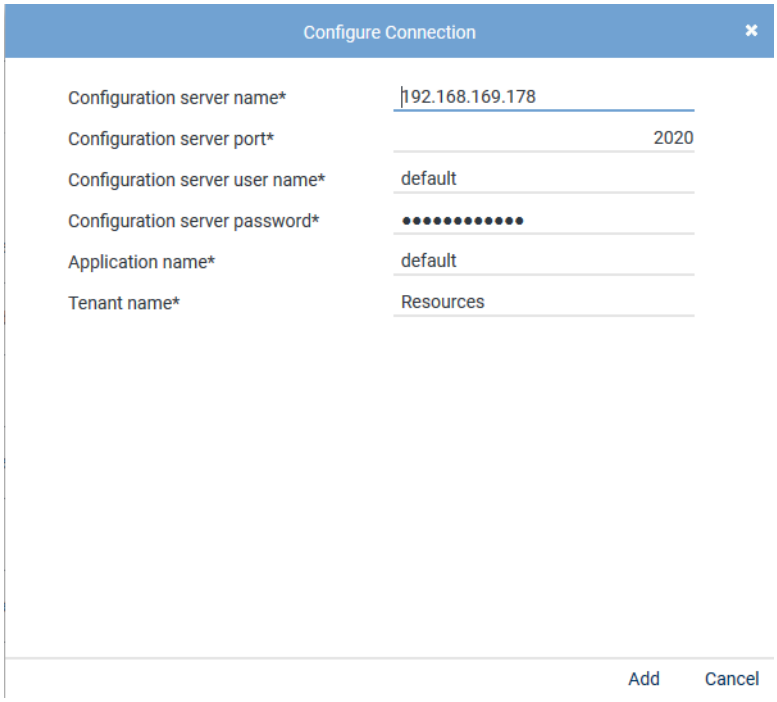


Fig. 139: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 35: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

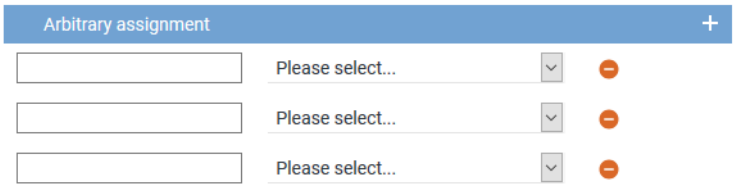


Fig. 140: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

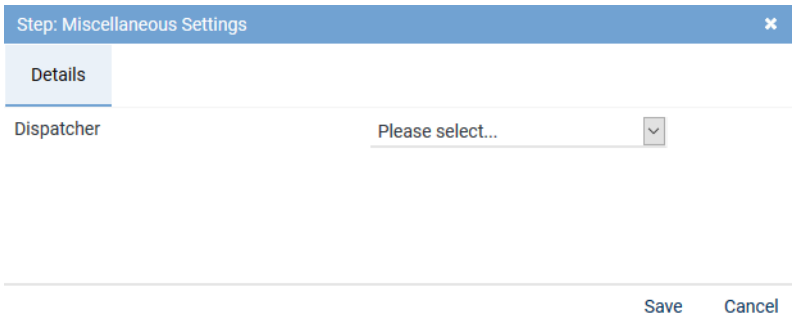


Fig. 141: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

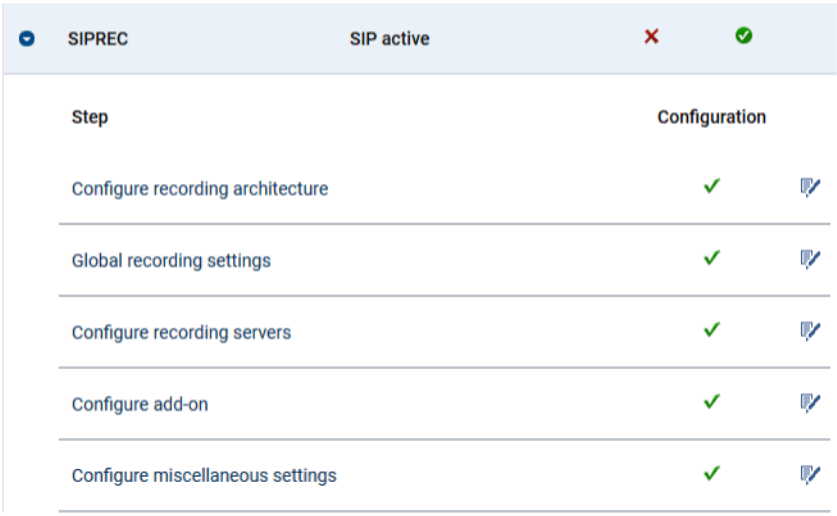


Fig. 142: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

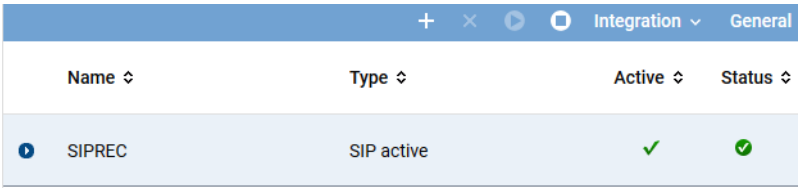


Fig. 143: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

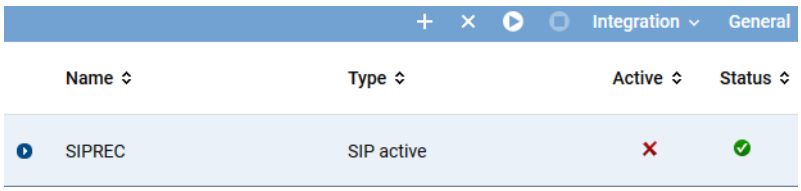


Fig. 144: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.2.3 Configure recording solution All-in-one Parallel Recording

7.1.2.3.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

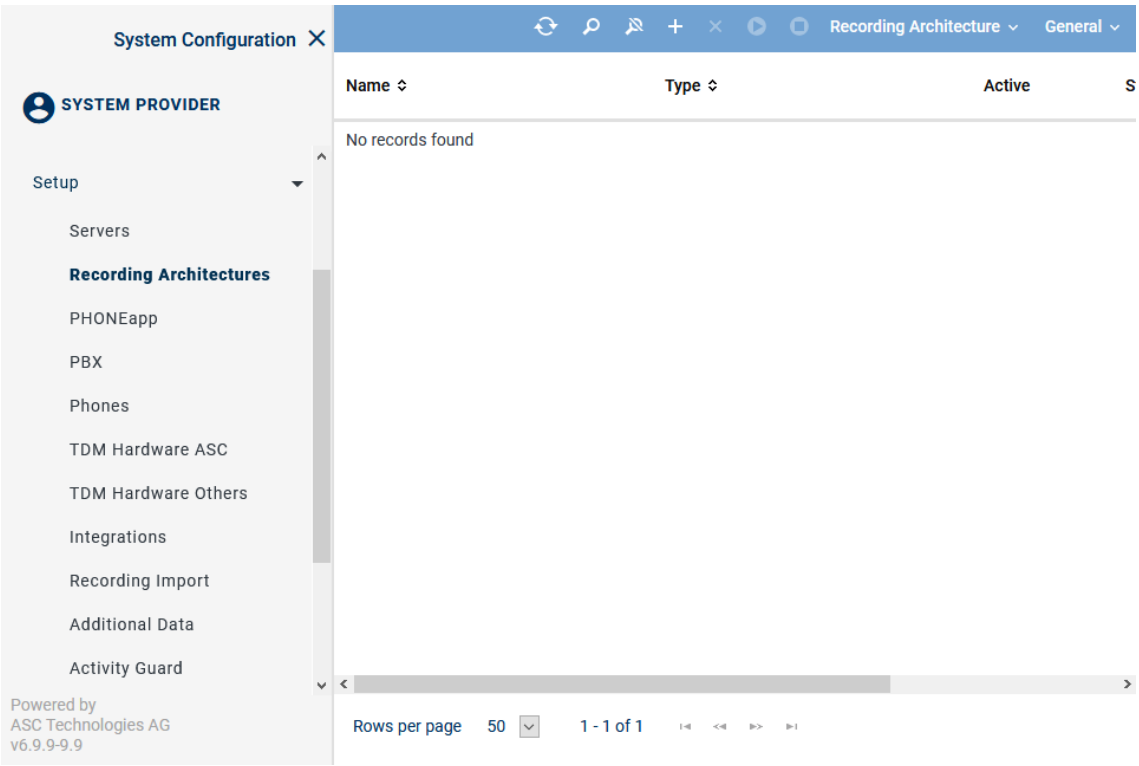


Fig. 145: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Recording Architectures module

The toolbar offers the following functions.

Fig. 146: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.

		The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Create	Creates a new recording architecture.
	Delete	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. **NOTICE!** You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	Activate	Activates the selected recording architecture.
	Deactivate	Deactivates the selected recording architecture. **NOTICE!** You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
Recording Architecture	*Standby Management*	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create recording architecture All-in-one Parallel Recording

If there are two recording servers which are supposed to record the same trunks in parallel, you must create a recording architecture of the type *All-in-one Parallel Recording*.

1. To create a new recording architecture, click on the icon *(Create)* in the toolbar of the main view.
   ⇨ The window *New Recording Architecture* appears.

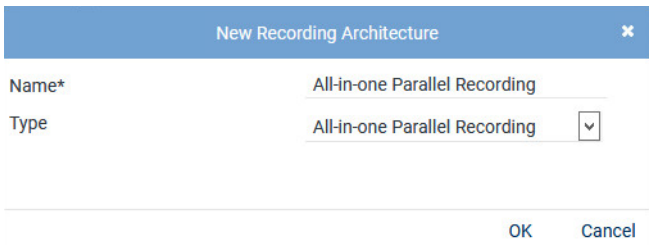


Fig. 147: Create recording architecture - All-in-one Parallel Recording

2. In the entry field *Name*, enter a descriptive name for the recording architecture.

3. From the drop-down list *Type*, select the recording architecture type *All-in-one Parallel Recording*.
   NOTICE! The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.
   ⇨ Your entries now appear in the detail view.

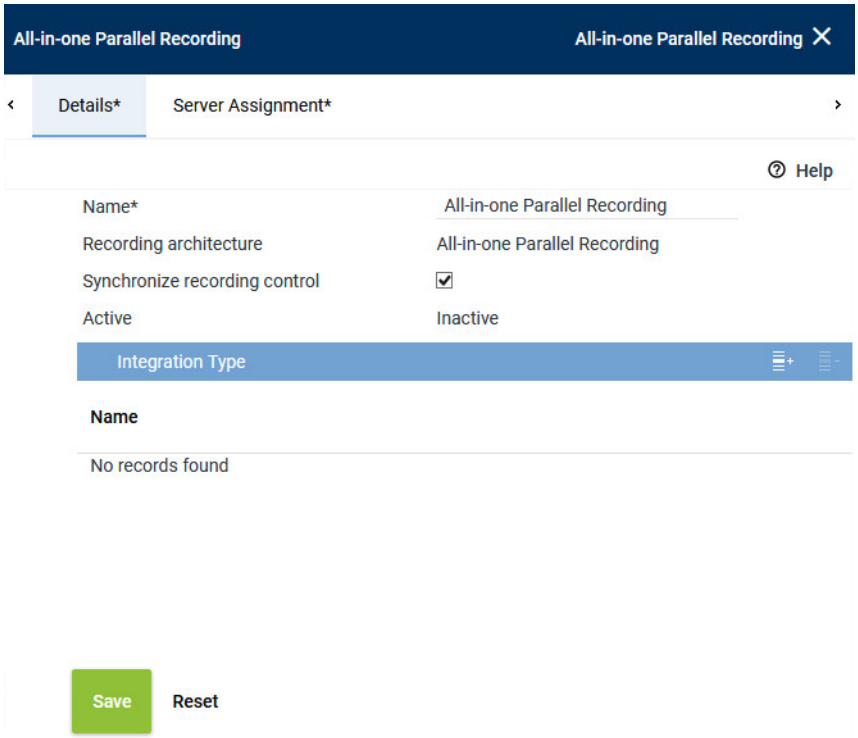


Fig. 148: Recording architecture - tab Details - All-in-one Parallel Recording

5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see chapter "Synchronization of recording control", p. 365.

NOTICE! If you have activated the option *Synchronize recording control*, only one set of data is generated in the database but audio data is recorded on both recording servers. This methods makes duplicate detection impossible. Ensure that there is enough storage capacity for twice the amount of data.

If you do not want to synchronize recording control, you can configure duplicate detection, see chapter "Duplicates in parallel recording architectures", p. 369.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 149: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for All-in-one Parallel Recording

1. Click on the tab *Server Assignment* to assign the recording servers to the recording architecture *All-in-one Parallel Recording*.

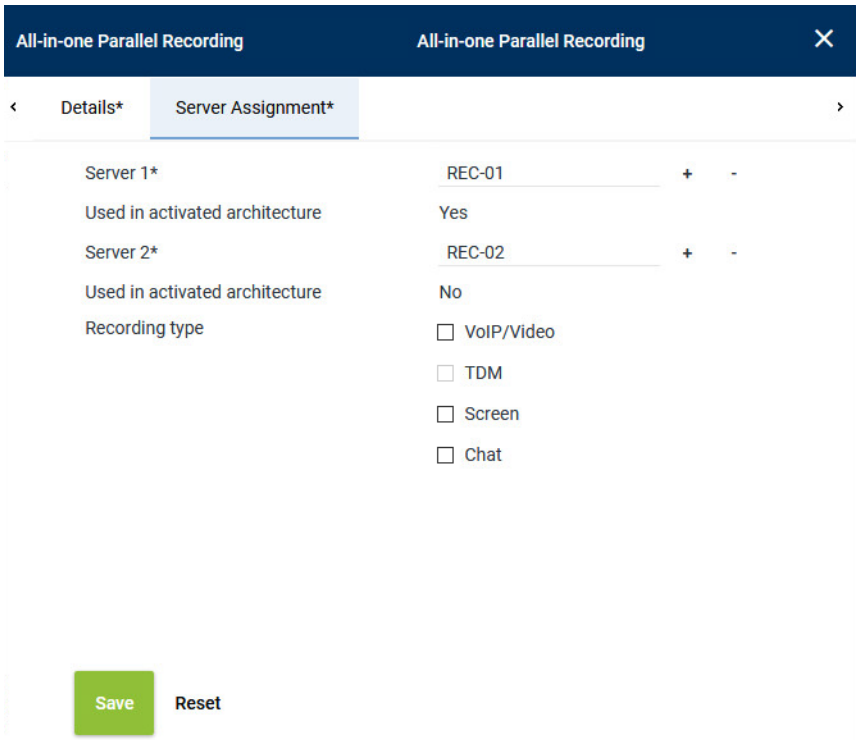


Fig. 150: Recording Architecture - tab Server Assignment

2. Click on the button + behind the entry field *Server 1*.
   ⇨ The window *Servers* appears.

Fig. 151: Recording Architecture - assign server - example

3. Select *Server 1*.

ⓘ A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

4. Click on the button *Add*.

⇨ The name of the server now appears in the detail view.

5. To delete an assignment, click on the button - .
6. Repeat the steps and select Server 2 for the entry field *Server 2*.
7. Select the recording type you would like to use for these servers by activating the check box.

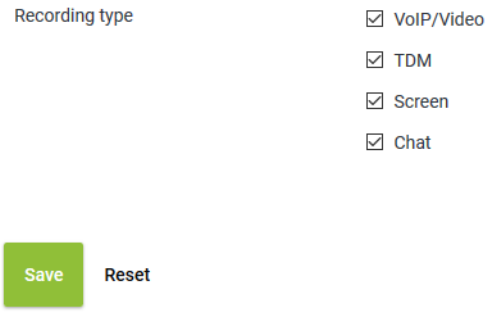


Fig. 152: Recording Architecture - activate recording type

8. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

You can activate several recording types if the integration has been designed for this and if you have installed the respective licenses.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the toolbar becomes active.
3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

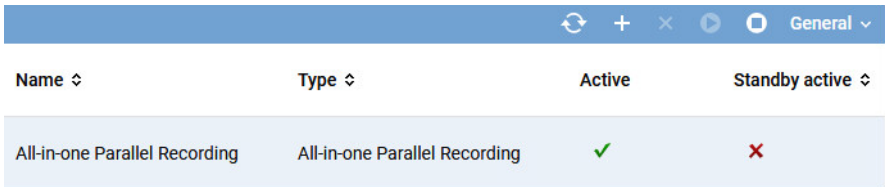


Fig. 153: Activate recording architecture

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✗ *(Inactive)* appears.

The recording architecture must have been activated so that the integration can be configured.

Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see chapter "Configure duplicate detection", p. 369.

If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.3.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

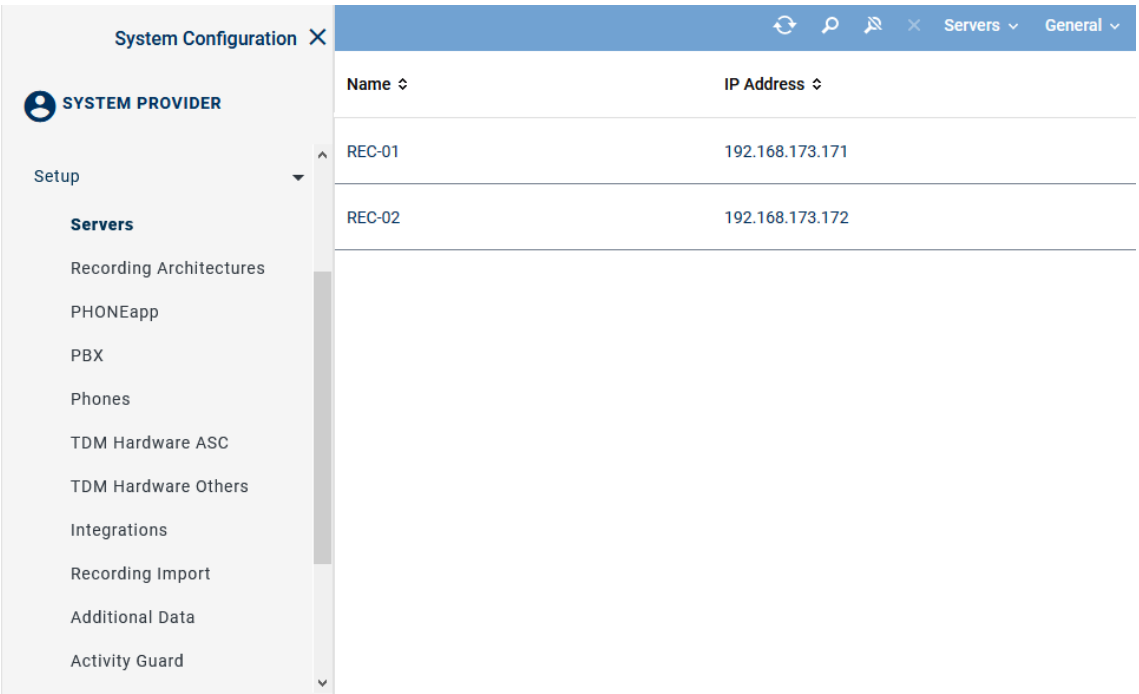


Fig. 154: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.
Path	Shows the path of the server.
Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 155: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.

	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.
Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 137.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.

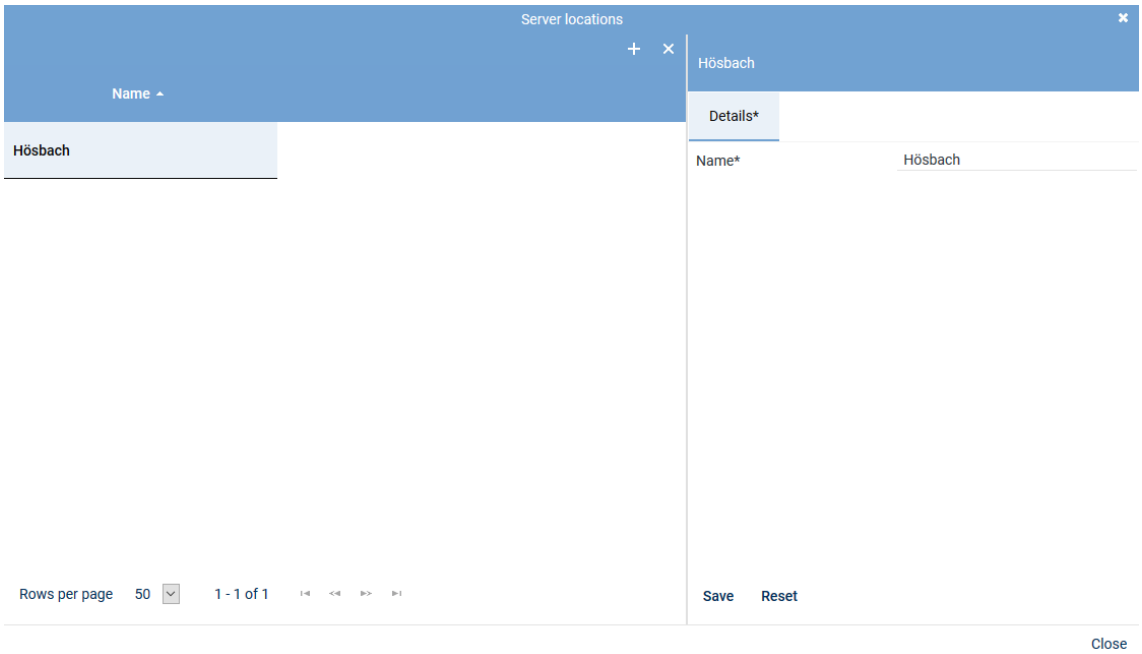


Fig. 156: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

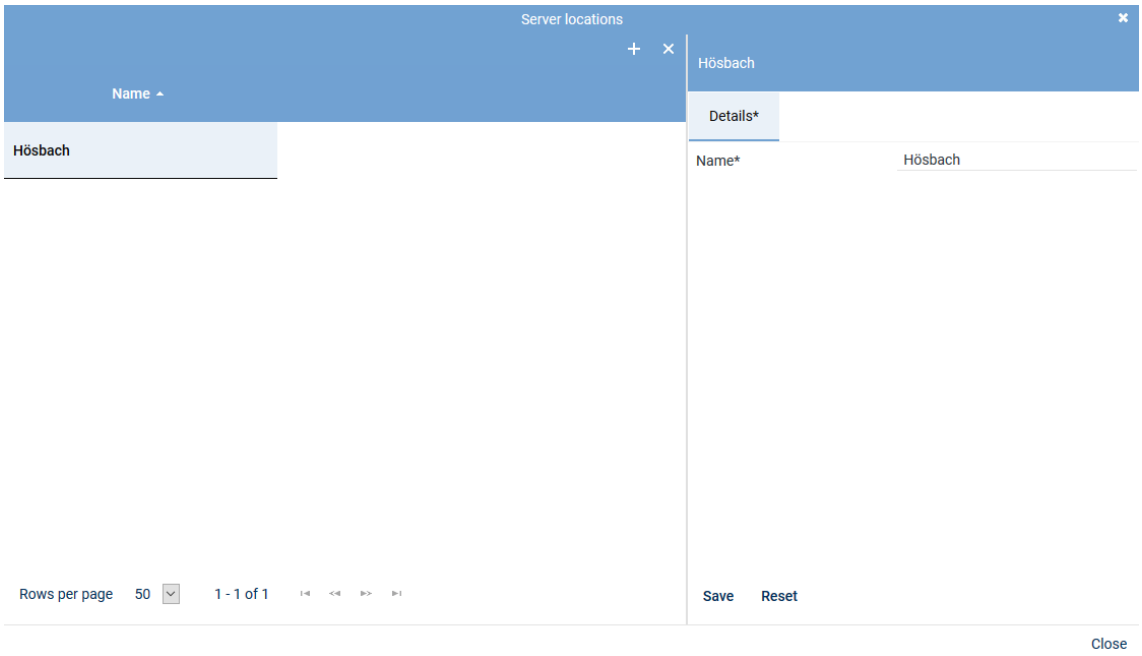


Fig. 157: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

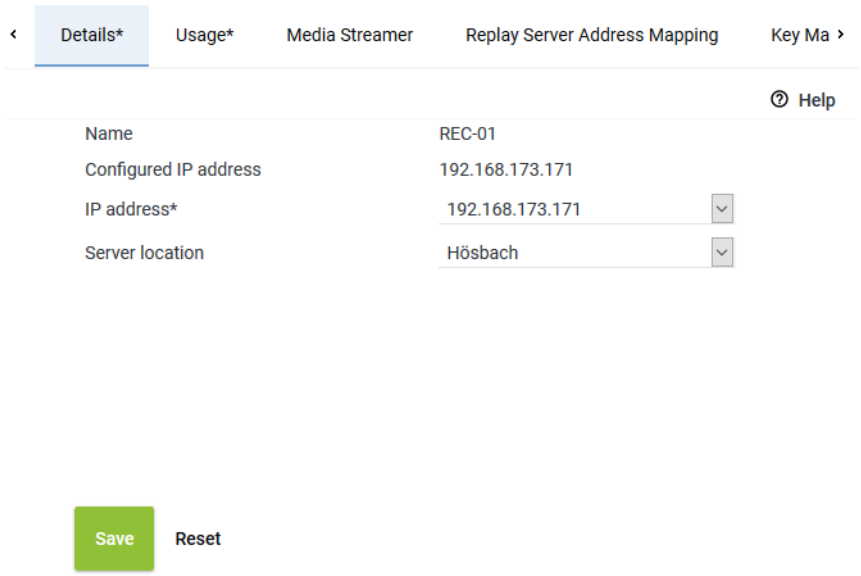


Fig. 158: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.

4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

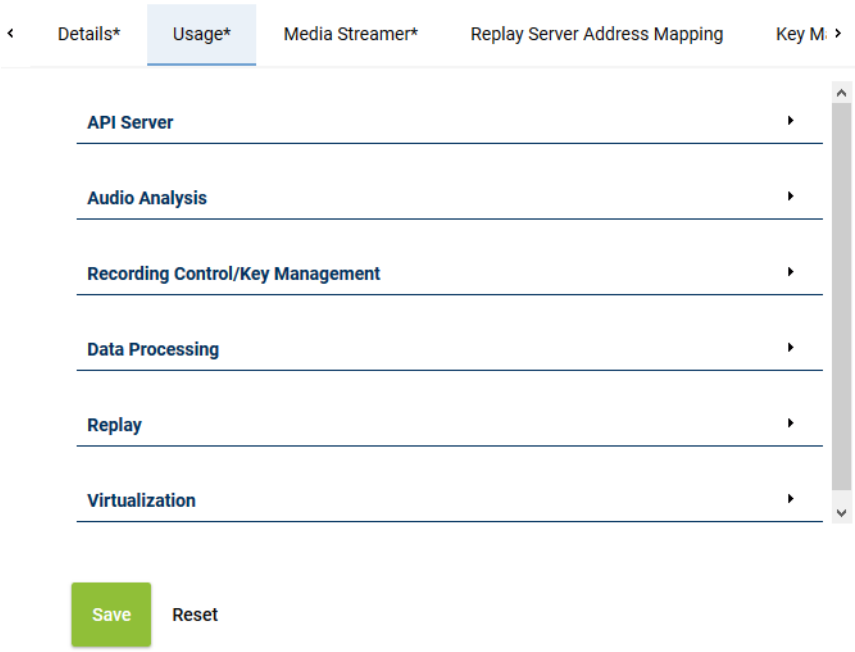


Fig. 159: Servers - tab usage

Group field API Server

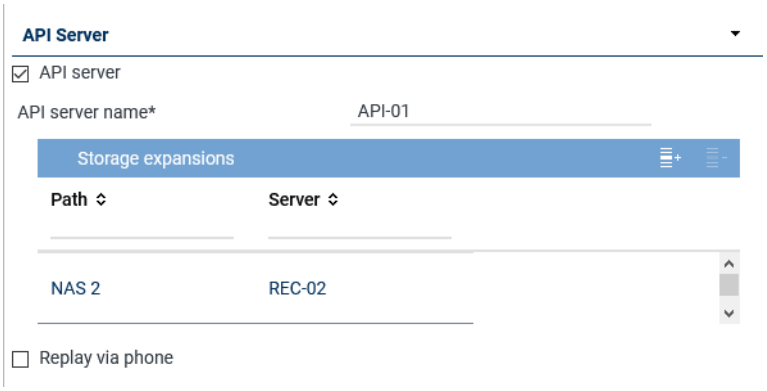


Fig. 160: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server.

Parameter	Value/Description
	☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 151.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List *Storage expansions*	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 142. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list. If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 149. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

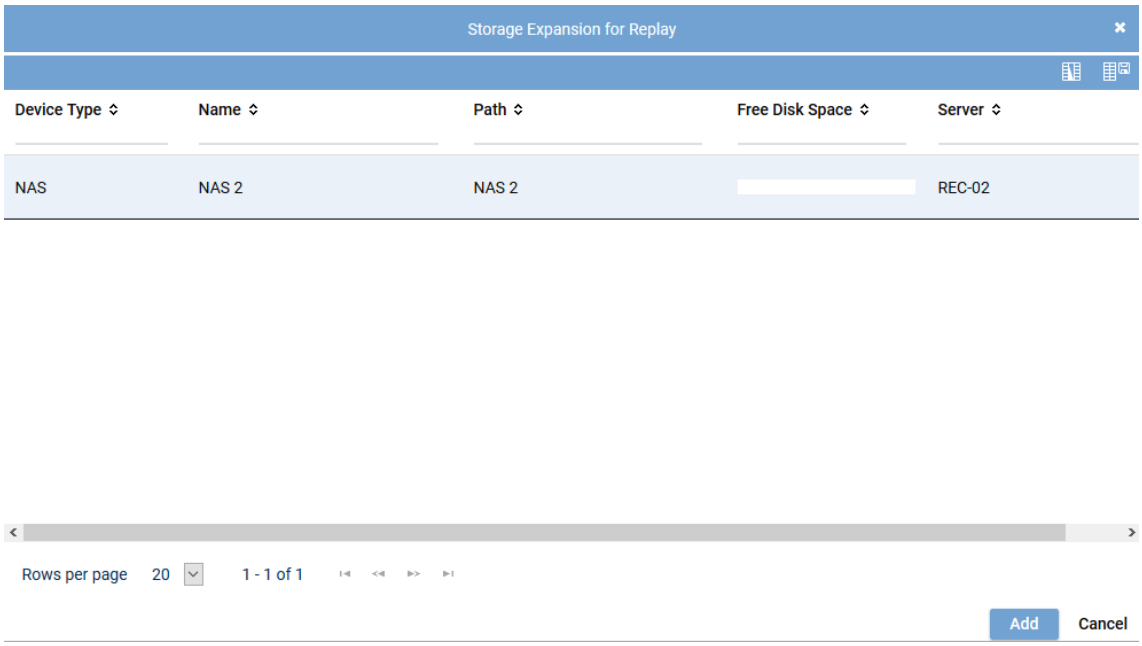


Fig. 161: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

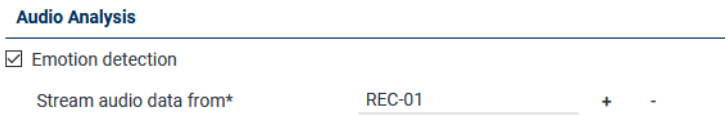


Fig. 162: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 36: Configure audio analysis

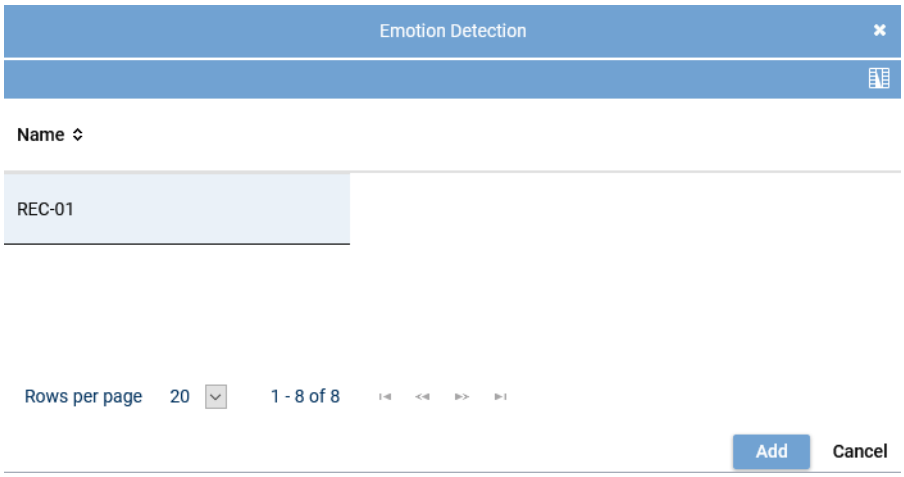


Fig. 163: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

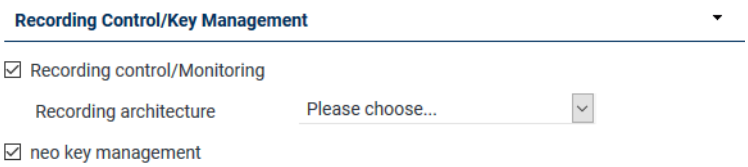


Fig. 164: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 37: Configure recording control/key management

Group field Data Processing

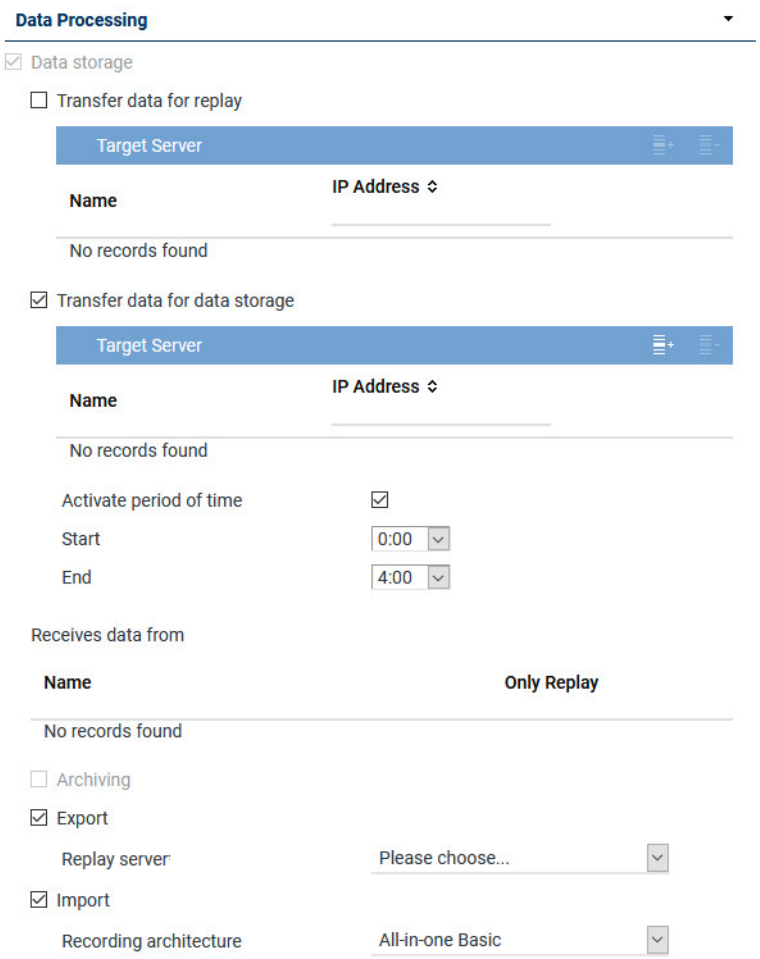


Fig. 165: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 146. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be trans-

Parameter	Value/Description
	ferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 146. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.

Parameter	Value/Description
	NOTICE! If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 38: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 166: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

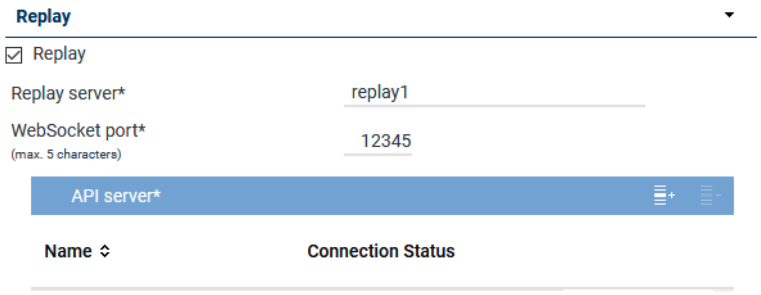


Fig. 167: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 147. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 39: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.

- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

Fig. 168: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 140.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 169: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management.

Parameter	Value/Description
	• *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 40: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

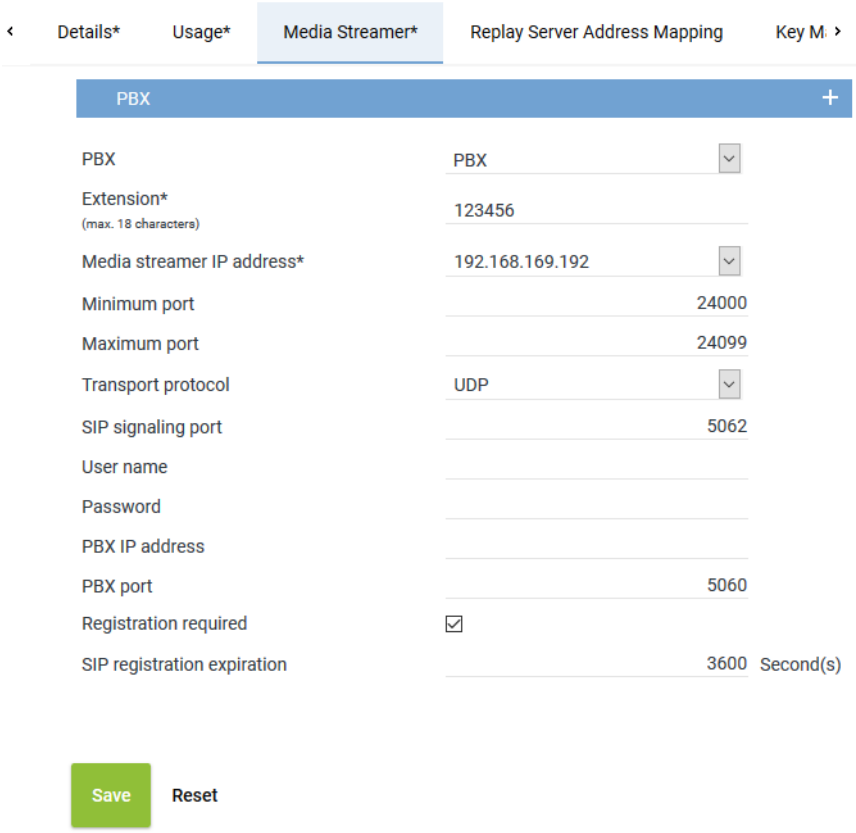


Fig. 170: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.

	If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 155.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number. A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

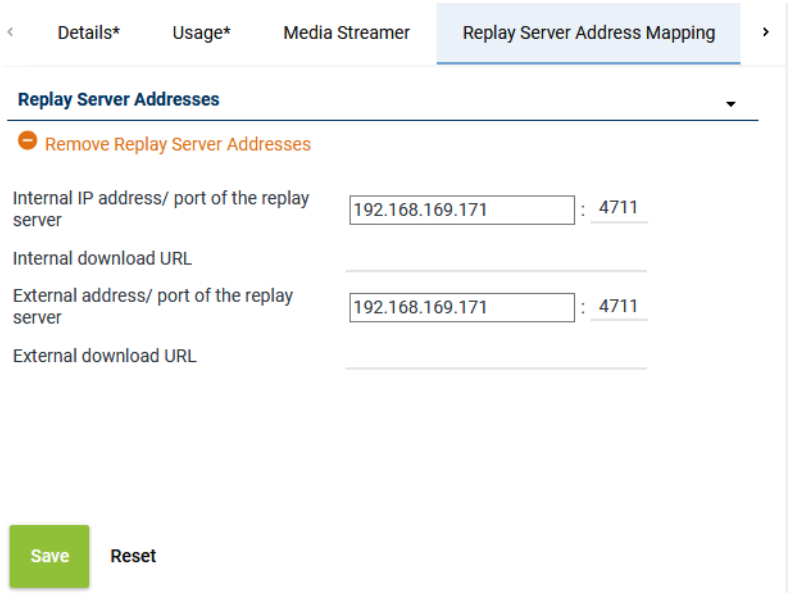


Fig. 171: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

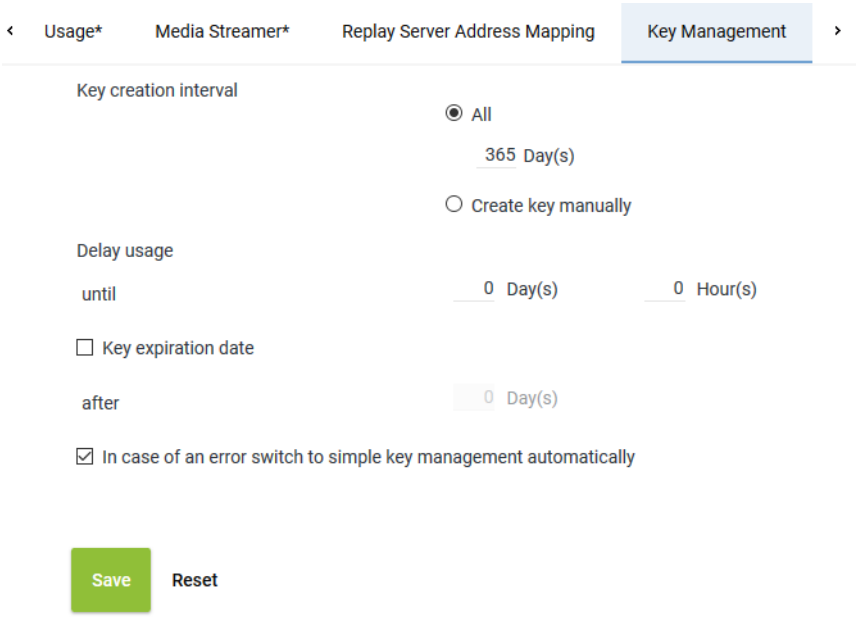


Fig. 172: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.

Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid. ☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

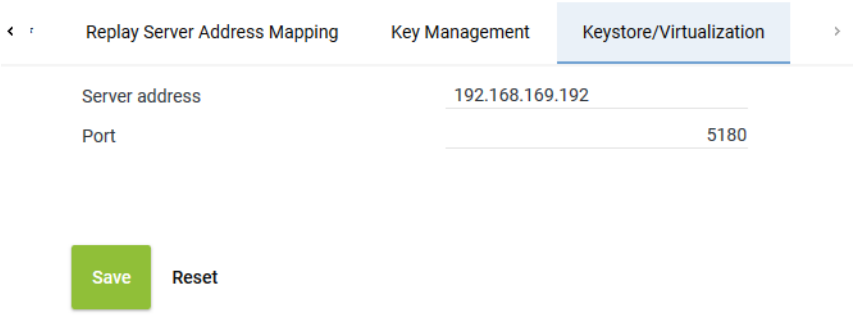


Fig. 173: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management:

	IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.3.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

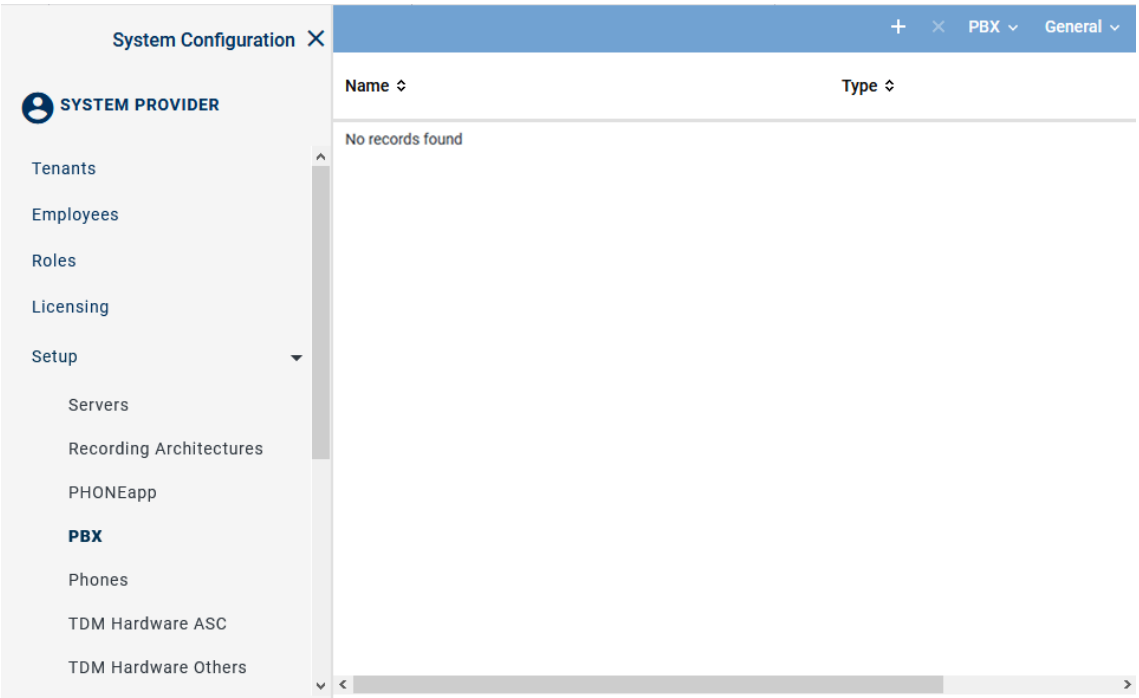


Fig. 174: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 175: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.

PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

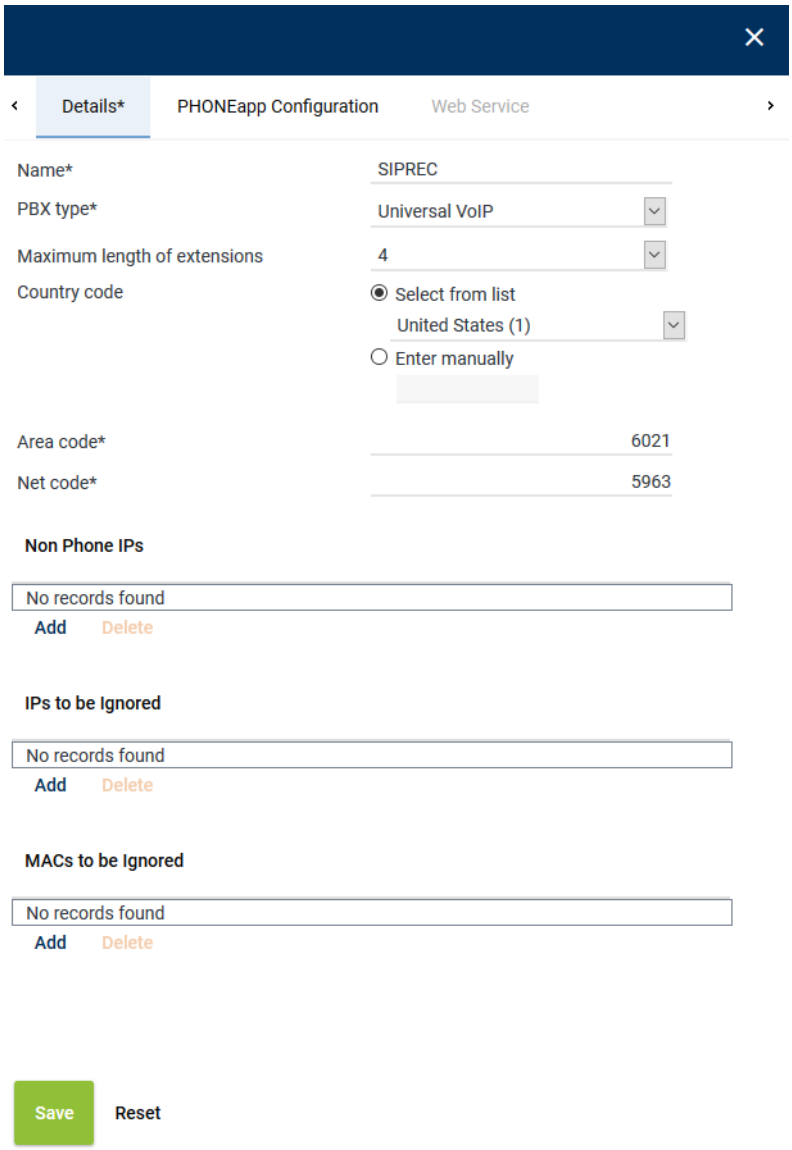


Fig. 176: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list* Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 41: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 42: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.3.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

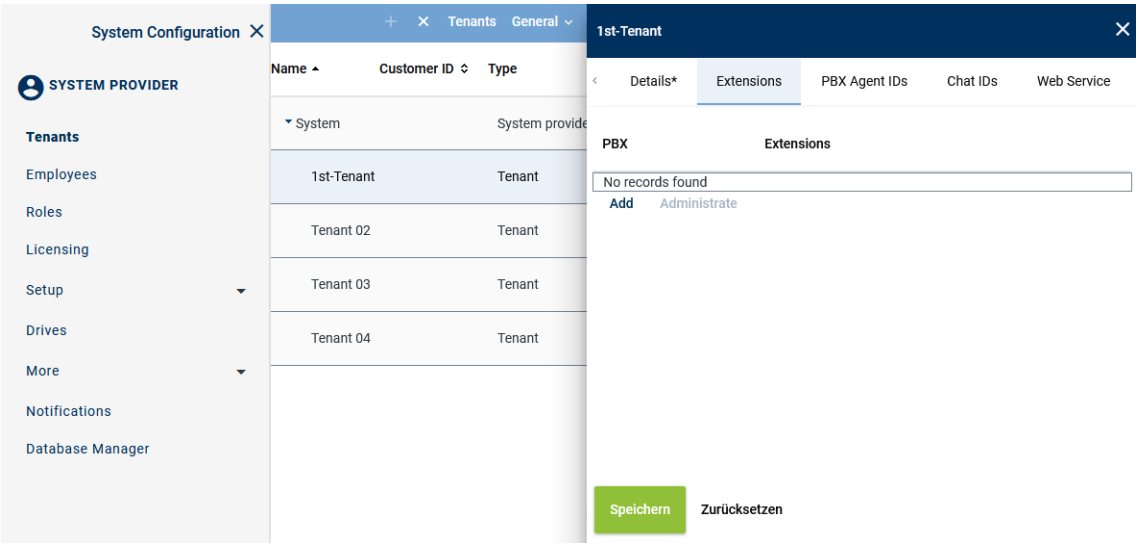


Fig. 177: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.

⇨ The following window appears:

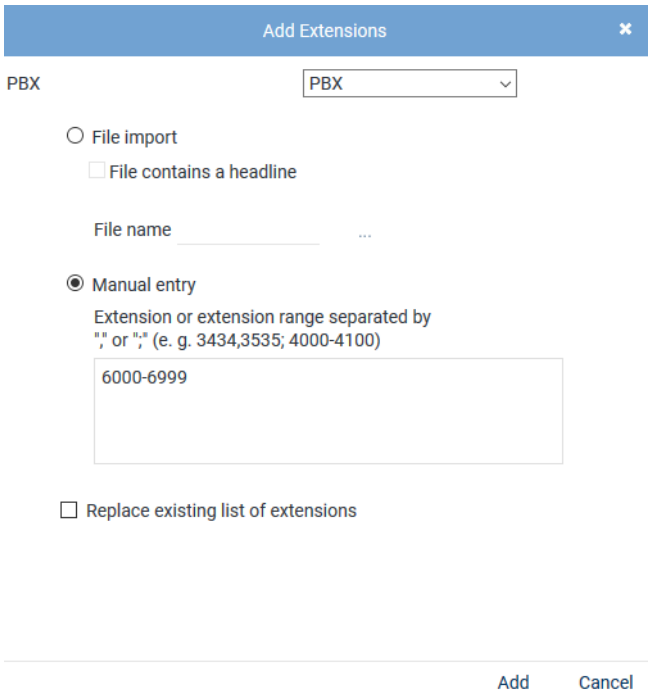


Fig. 178: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT* • *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually.

	To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

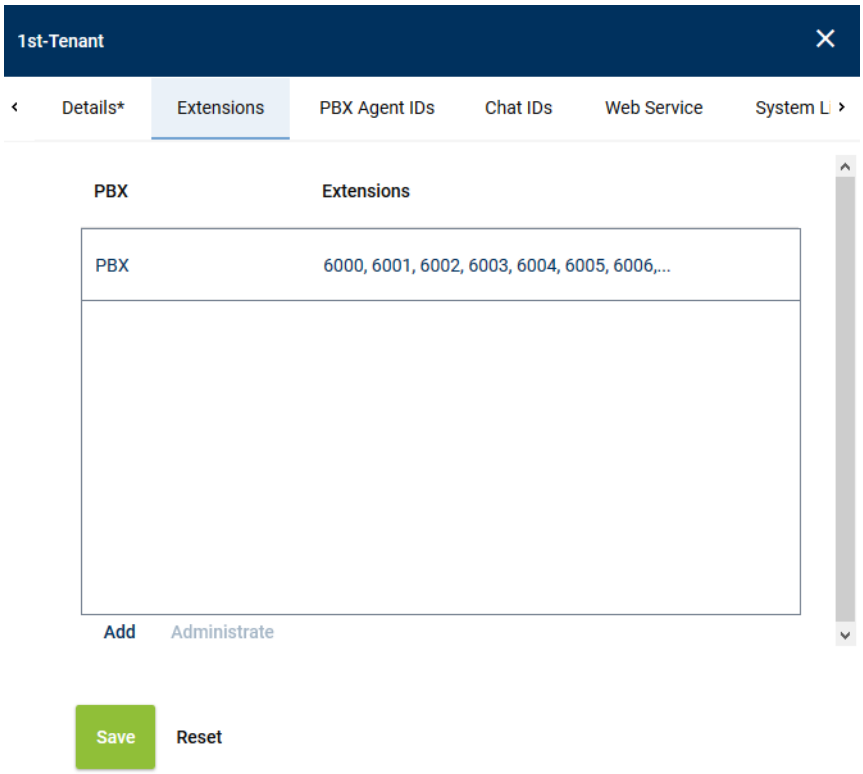


Fig. 179: Remove extensions

2. Click the button *Administrate*.

3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 180: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

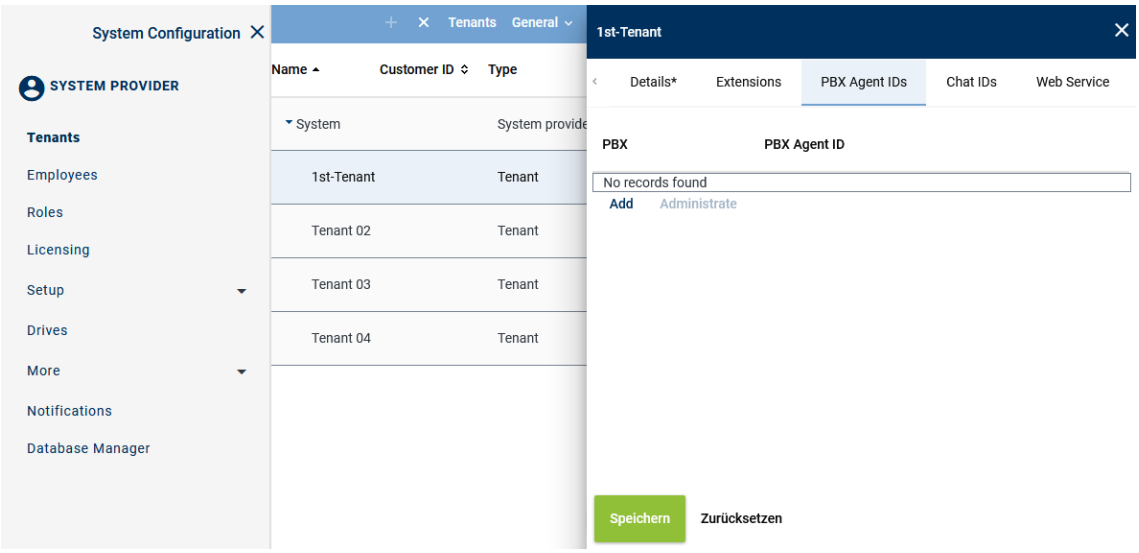


Fig. 181: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

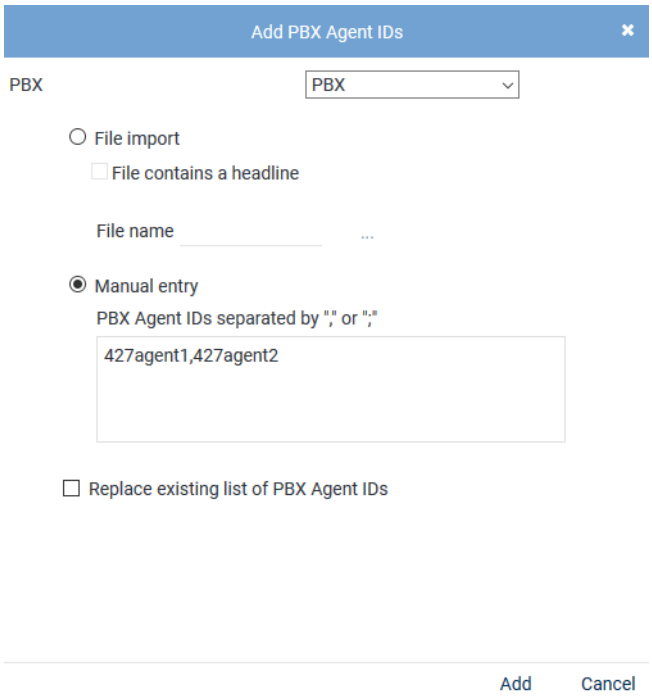


Fig. 182: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline

	Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

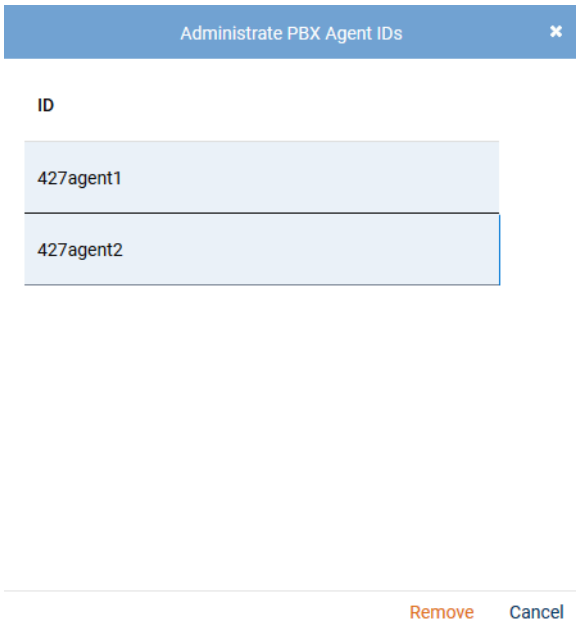


Fig. 183: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.3.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

> In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

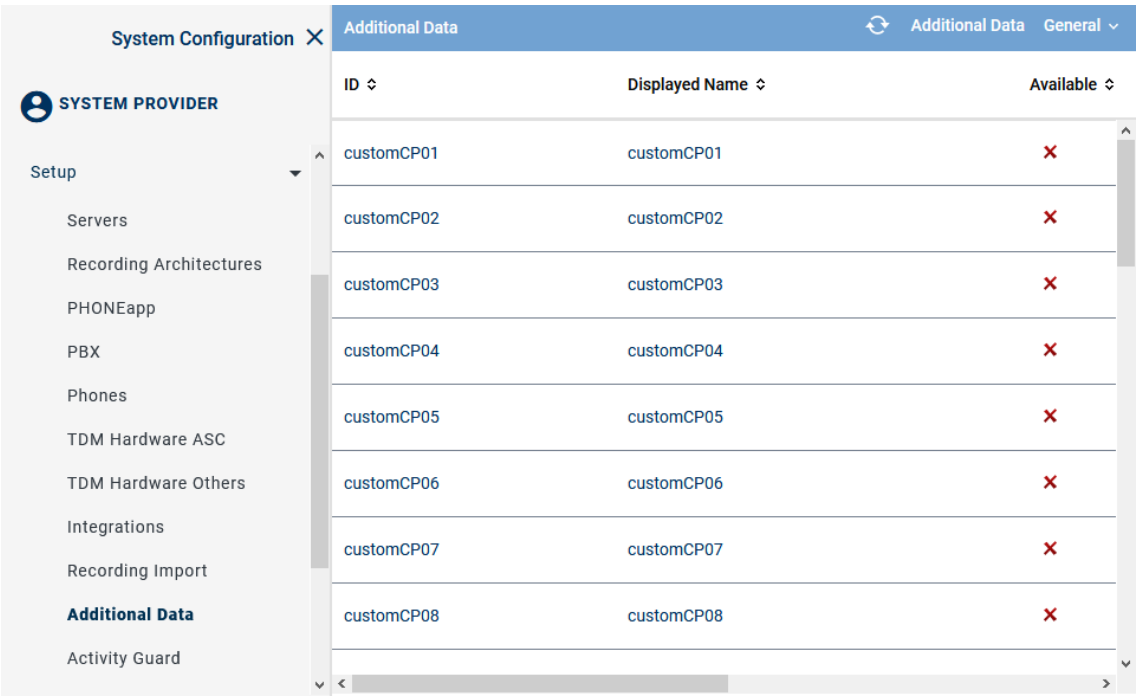


Fig. 184: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

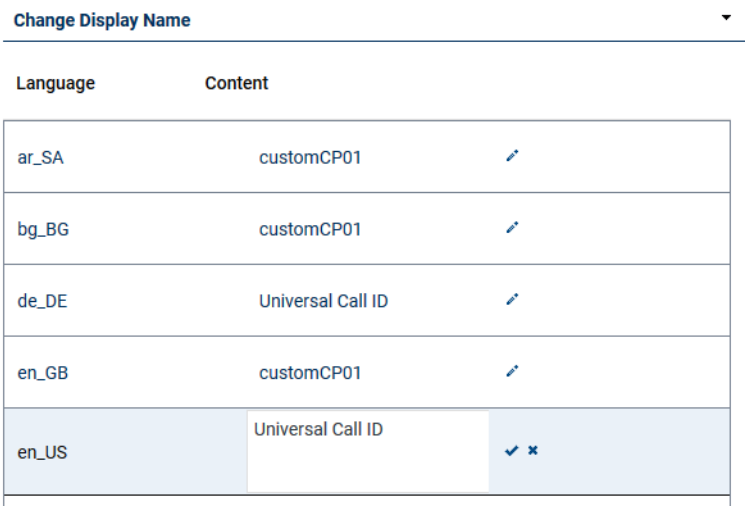


Fig. 185: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 186: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.3.6 Create integration for All-in-one Parallel Recording

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

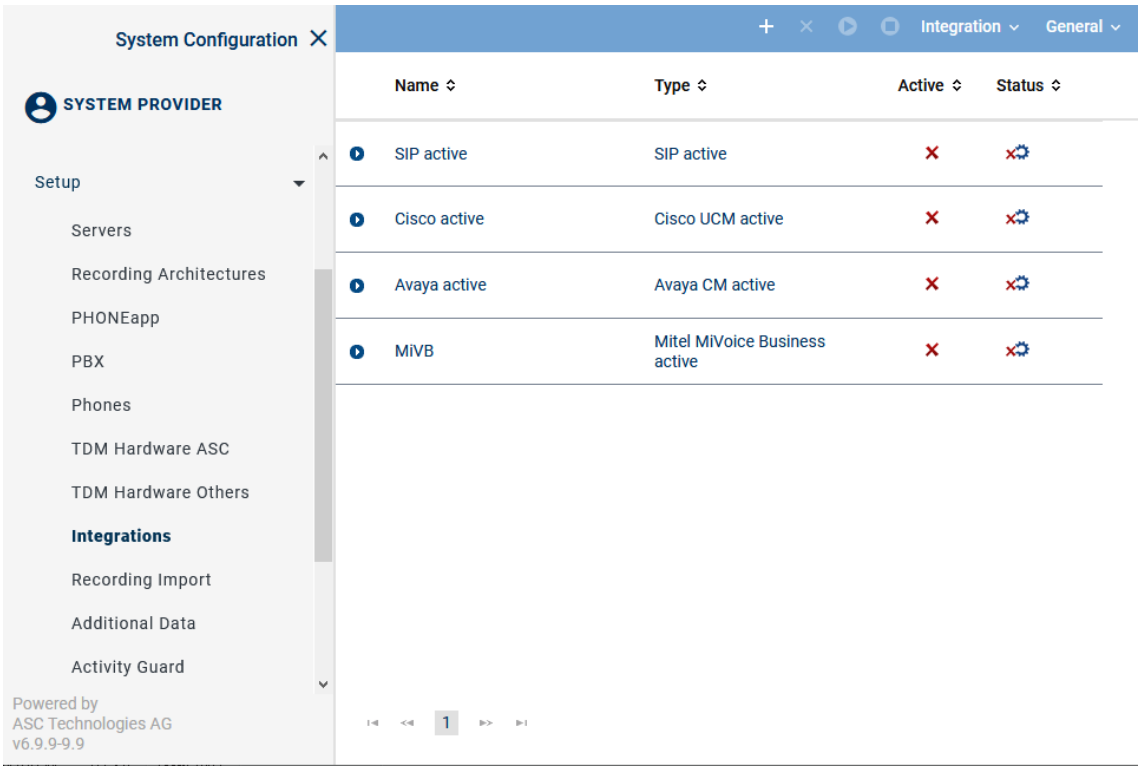


Fig. 187: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 188: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

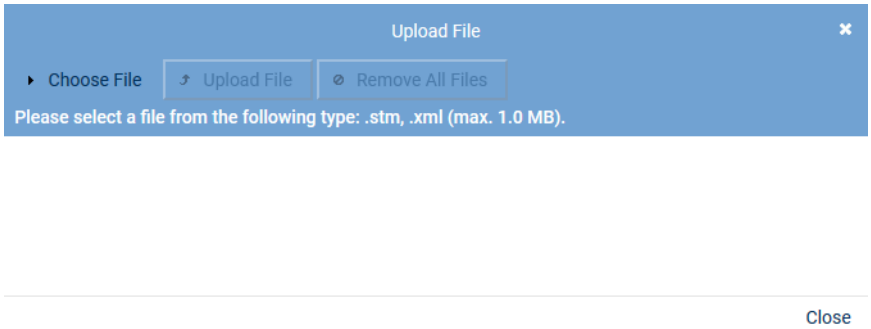


Fig. 189: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

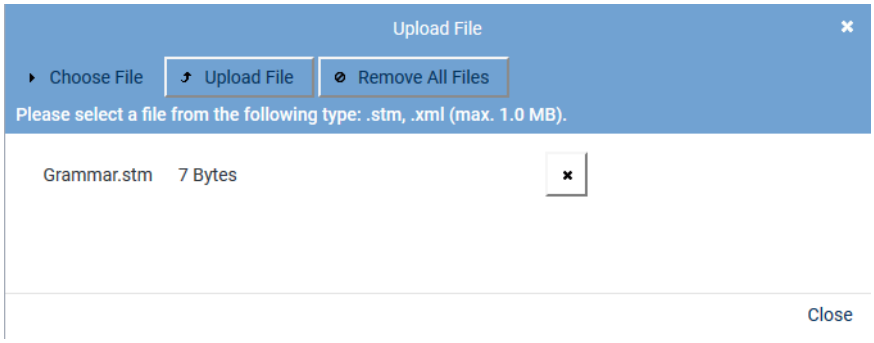


Fig. 190: Upload grammar

5. To remove a selected file from the list, click on the button × *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 191: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 43: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 192: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for All-in-one Parallel Recording

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

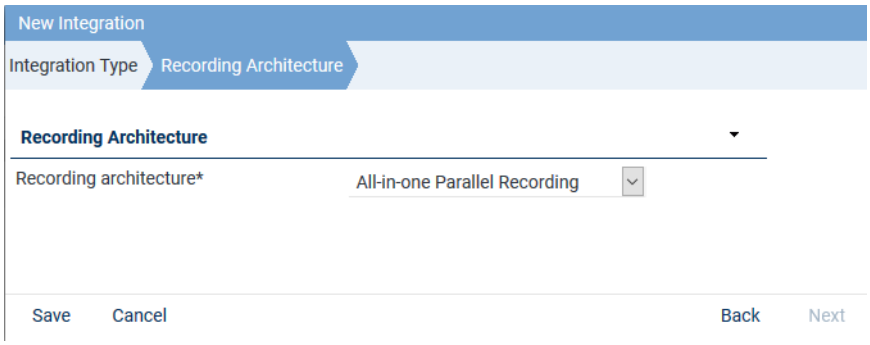


Fig. 193: Assign recording architecture - All-in-one Parallel

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see chapter "Duplicates in parallel recording architectures", p. 369.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

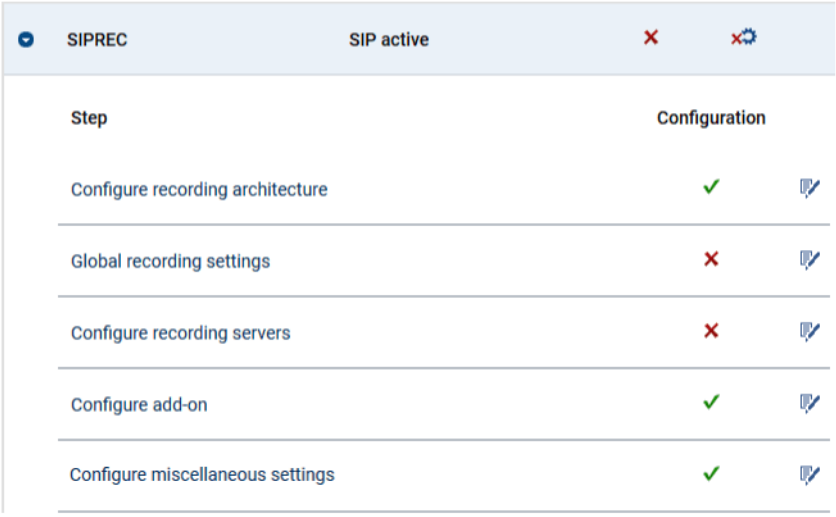


Fig. 194: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

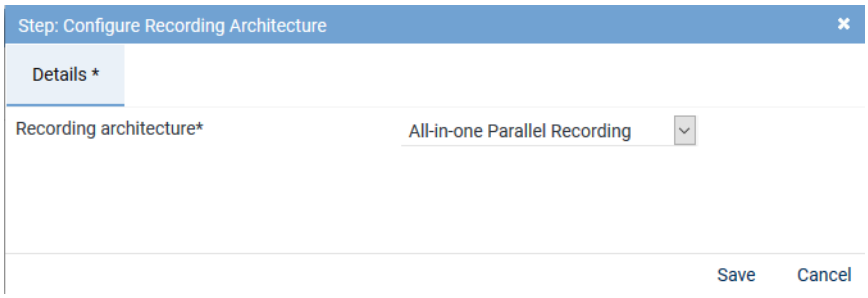


Fig. 195: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for All-in-one Parallel Recording

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.

   ⇨ The window *Step: Global Recording Settings* appears.

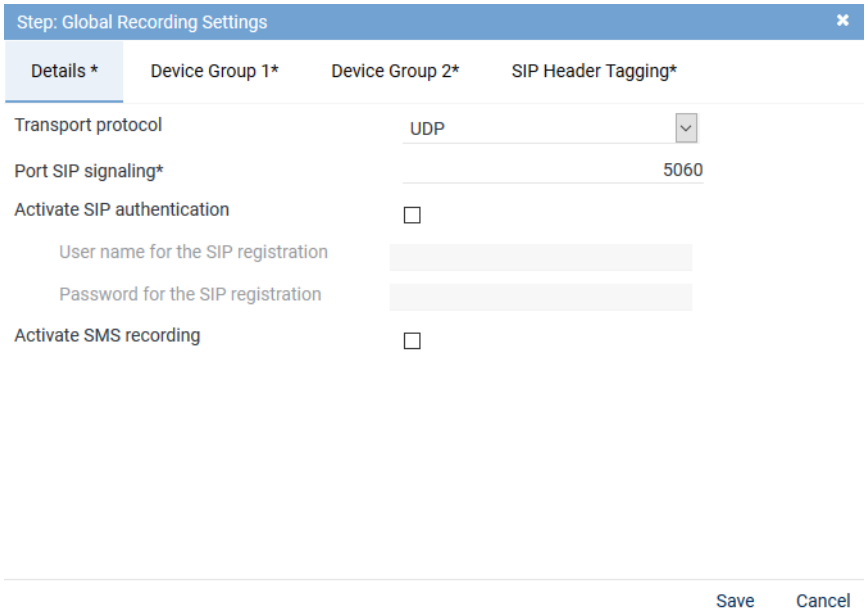


Fig. 196: Configuration step - Global Recording Settings - All-in-one Parallel Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	Select the transport protocol *UDP* for the SIP signaling between the recording server and the PBX.
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*
Activate SIP authentication	Deactivate this option for this recording solution.
Activate SMS recording	This function is not supported in this recording solution.

Tab. 44: Global recording settings

3. To save the entries, click on the button *Save*.
   To discard entries, click on the button *Cancel*.

Tab Device Groups

In parallel recording, you can configure connections to different PBXs.

1. Select the tab Device Group 1 to configure the connection to PBX 1.

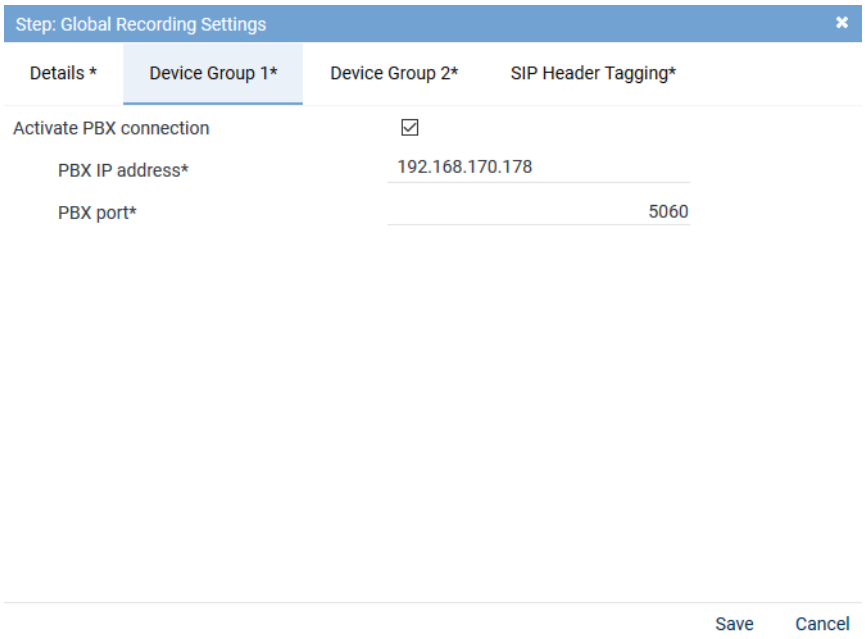


Fig. 197: Configure device group 1

Parameter	Description
Activate PBX connection	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
PBX IP address	Enter the IP address of the PBX for the first device group.
PBX port	Enter the port of the PBX which is used to communicate with the PBX.

2. Select the tab *Device Group 2* to configure the connection to PBX 2.

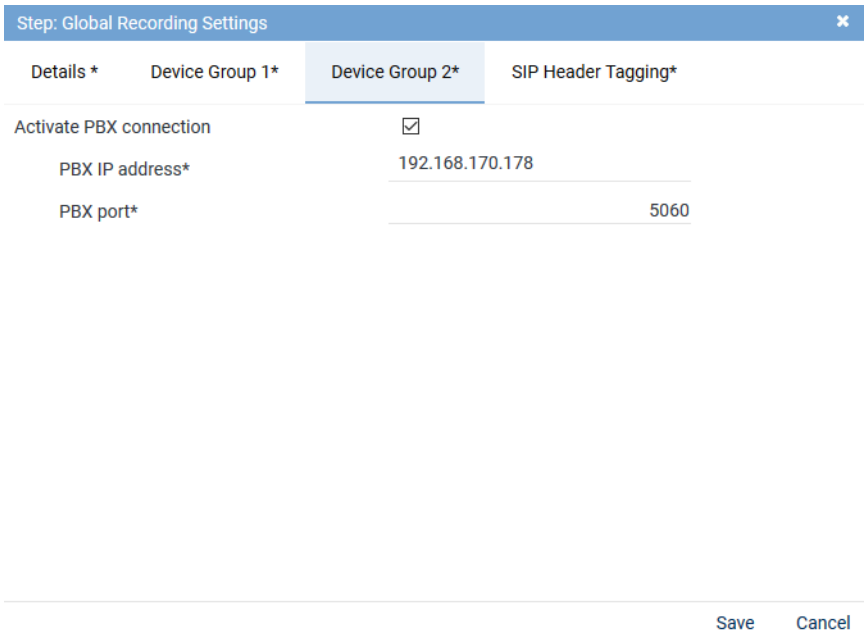


Fig. 198: Configure device group 2

Parameter	Description
Activate PBX connection	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
PBX IP address	Enter the IP address of the PBX for the second device group.
PBX port	Enter the port of the PBX which is used to communicate with the PBX.

3. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

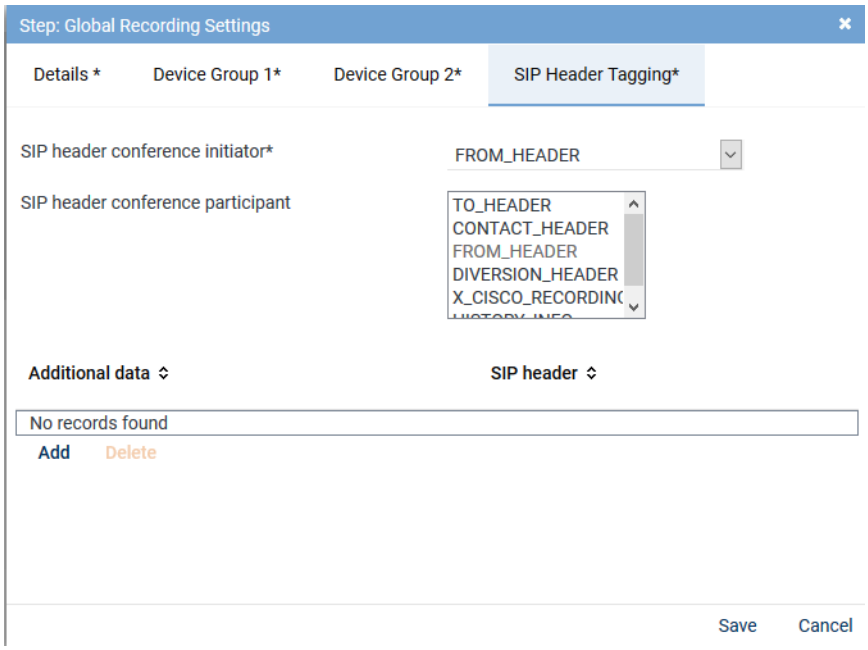


Fig. 199: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.

   ⇨ The window *SIP Additional Data* appears.

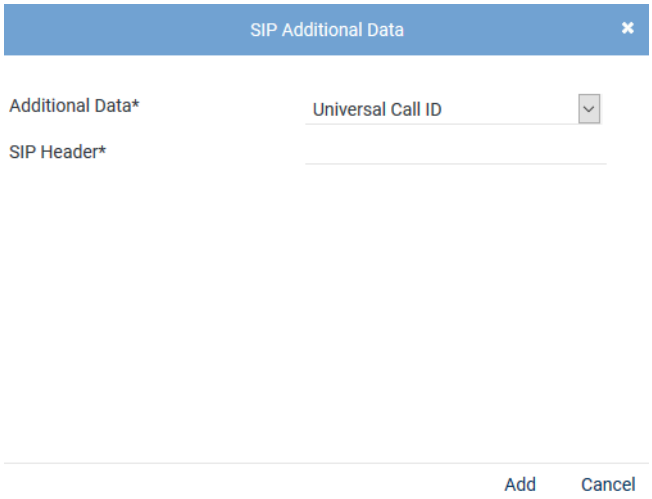


Fig. 200: SIP Additional Data

ⓘ Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted.

Parameter	Value/Description
	To have ASC configure the mapping file, contact your distribution partner.

Tab. 45: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for All-in-one Parallel Recording

For parallel recording to run smoothly, you must define a port range for both recording servers. The range may be the same on both recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

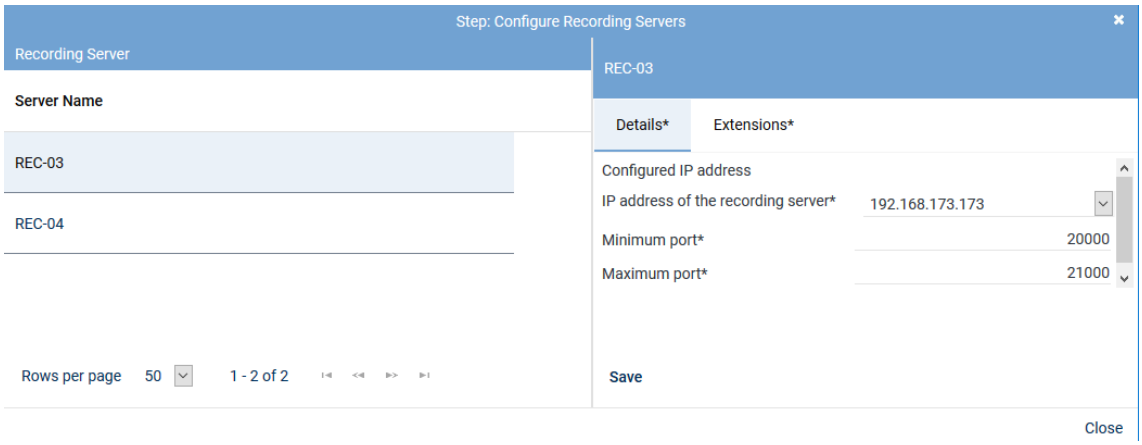


Fig. 201: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 46: Configure recording servers

ⓘ For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.
In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Tab Extensions

1. Click on the tab *Extensions*.

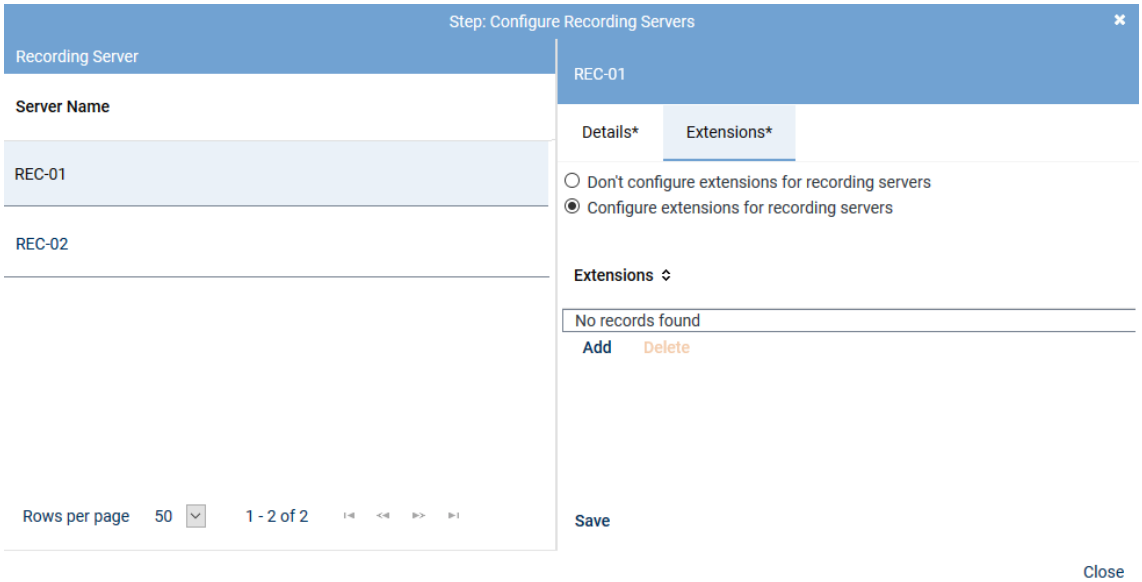


Fig. 202: Tab Extensions

The following options are available:

Configure no extensions for recording servers	Activate this option if you have not configured the extensions for the recording server in the PBX.
Configure extensions of the recording server	Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

2. To add extensions, click on the button *Add* in the table *Extensions*.
   ⇨ The window *Add Extensions* appears.

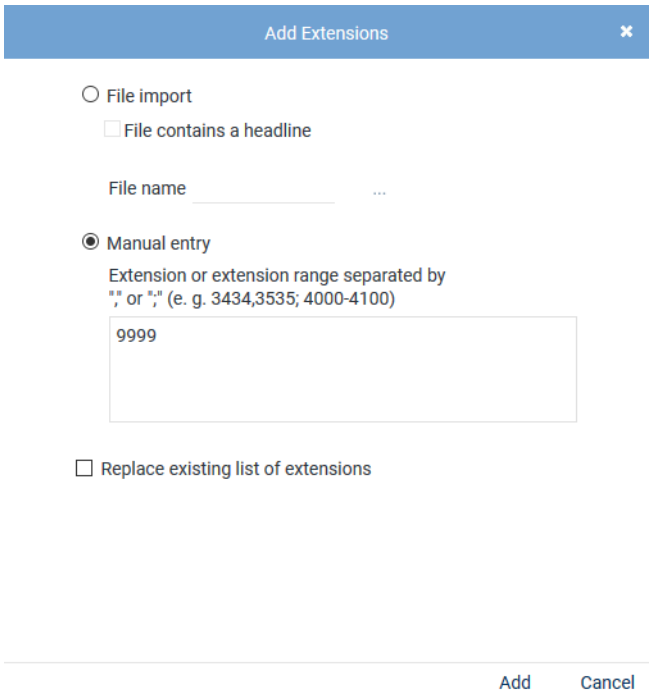


Fig. 203: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

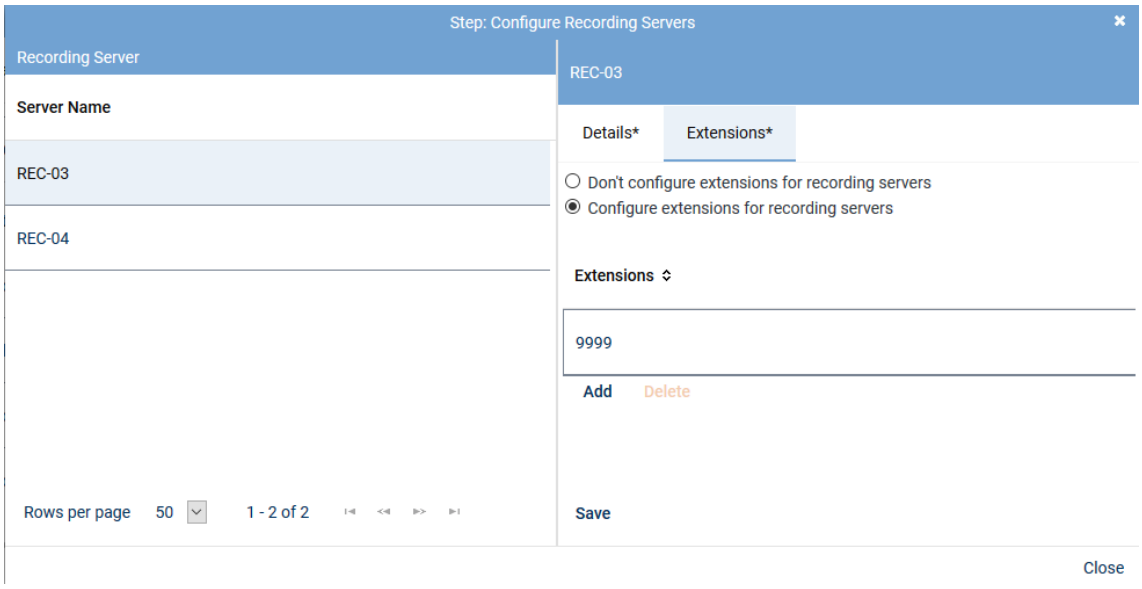


Fig. 204: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.
8. Click on the button *Save*.

9. Click on the button *Close* to finish this configuration step.

Configure add-on

The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

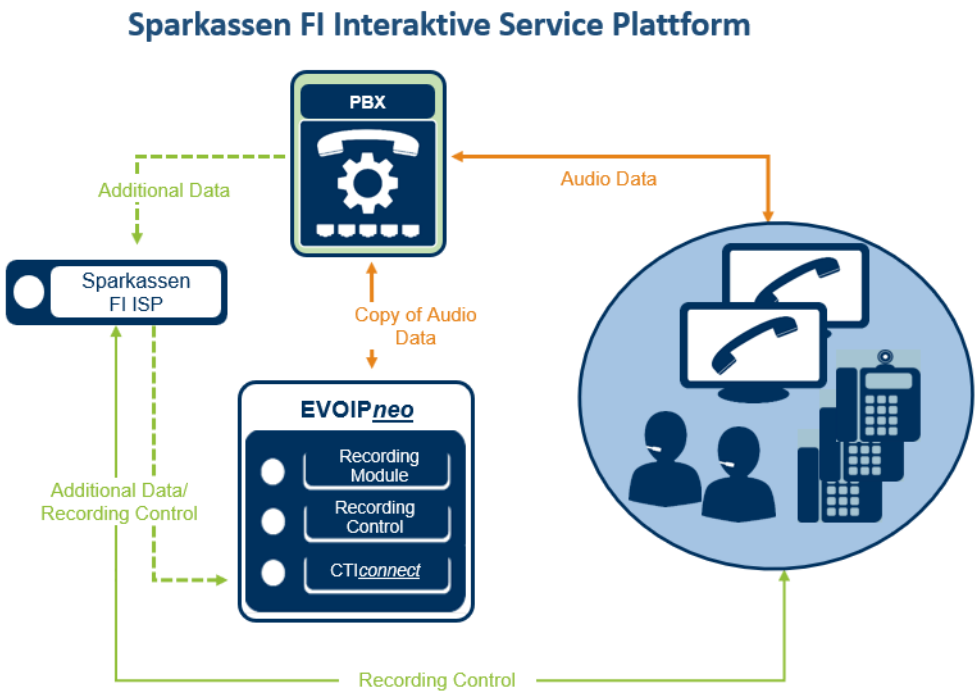


Fig. 205: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

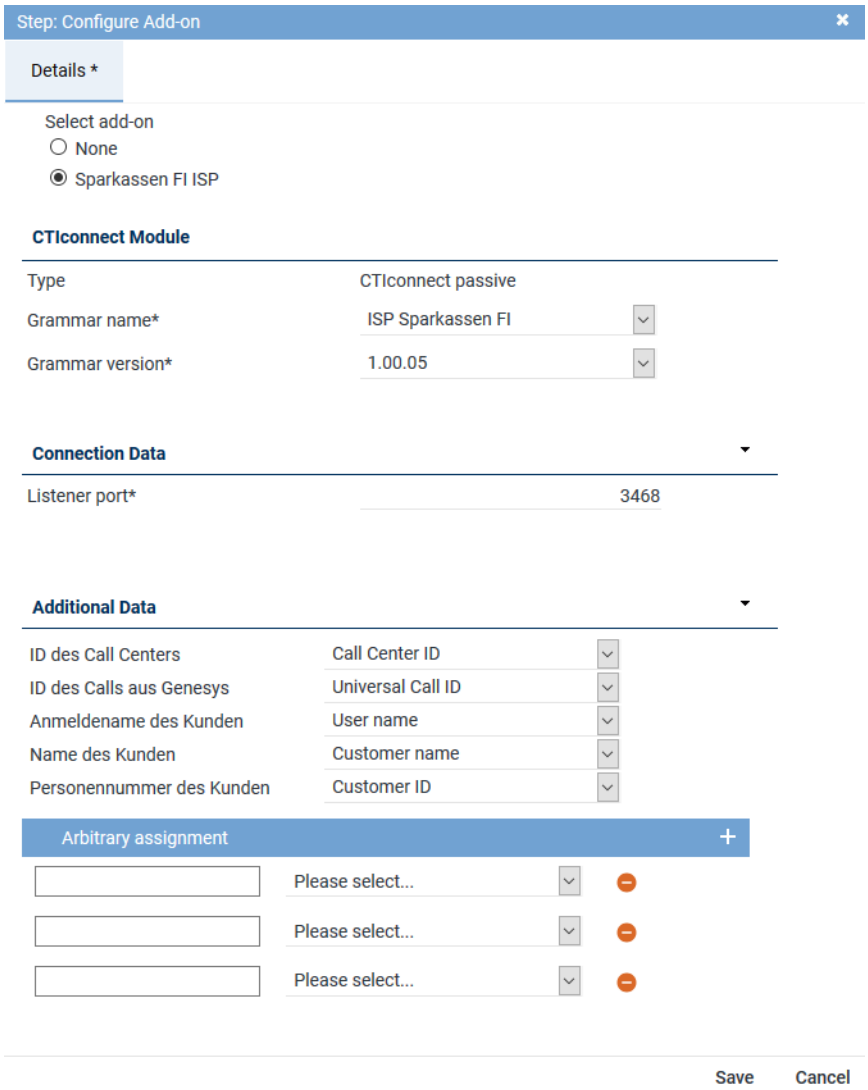


Fig. 206: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 47: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 168.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 48: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

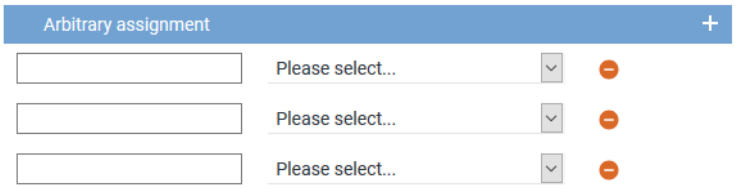


Fig. 207: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.

   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

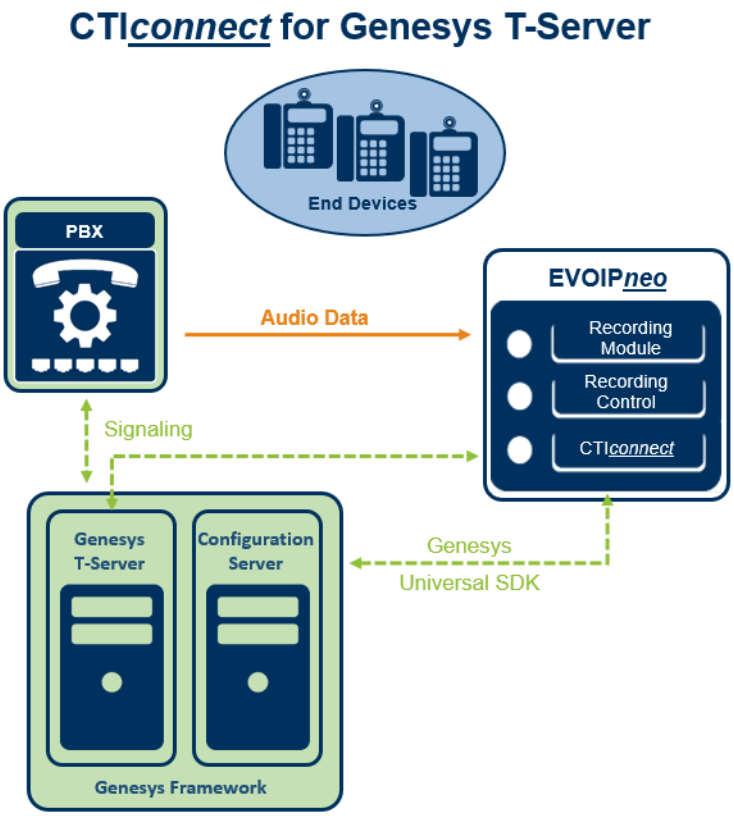


Fig. 208: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

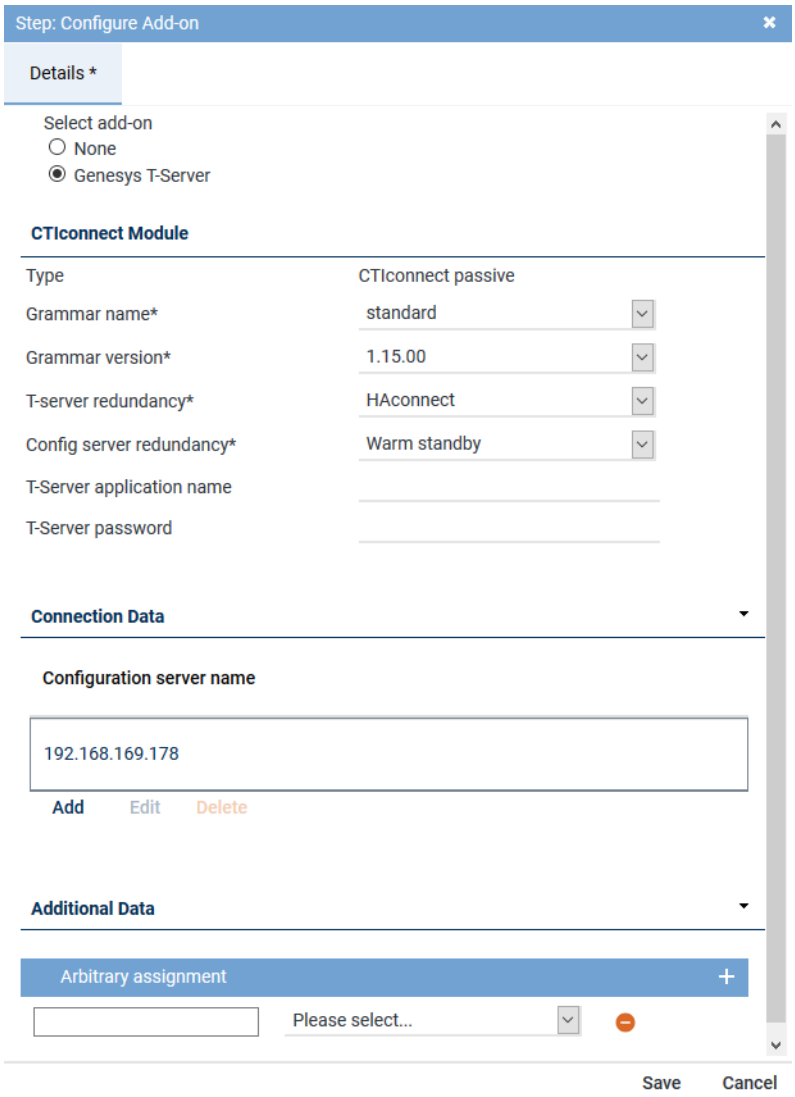


Fig. 209: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 49: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

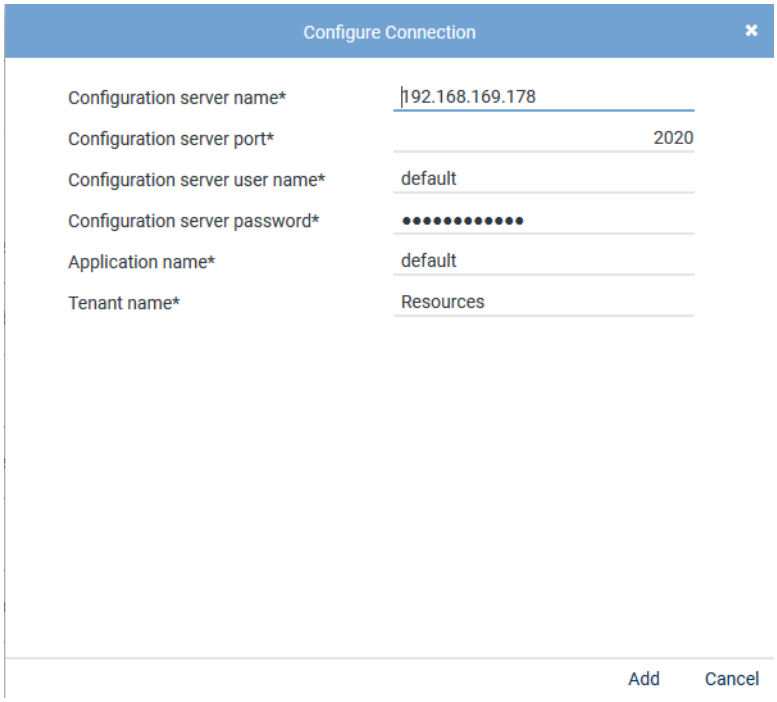


Fig. 210: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 50: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

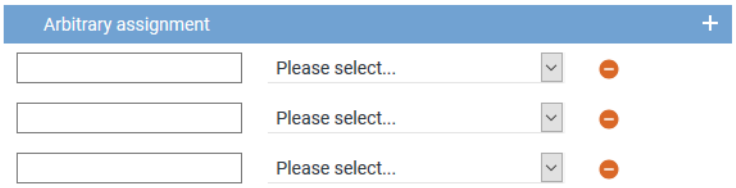


Fig. 211: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

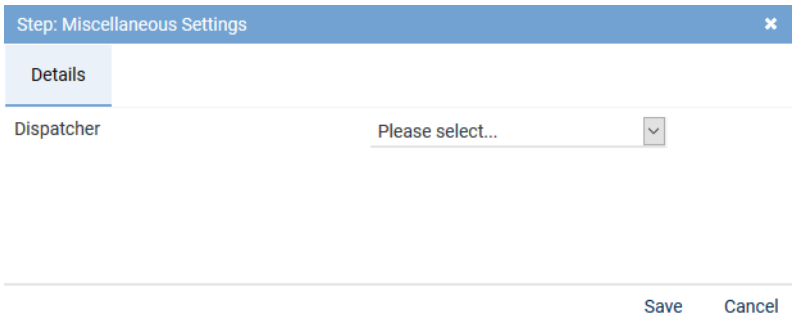


Fig. 212: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

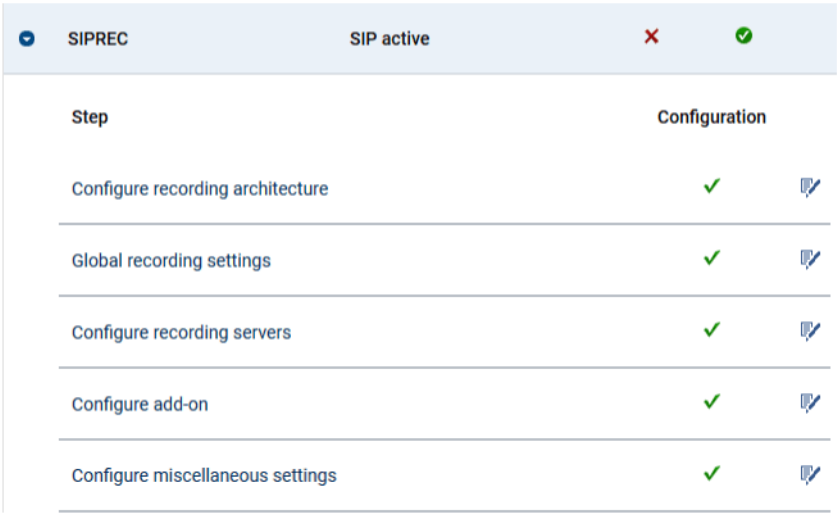


Fig. 213: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

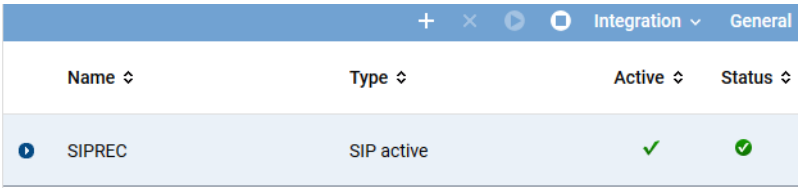


Fig. 214: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

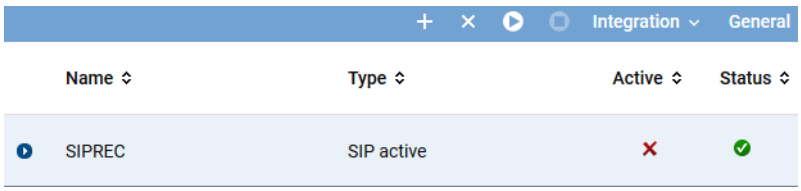


Fig. 215: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.2.4 Configure recording solution Multi-Server Recording

7.1.2.4.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

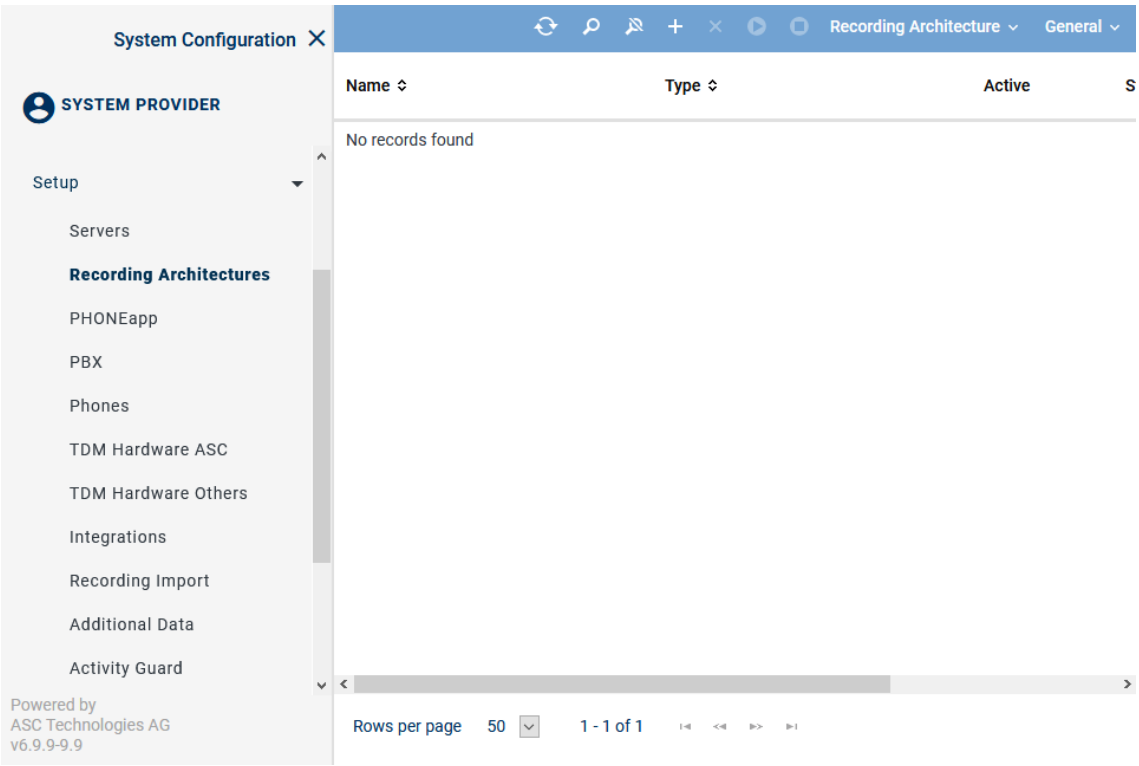


Fig. 216: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 217: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Create recording architecture Multi-Server Recording

If there are several recording servers which are supposed to record different trunks, you must create a recording architecture of the type *Multi-Server Recording*.

1. To create a new recording architecture, click on the icon + *(Create)* in the toolbar of the main view.
   ⇨ The window *New Recording Architecture* appears.

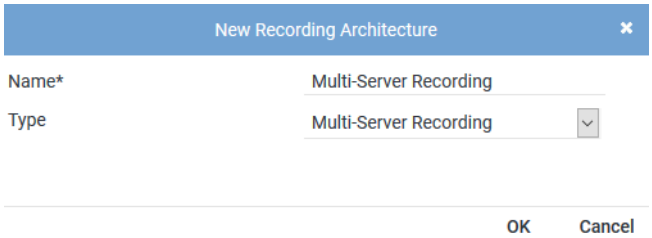


Fig. 218: Create recording architecture - Multi-Server Recording

2. In the entry field *Name*, enter a descriptive name for the recording architecture.

3. From the drop-down list *Type*, select the recording architecture type *Multi-Server Recording*.
   NOTICE! Only the supported recording architecture types are displayed in the drop-down list.
4. Click on the button *OK*.
   ⇨ The entries now appear in the detail view.

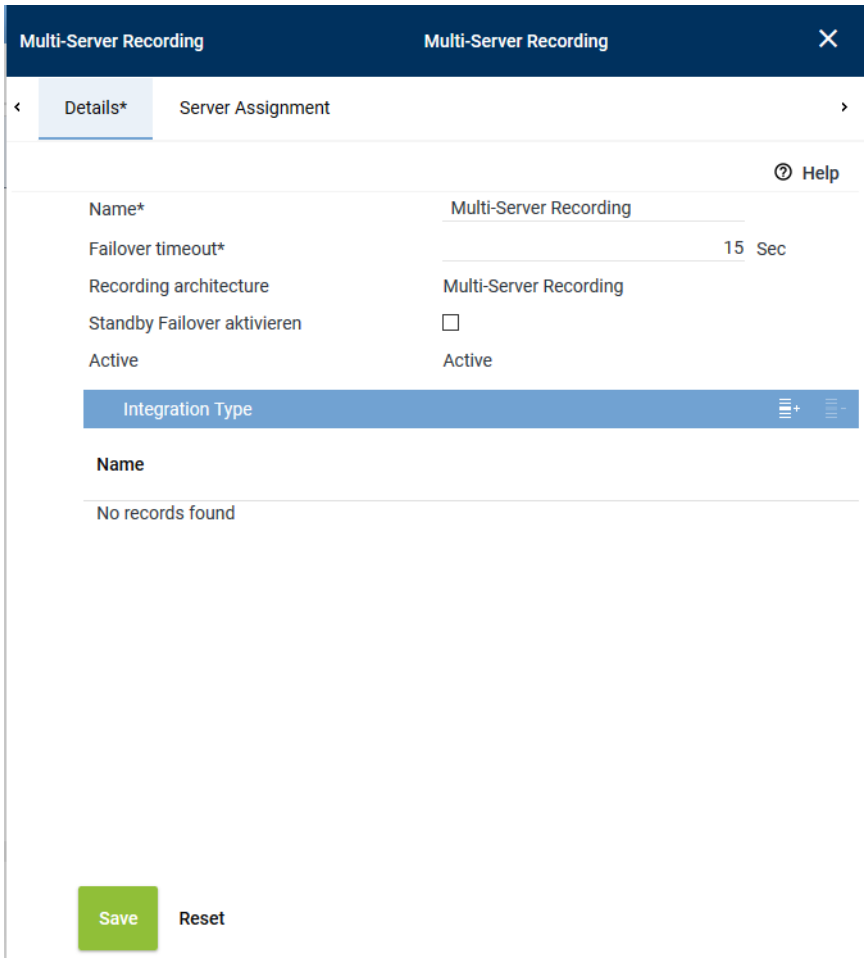


Fig. 219: Recording architecture - tab Details - Multi-Server Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture.

ⓘ Set the failover timeout to a minimum of 15 seconds until the failover process is initiated. Depending on the system architecture it may be useful to set the timeout even higher. The timeout defines how long to wait until the failover process is started. If the state switches back to *OK* within this time, the failover process is not initiated.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 220: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for Multi-Server Recording

1. Click on the tab *Server Assignment* to configure the distribution of the recording components for the recording architecture *Multi-Server Recording*.

Group field Recording Control and CTI*connect*

In this group field, you can configure recording control. You can configure two different servers or the same server for this.

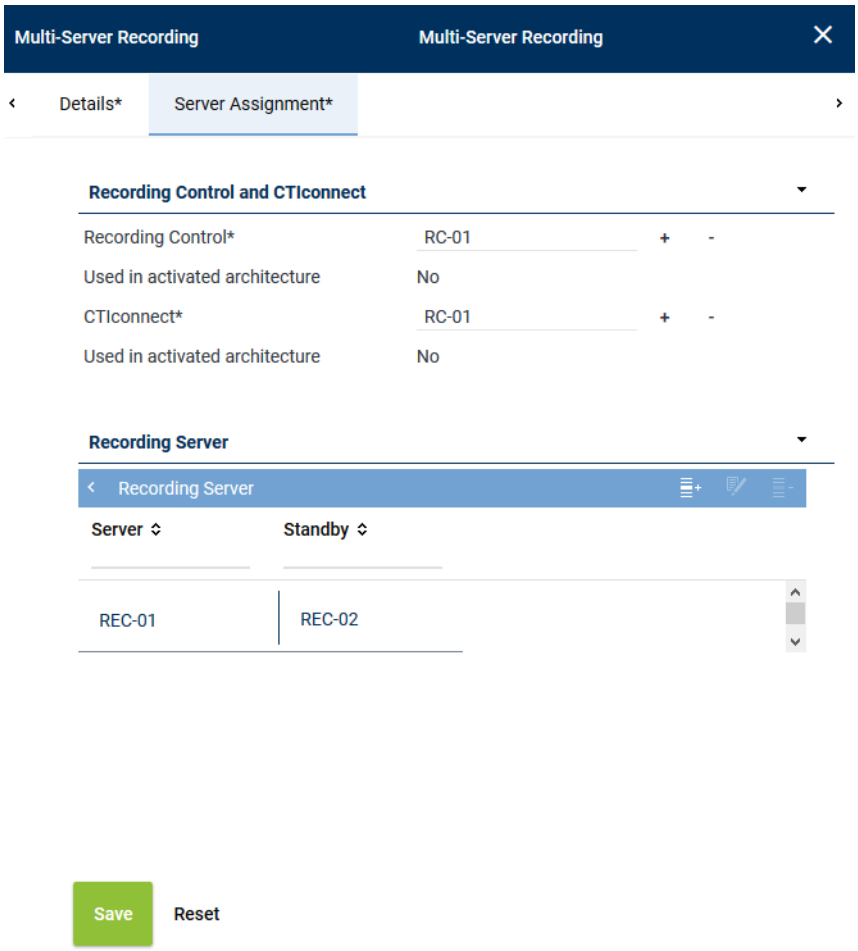


Fig. 221: Recording architecture - tab Server Assignment

1. Click on the button next to the entry field *Recording Control*.
   ⇨ The window *Servers* appears.

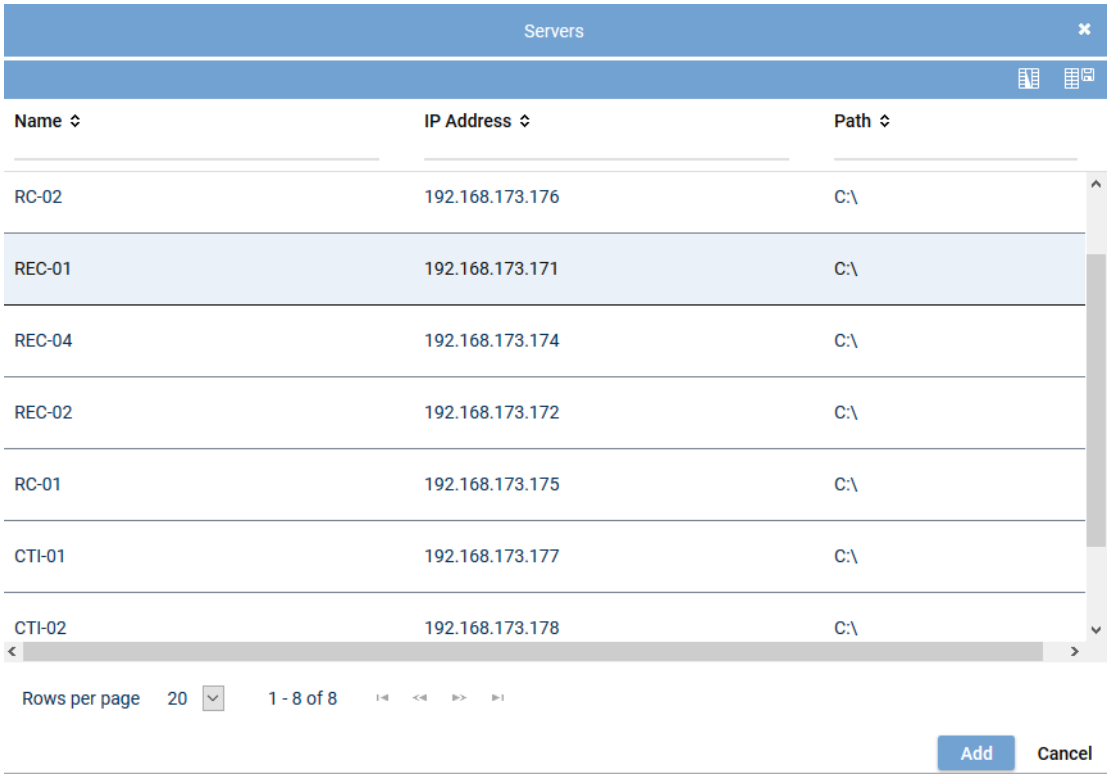


Fig. 222: Recording architecture - assign server - example

2. Select the server for the *Recording Control module*.
3. Click on the button *Add*.
   ⇨ The name of the server appears in the detail view.
4. To delete an assignment, click on the icon - .

A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the CTI*connect module* in the entry field CTI*connect*.

Group field Recording Server

1. In the table headline *Recording Server*, click on the icon .
   ⇨ The following window appears:

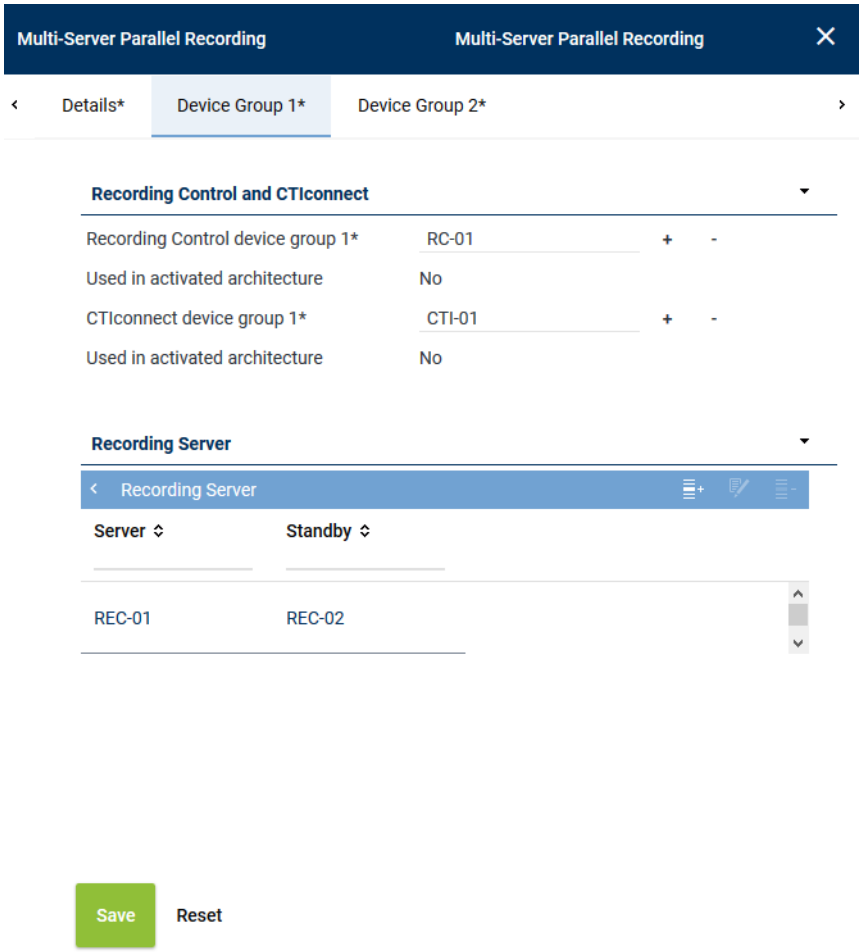


Fig. 223: Add recording server

2. Following the steps described above, go to the entry field *Primary server* and click on the icon + to select the primary server where recording is supposed to be active.
3. In the entry field *Standby server*, click on the icon + to select the standby server which is supposed to do the recording in case of an error.
4. Tick the check box to activate the recording type you would like to use for this server.
   NOTICE! You can activate several recording types if the integration supports them and if the corresponding licenses have been installed.

5. Click on the button *OK* to close the window.
   ⇨ The name of the server appears in the detail view.
6. To edit the assignment subsequently, click on the icon .
   To delete an assignment, click on the icon .
7. If you would like to add additional recording servers repeat the steps described above.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the toolbar becomes active.
3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

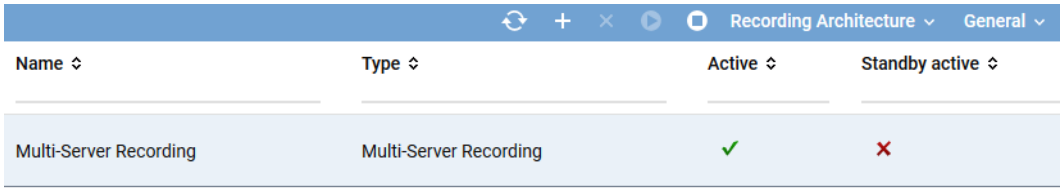


Fig. 224: Recording architecture - activate recording architecture

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✗ *(Inactive)* appears.

ⓘ The recording architecture must have been activated so that the integration can be configured.

ⓘ If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.4.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

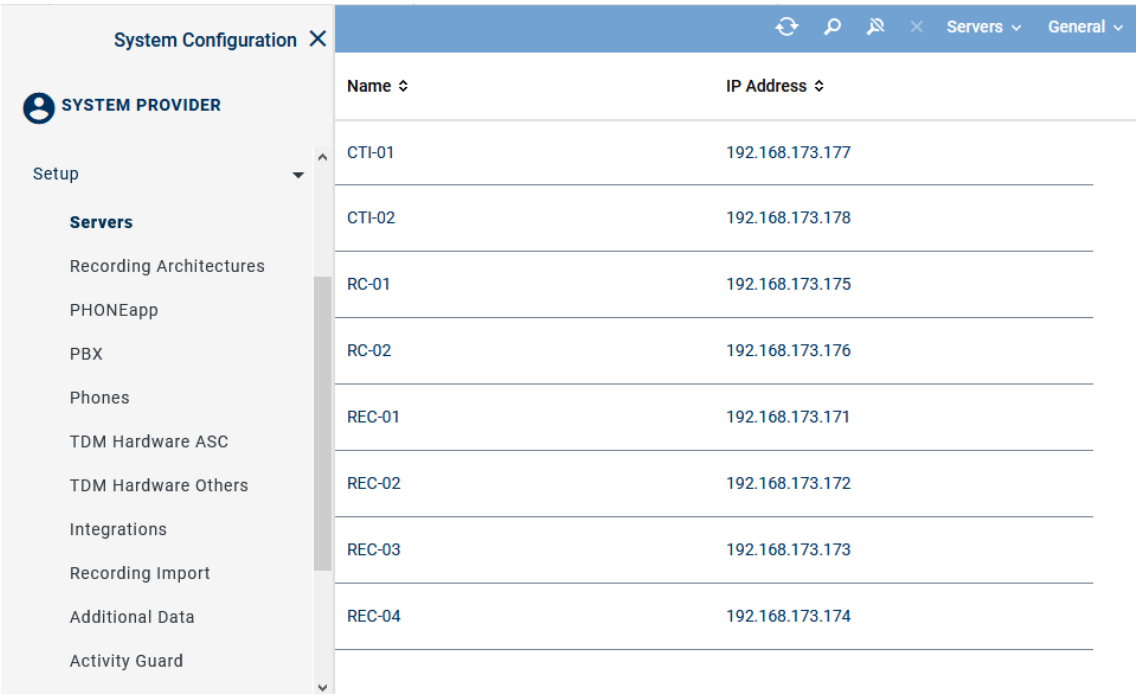


Fig. 225: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.
Path	Shows the path of the server.
Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 226: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.

Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 197.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.

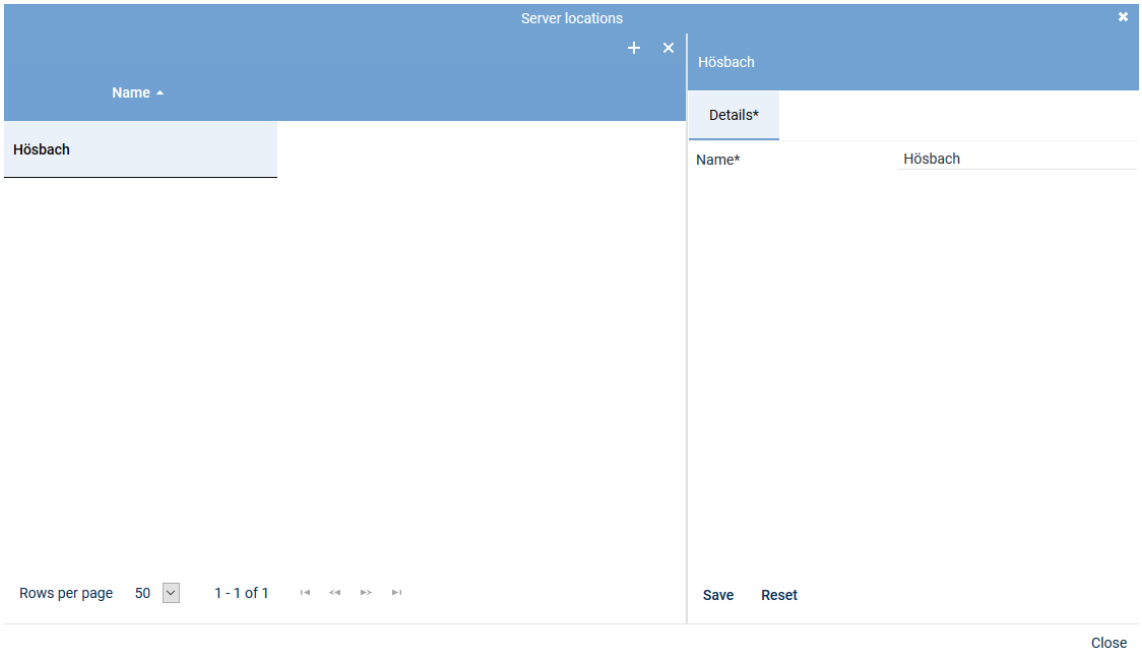


Fig. 227: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.

4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

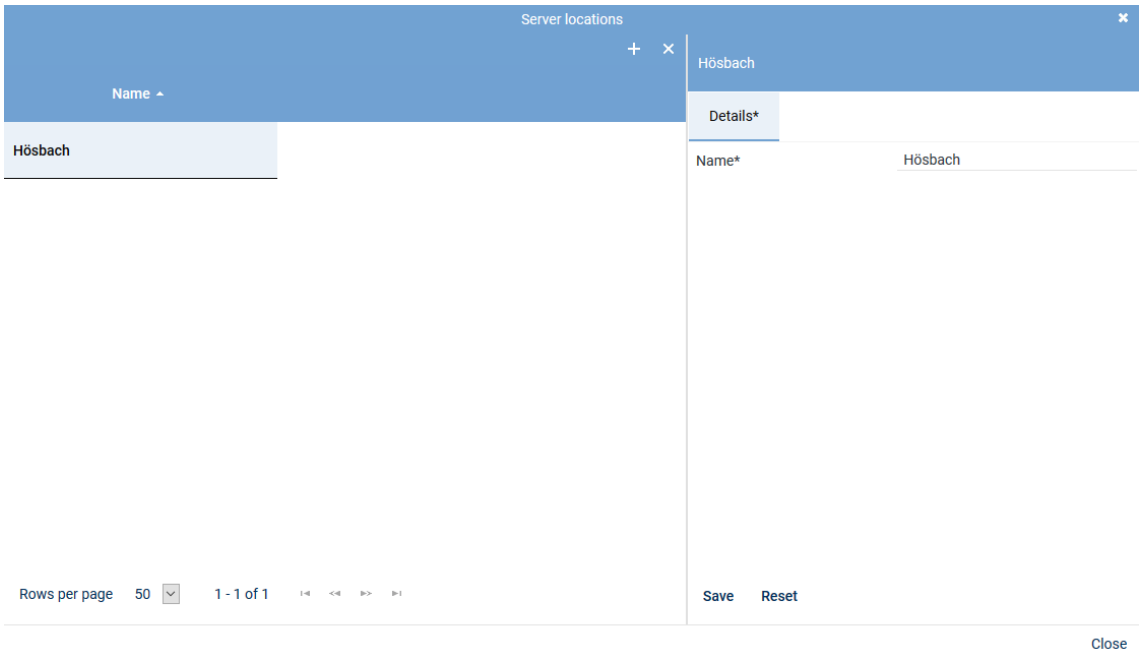


Fig. 228: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

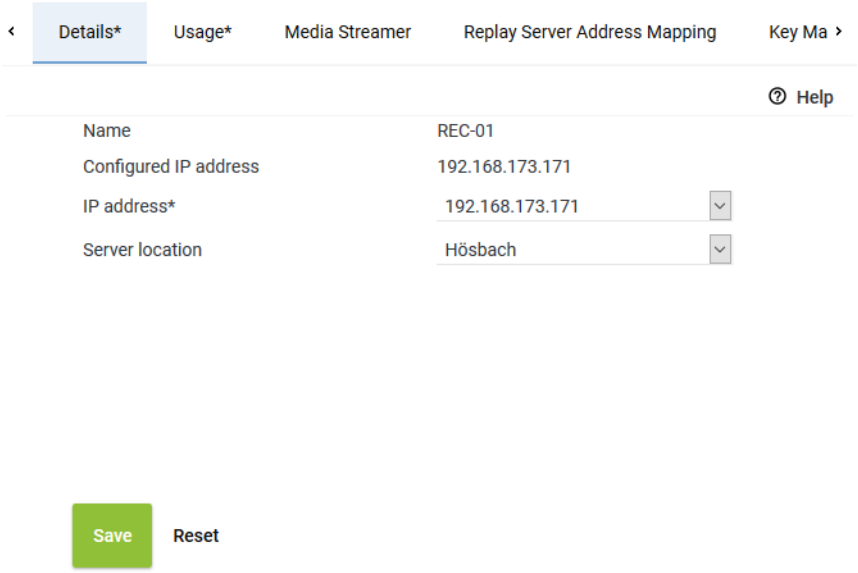


Fig. 229: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.
4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

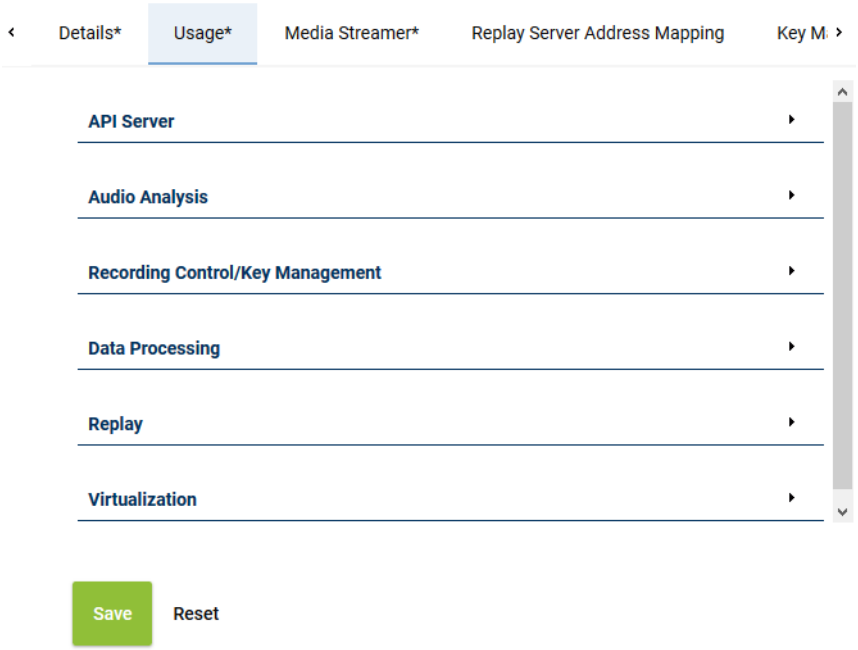


Fig. 230: Servers - tab usage

Group field API Server

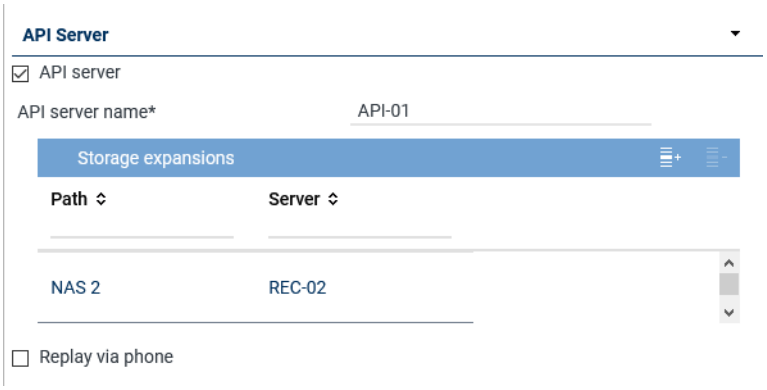


Fig. 231: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server. ☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 210.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List Storage expansions	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 201. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list.

Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 208. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

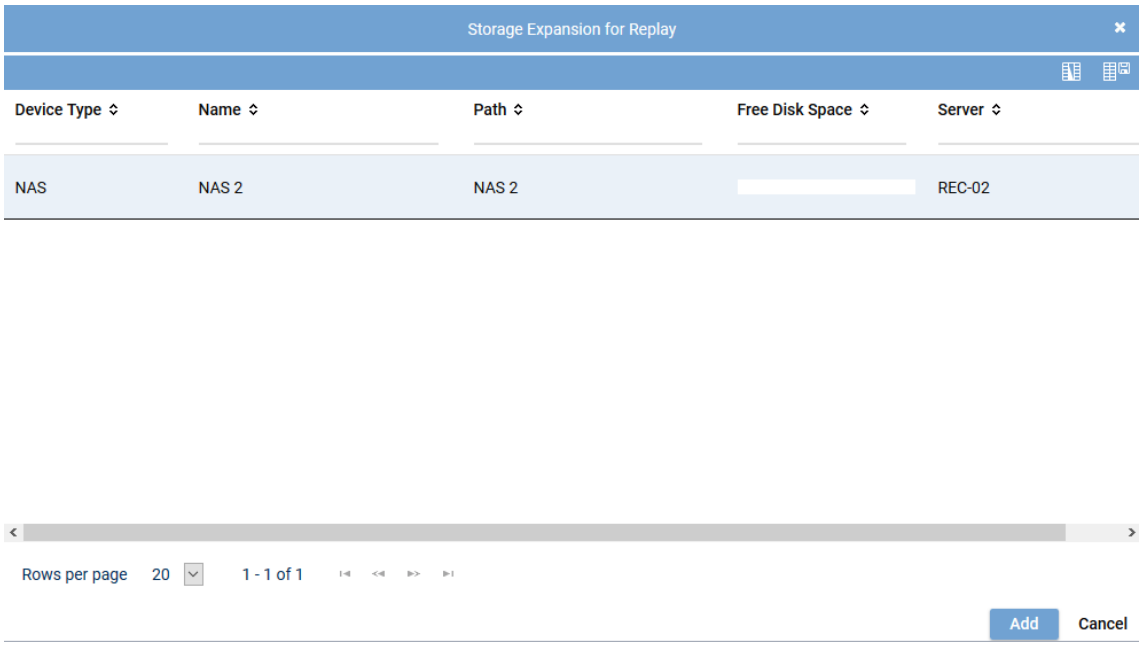


Fig. 232: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

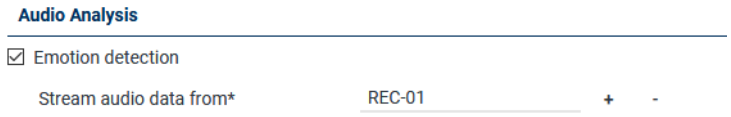


Fig. 233: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 51: Configure audio analysis

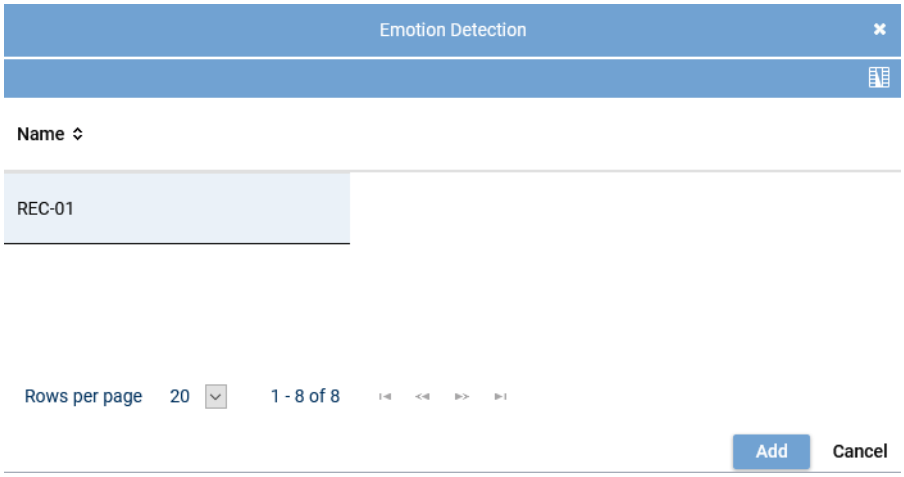


Fig. 234: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

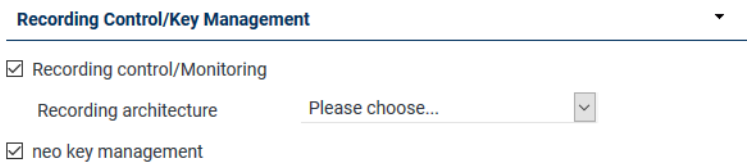


Fig. 235: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 52: Configure recording control/key management

Group field Data Processing

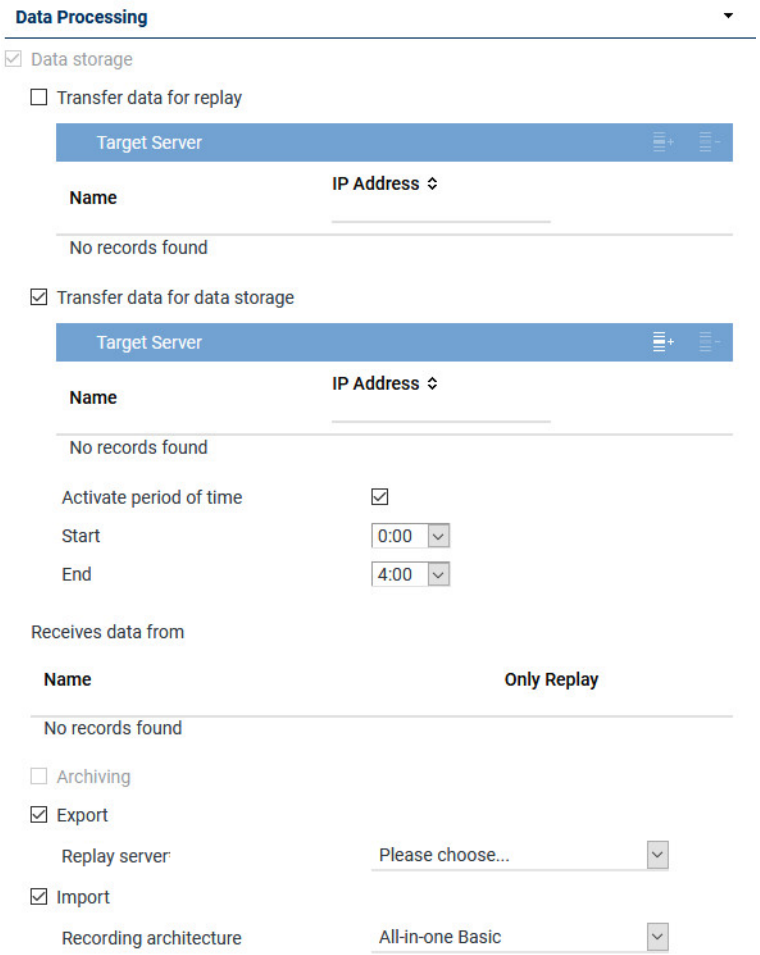


Fig. 236: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 205. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 205. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.

Parameter	Value/Description
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function. **NOTICE!** If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 53: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 237: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

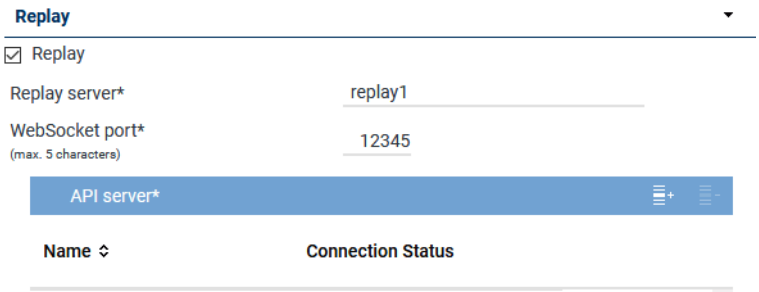


Fig. 238: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings:

Parameter	Value/Description
	• By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 207. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 54: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.
- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

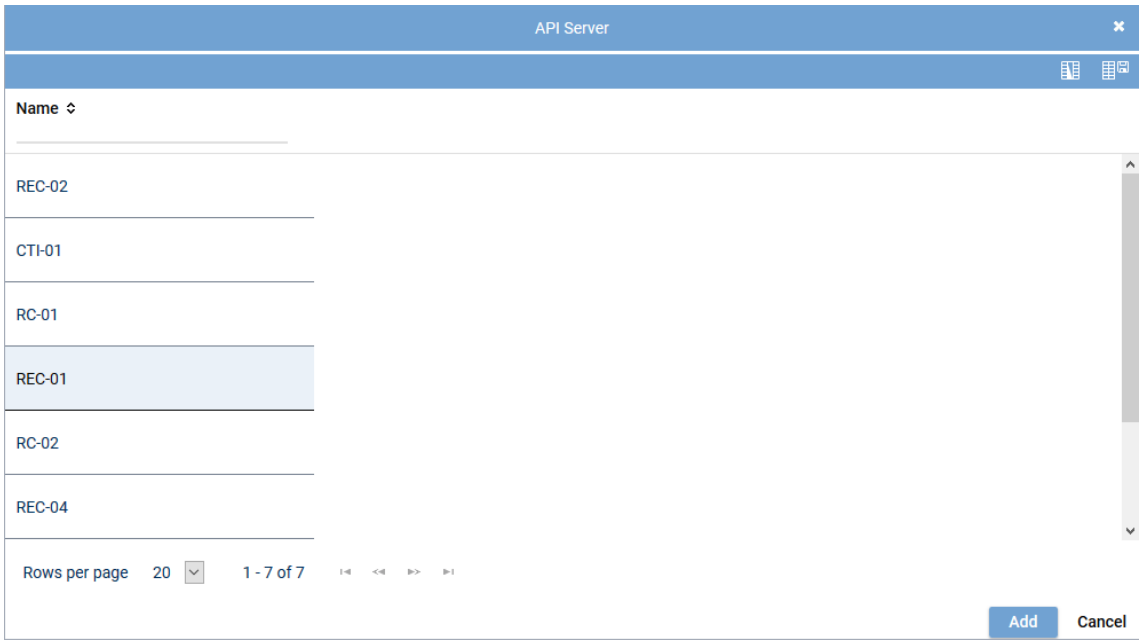


Fig. 239: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 200.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 240: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management. • *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 55: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

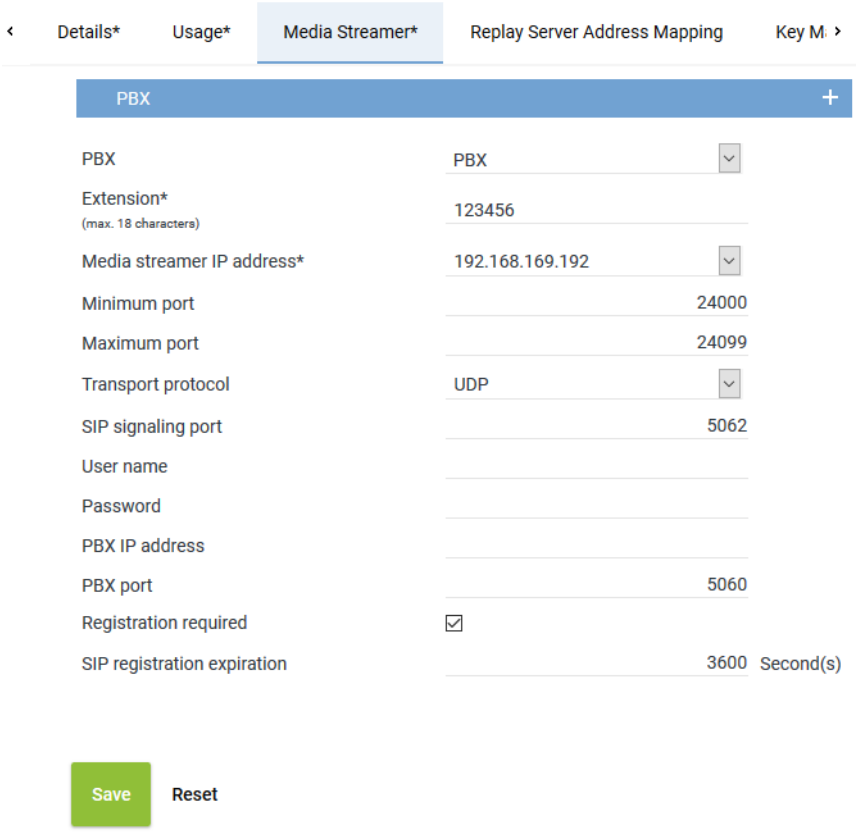


Fig. 241: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system. If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 215.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number.

	A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

ⓘ The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

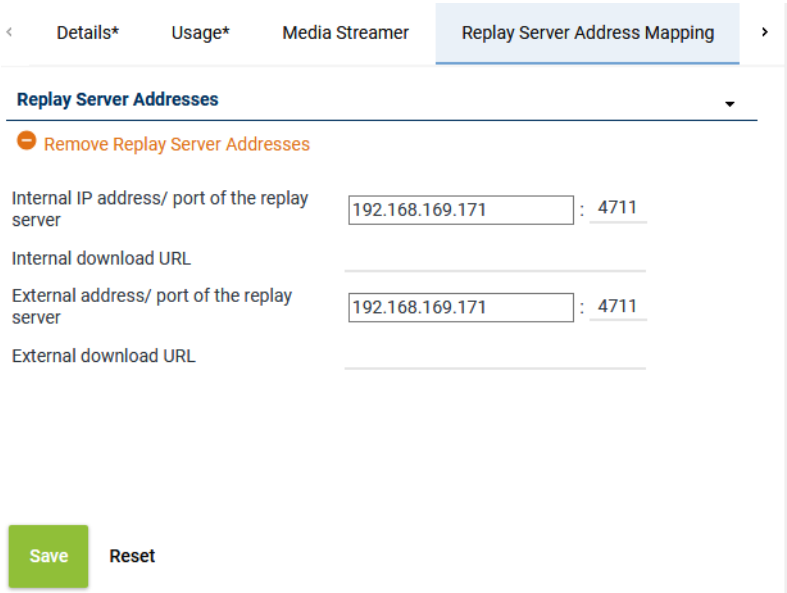


Fig. 242: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

ⓘ If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

ⓘ To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

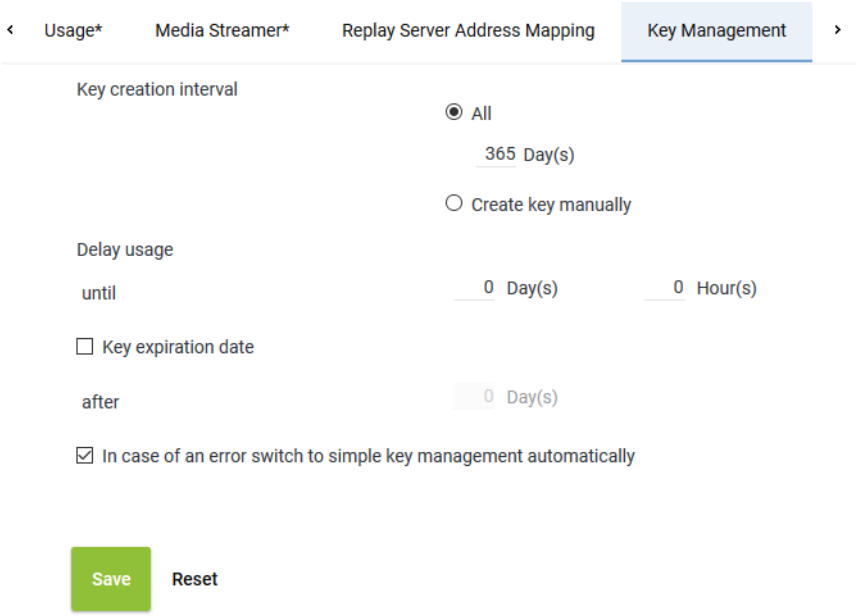


Fig. 243: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.
Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid.

	☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.
  In this case, no separate configuration is required.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

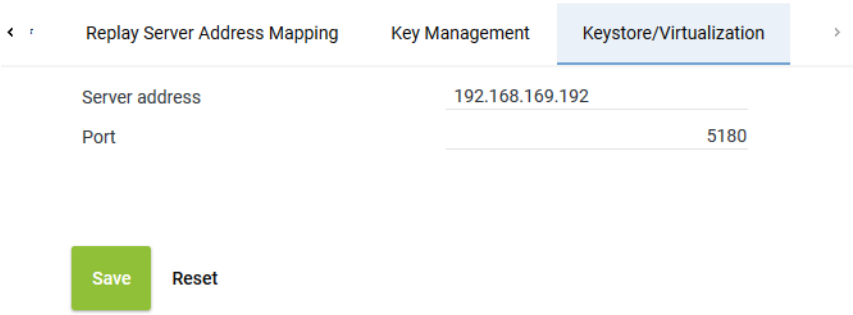


Fig. 244: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management: IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.4.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

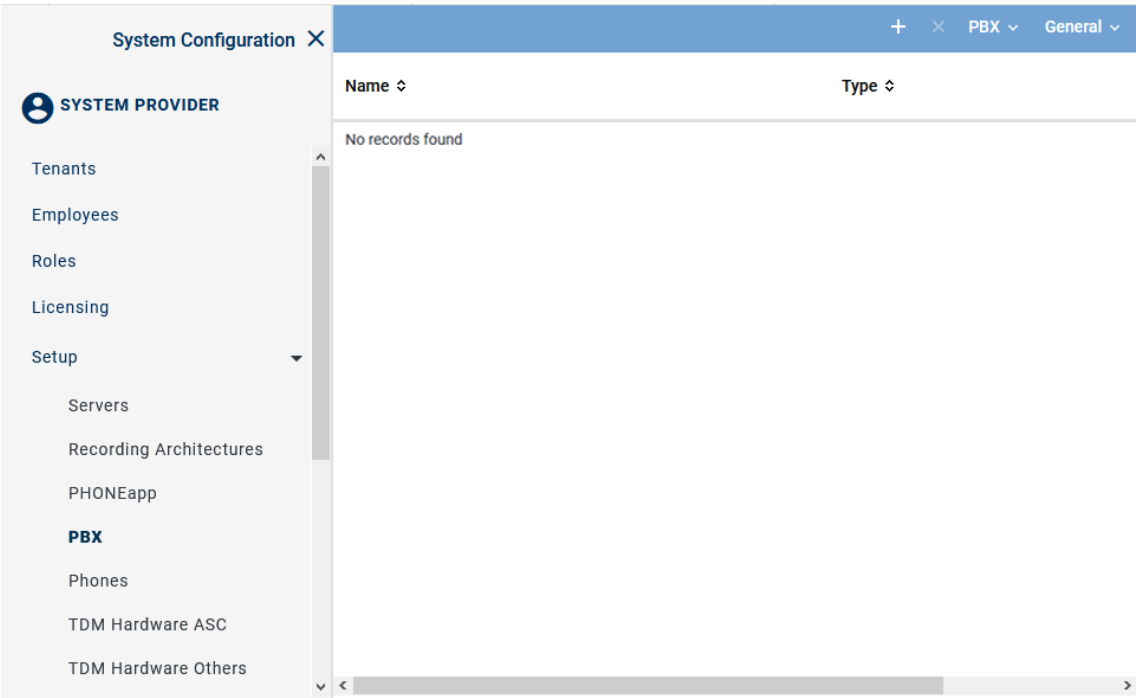


Fig. 245: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 246: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.

Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

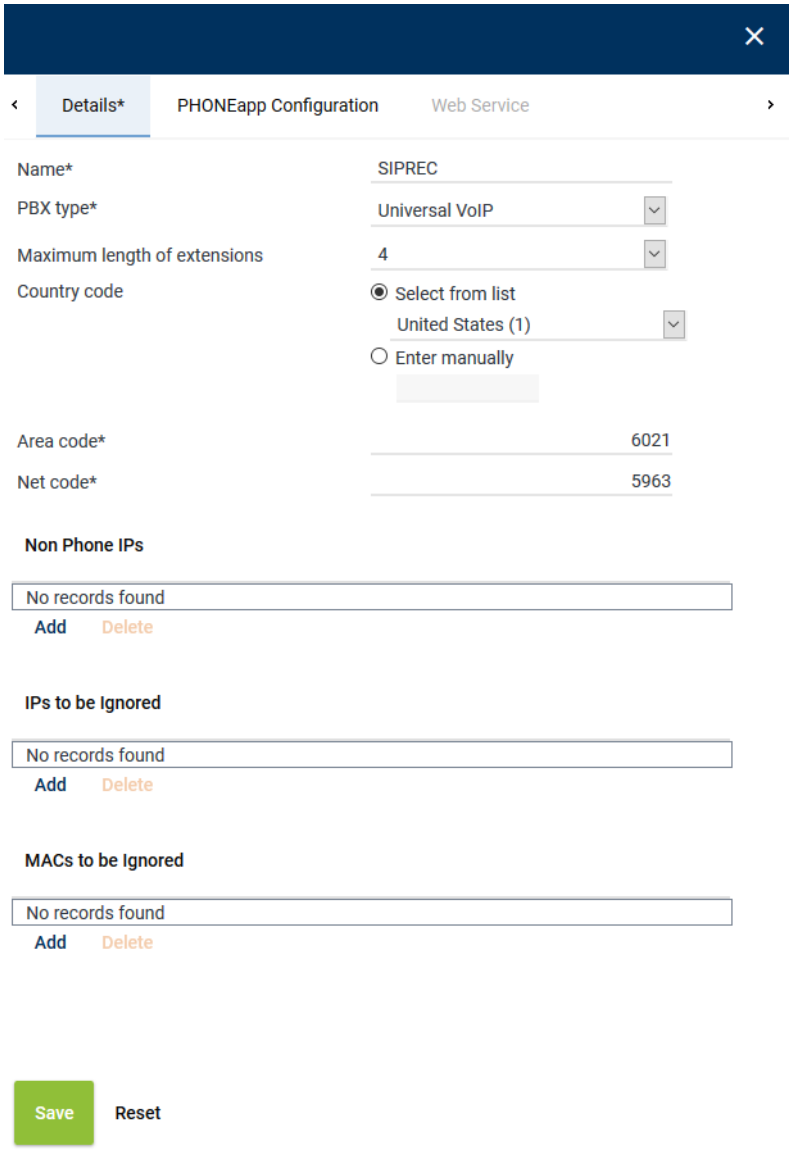


Fig. 247: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list*

Parameter	Value/Description
	Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 56: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 57: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.4.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

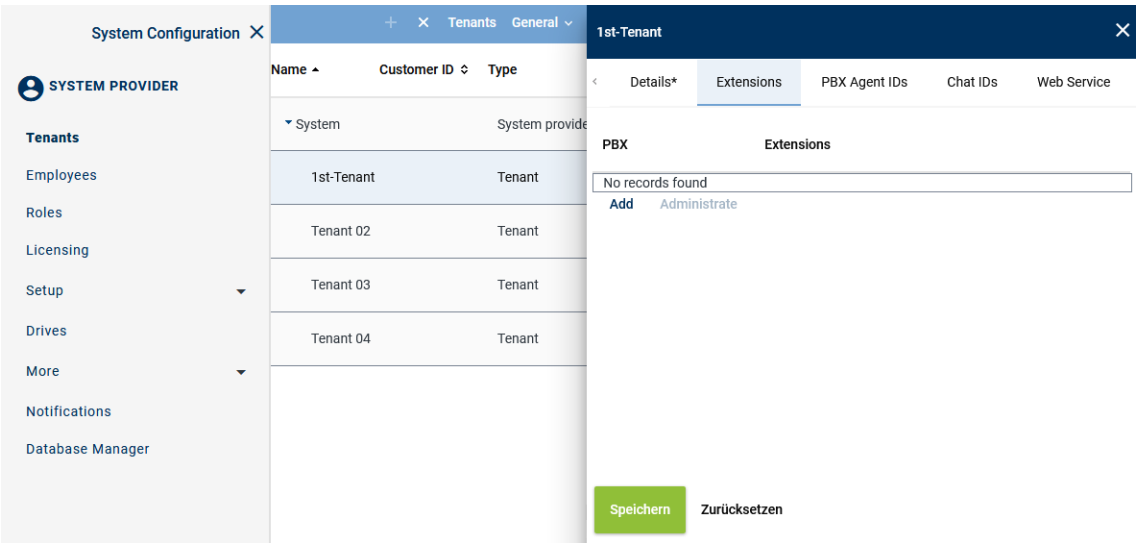


Fig. 248: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.
   ⇨ The following window appears:

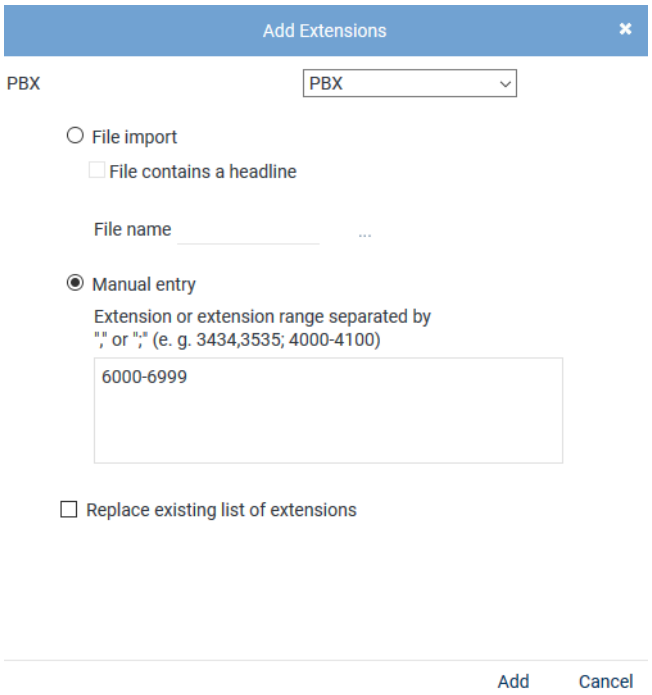


Fig. 249: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT*

	• *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually. To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

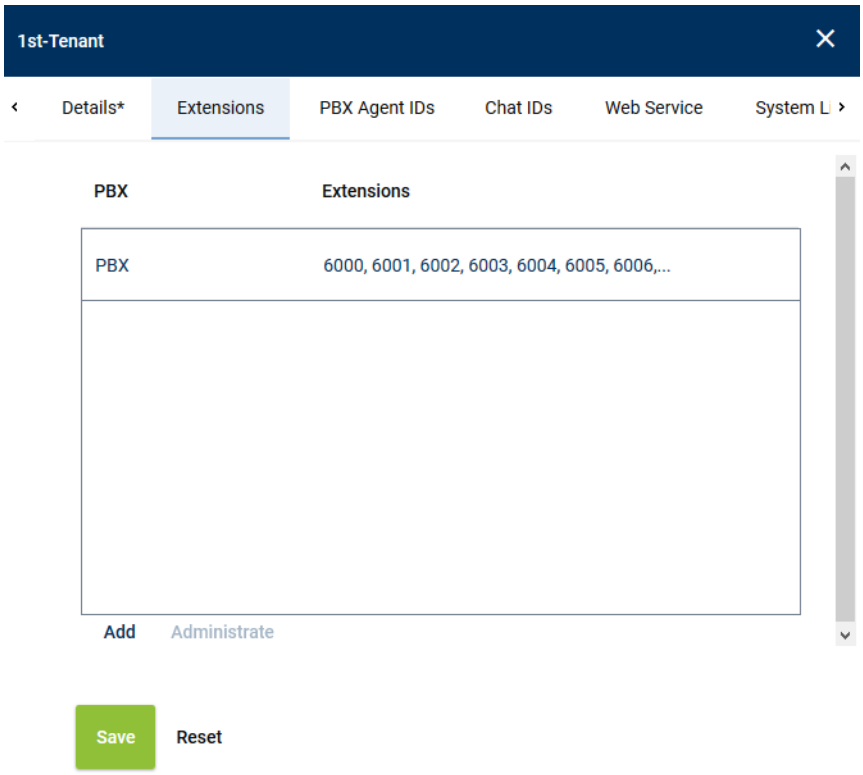


Fig. 250: Remove extensions

2. Click the button *Administrate*.
3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 251: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

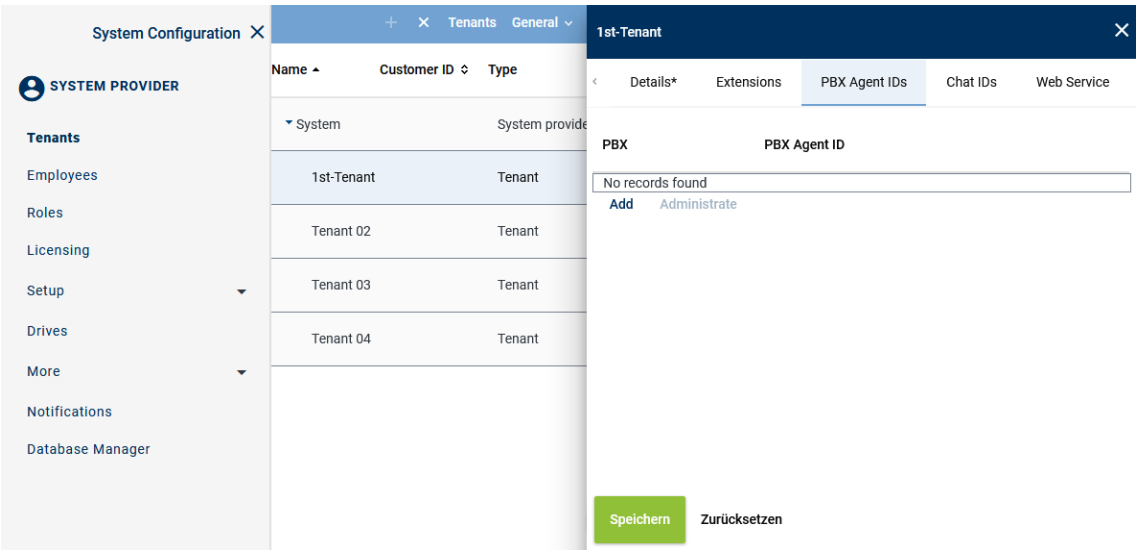


Fig. 252: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

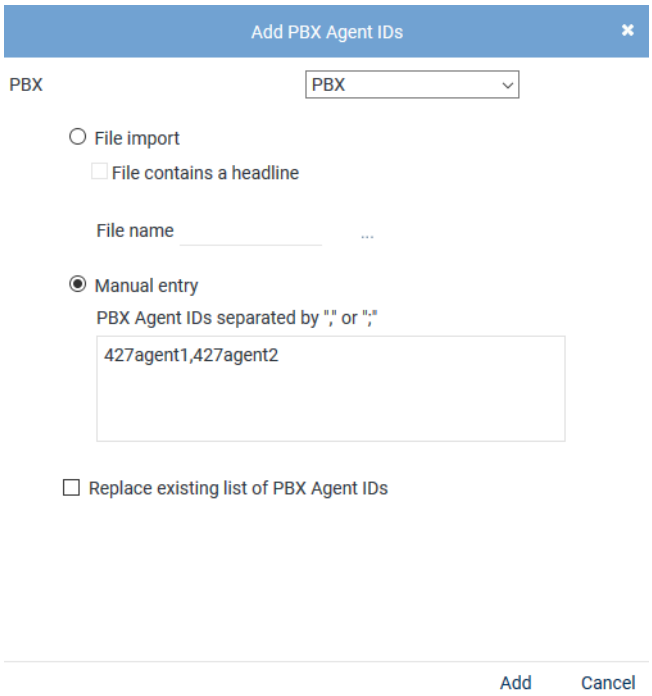


Fig. 253: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

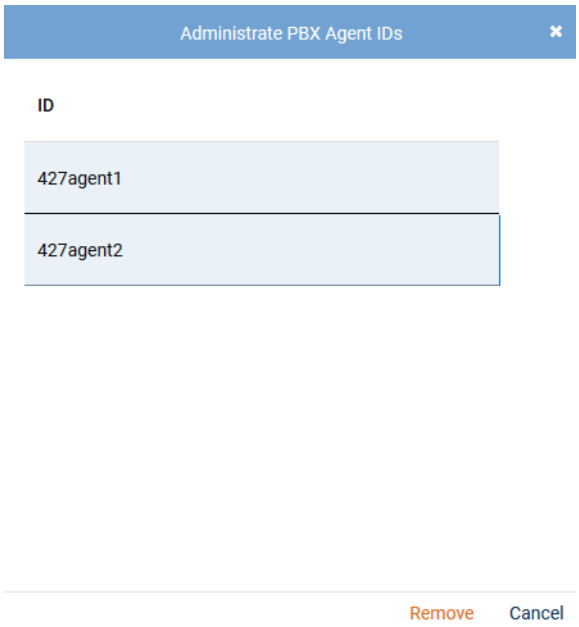


Fig. 254: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.4.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

ⓘ In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

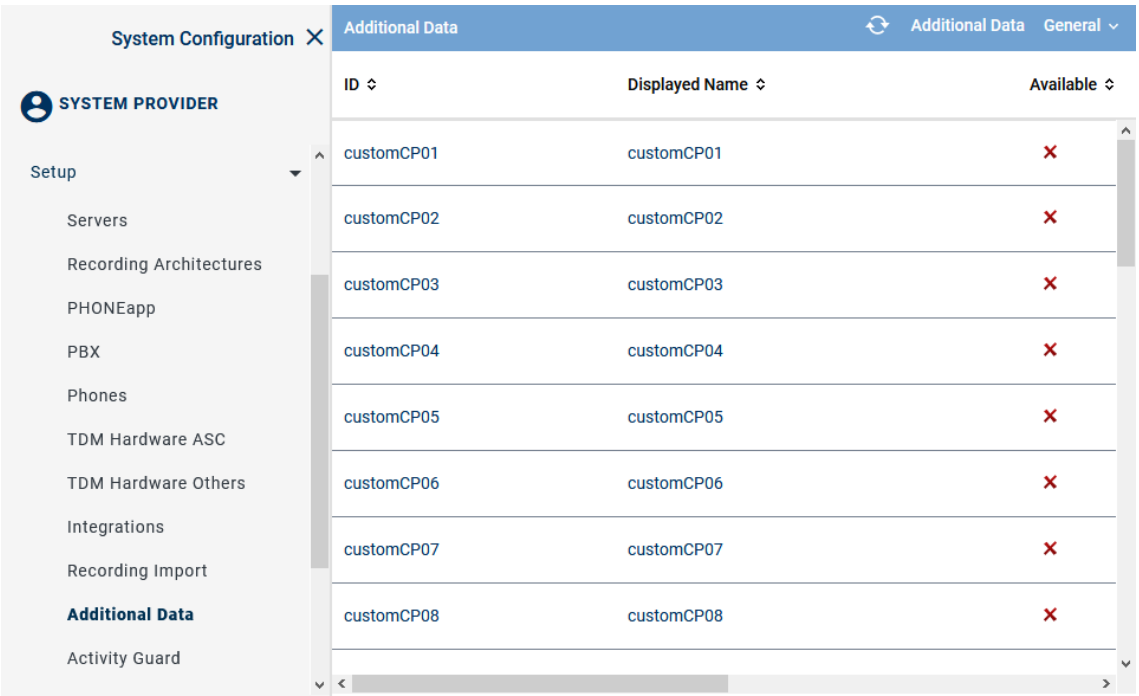


Fig. 255: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

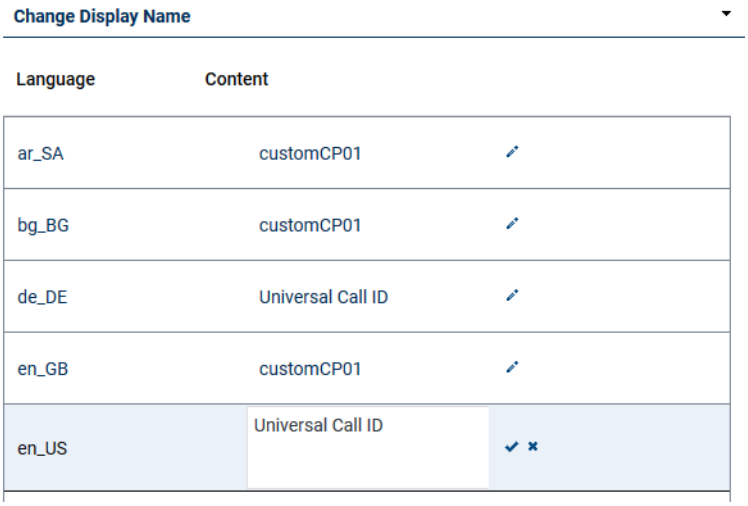


Fig. 256: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 257: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.4.6 Create integration for Multi-Server Recording

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

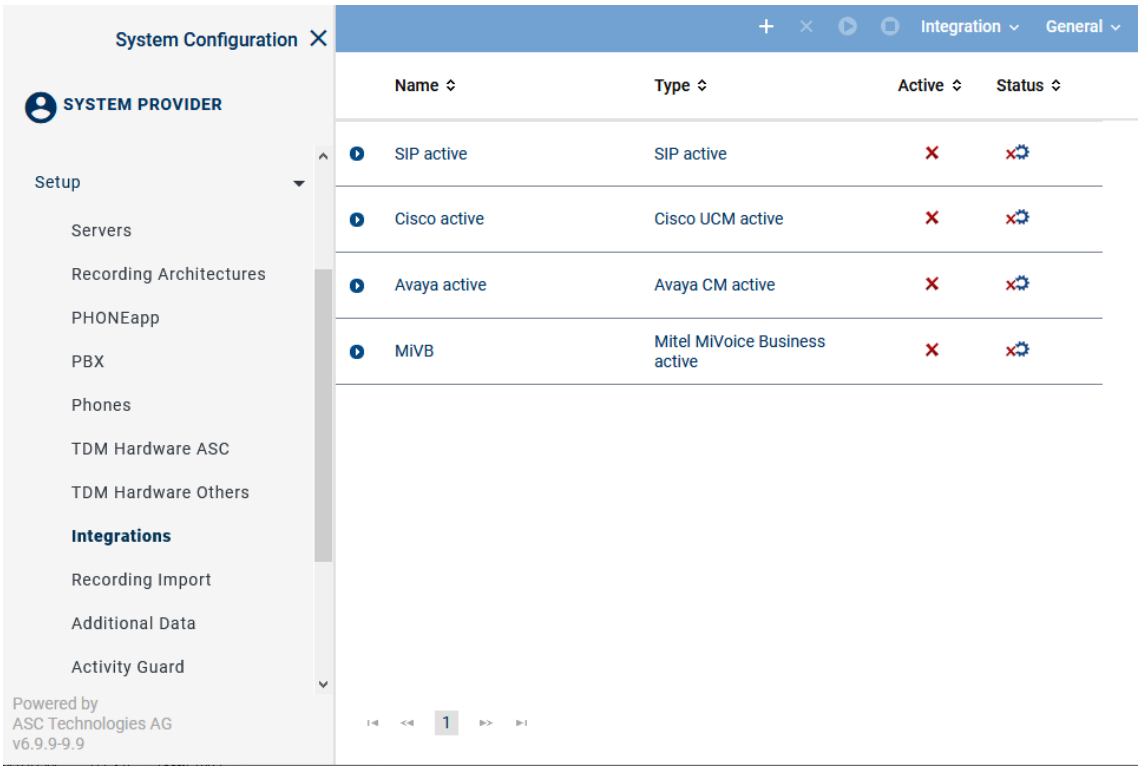


Fig. 258: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 259: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

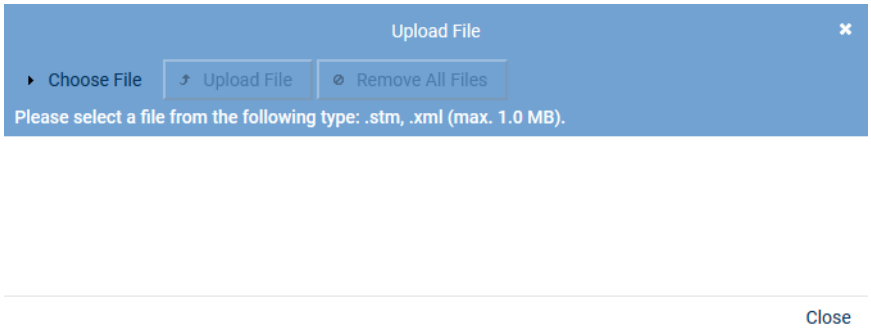


Fig. 260: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

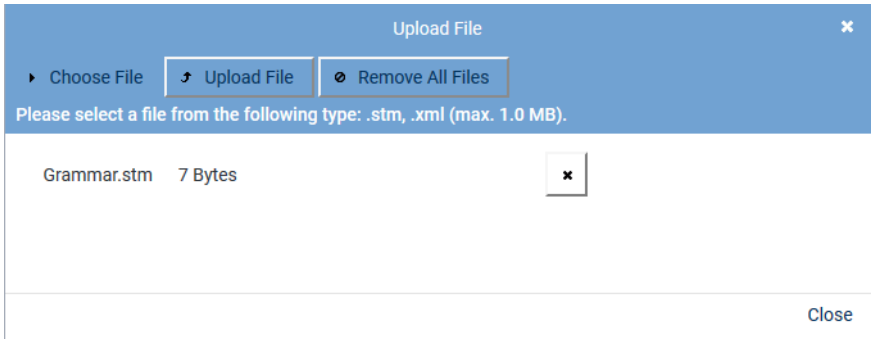


Fig. 261: Upload grammar

5. To remove a selected file from the list, click on the button ✖ *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 262: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 58: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 263: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for Multi-Server Recording

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

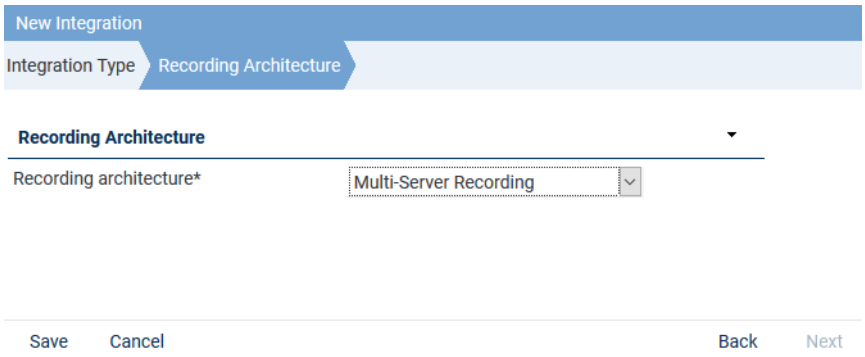


Fig. 264: Assign recording architecture - Multi-Server Recording

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

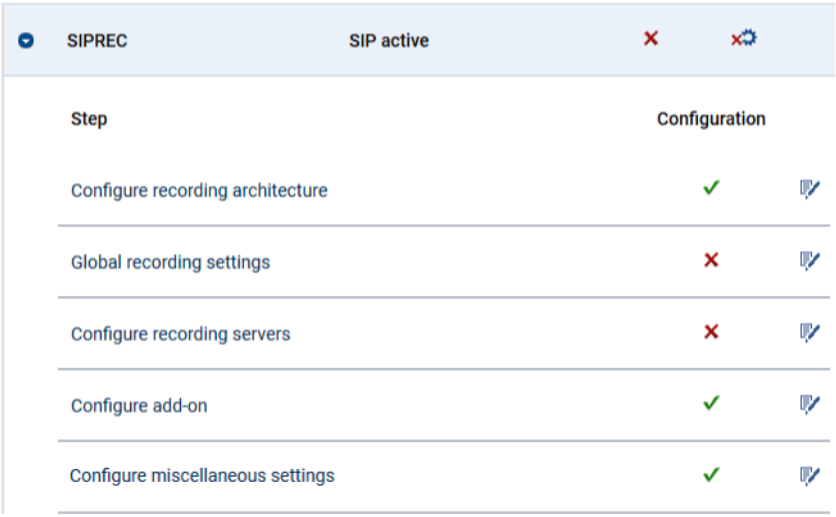


Fig. 265: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

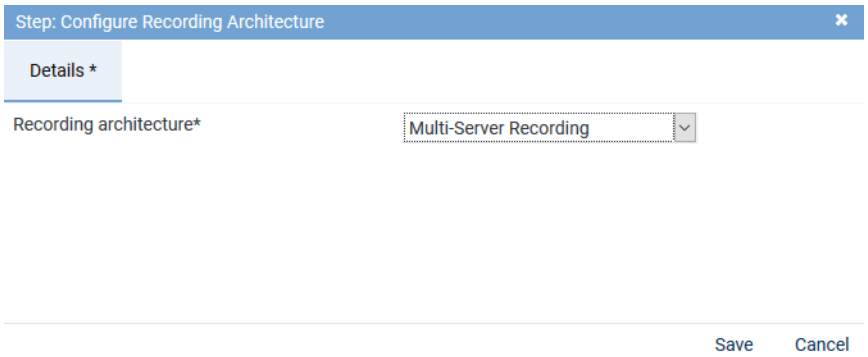


Fig. 266: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for Multi-Server Recording

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.
   ⇨ The window *Step: Global Recording Settings* appears.

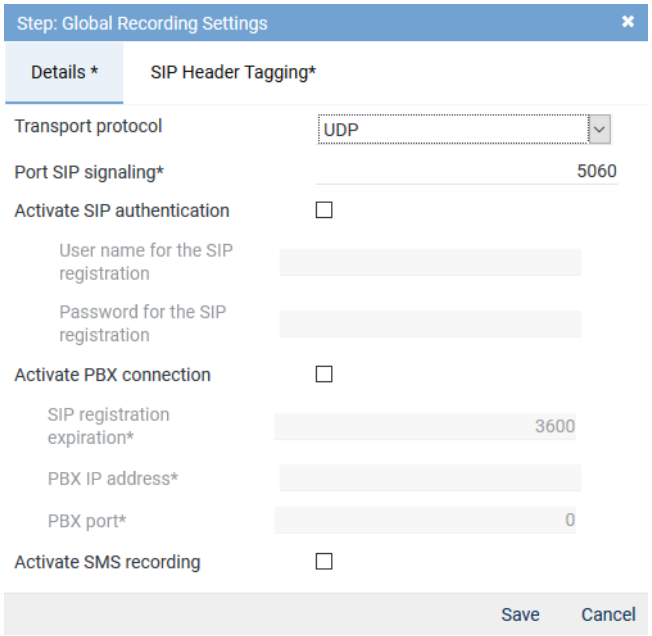


Fig. 267: Configuration step - Global Recording Settings - All-in-one Basic Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	Select the transport protocol *UDP* for the SIP signaling between the recording server and the PBX.
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*
Activate SIP authentication	Deactivate this option for this recording solution.

Parameter	Value/Description
Activate SMS recording	This function is not supported in this recording solution.

Tab. 59: Global recording settings

3. To save the entries, click on the button *Save*.
   To discard entries, click on the button *Cancel*.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

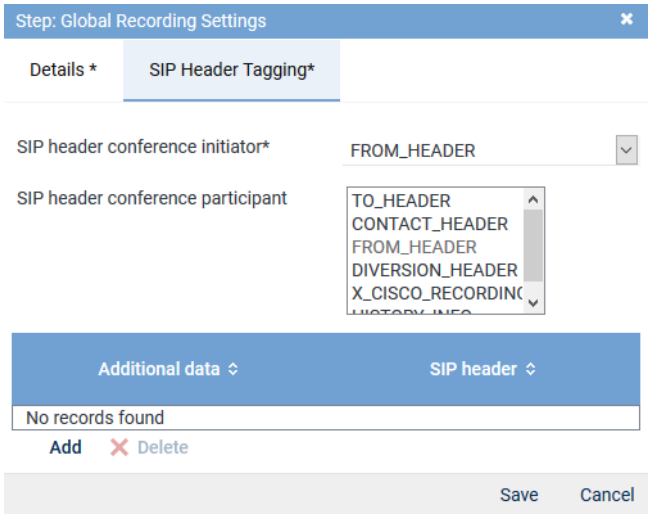


Fig. 268: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.
   ⇨ The window *SIP Additional Data* appears.

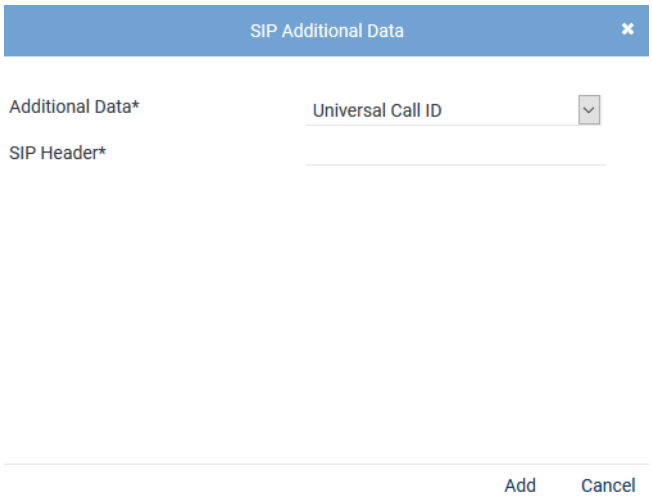


Fig. 269: SIP Additional Data

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted. To have ASC configure the mapping file, contact your distribution partner.

Tab. 60: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for Multi-Server Recording

When using several recording servers, you must configure the port range for each recording server separately. The range may be the same for all recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

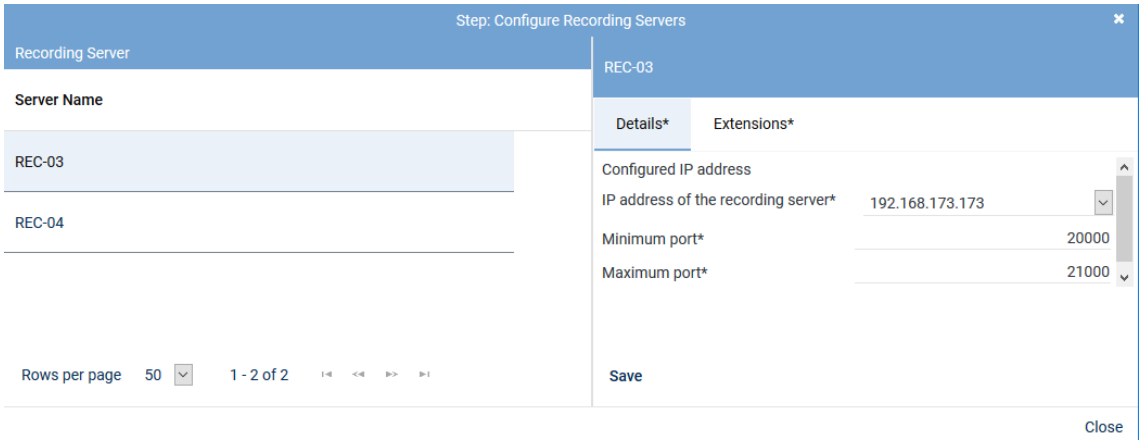


Fig. 270: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.

Parameter	Value/Description
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 61: Configure recording servers

For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.

In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Tab Extensions

1. Click on the tab *Extensions*.

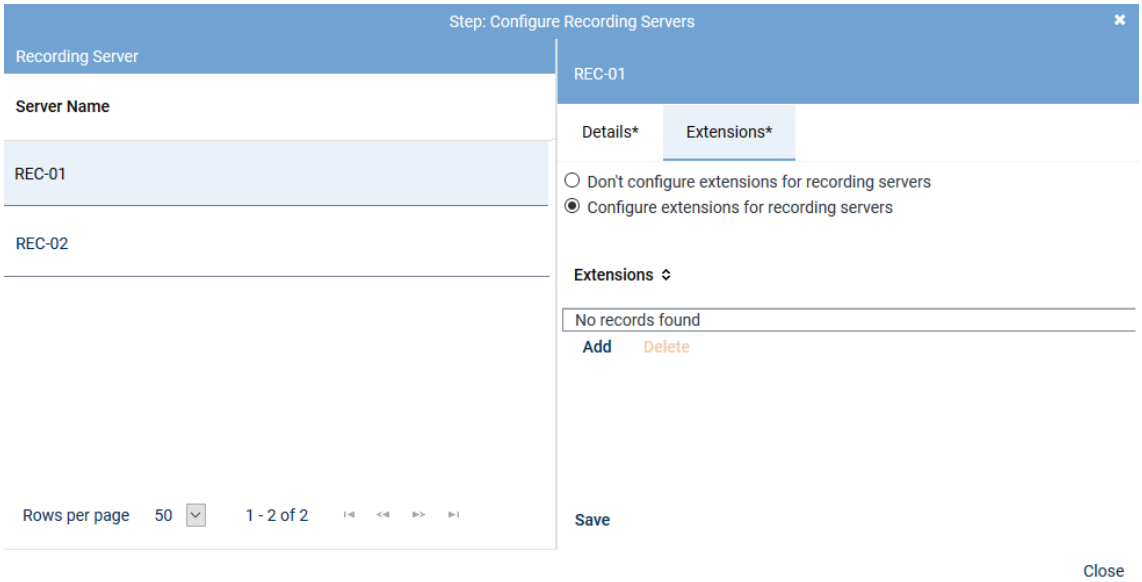


Fig. 271: Tab Extensions

The following options are available:

Configure no extensions for recording servers	Activate this option if you have not configured the extensions for the recording server in the PBX.
Configure extensions of the recording server	Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

2. To add extensions, click on the button *Add* in the table *Extensions*.
   ⇨ The window *Add Extensions* appears.

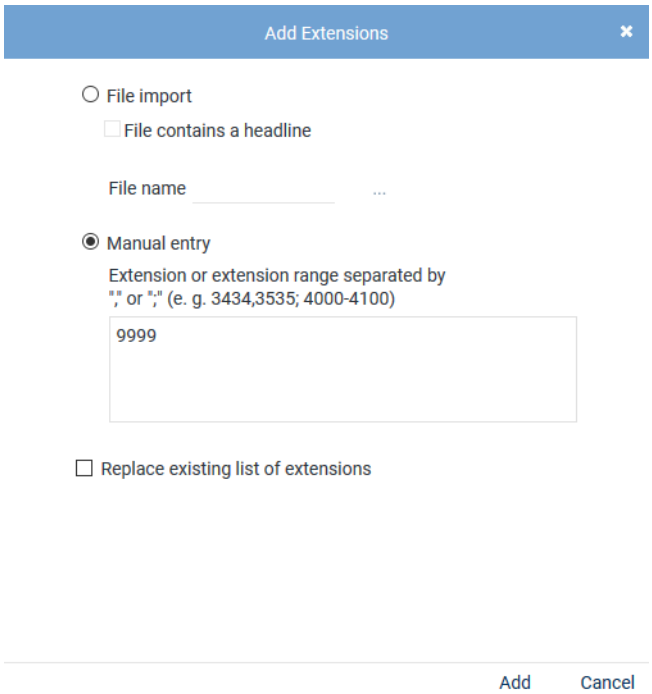


Fig. 272: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

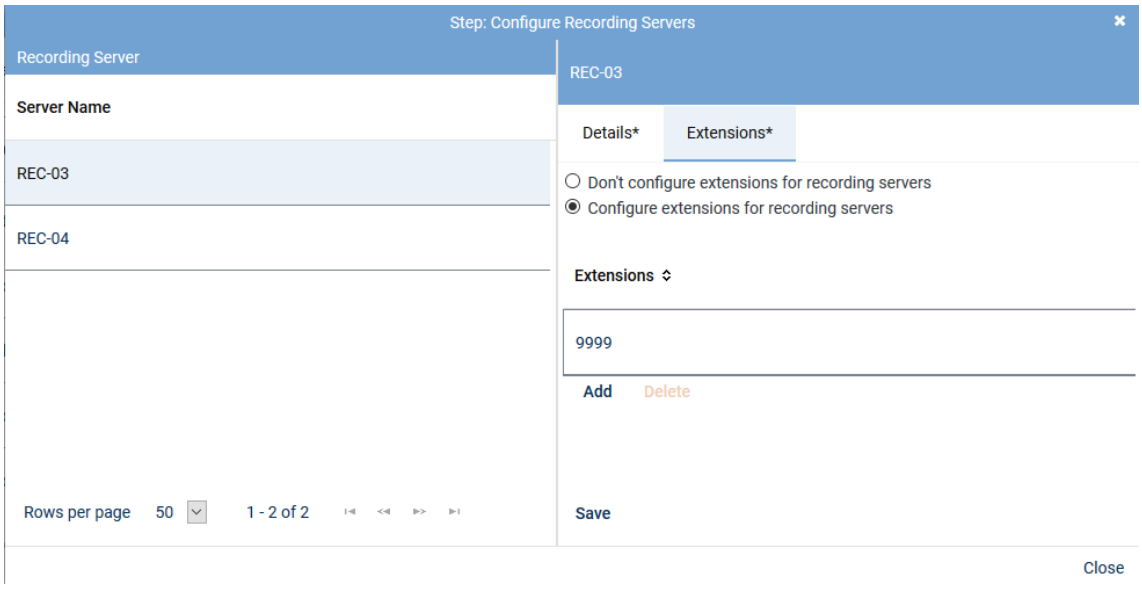


Fig. 273: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.
8. Click on the button *Save*.

9. Click on the button *Close* to finish this configuration step.

Configure add-on

The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

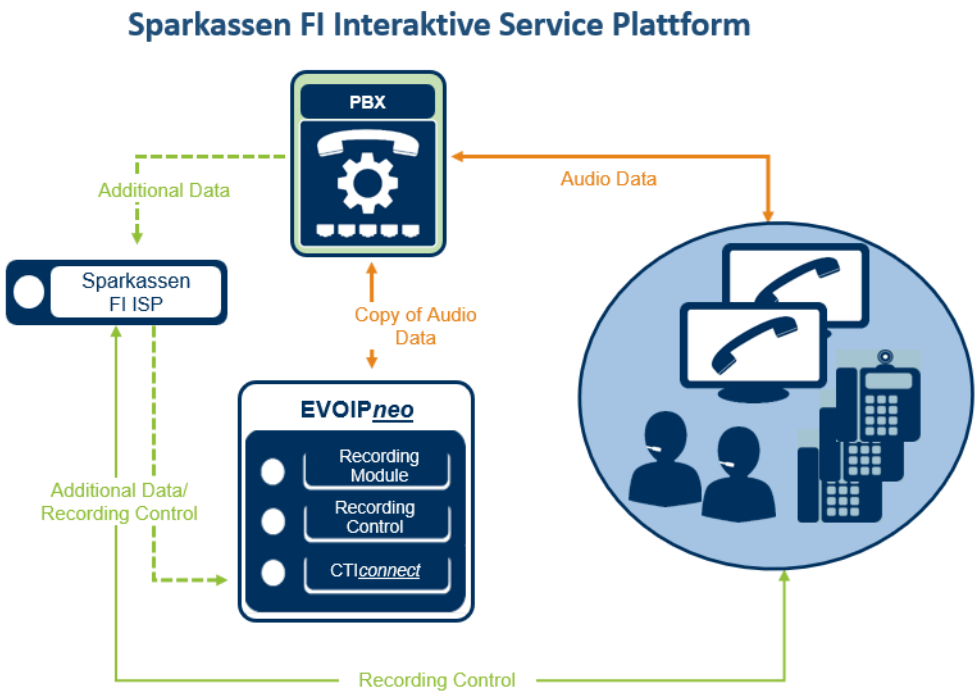


Fig. 274: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

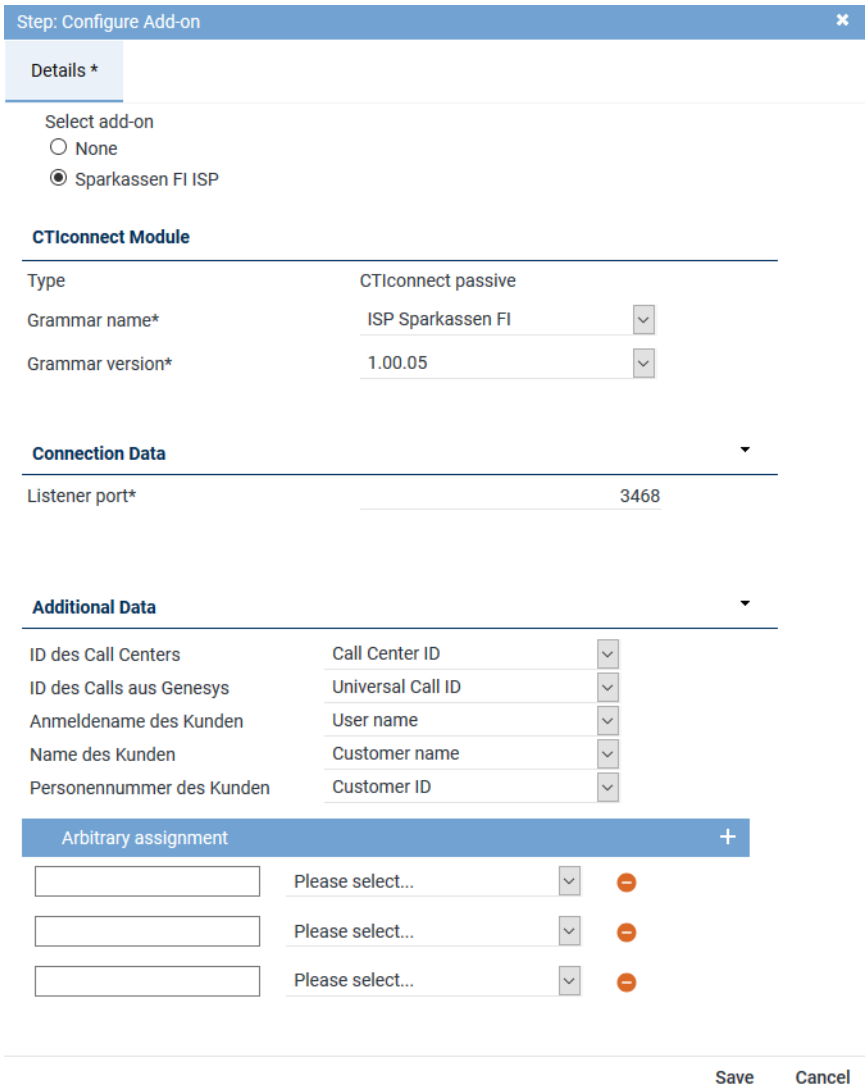


Fig. 275: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 62: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 227.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 63: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

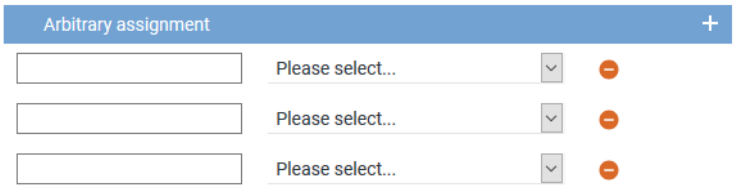


Fig. 276: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.

   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

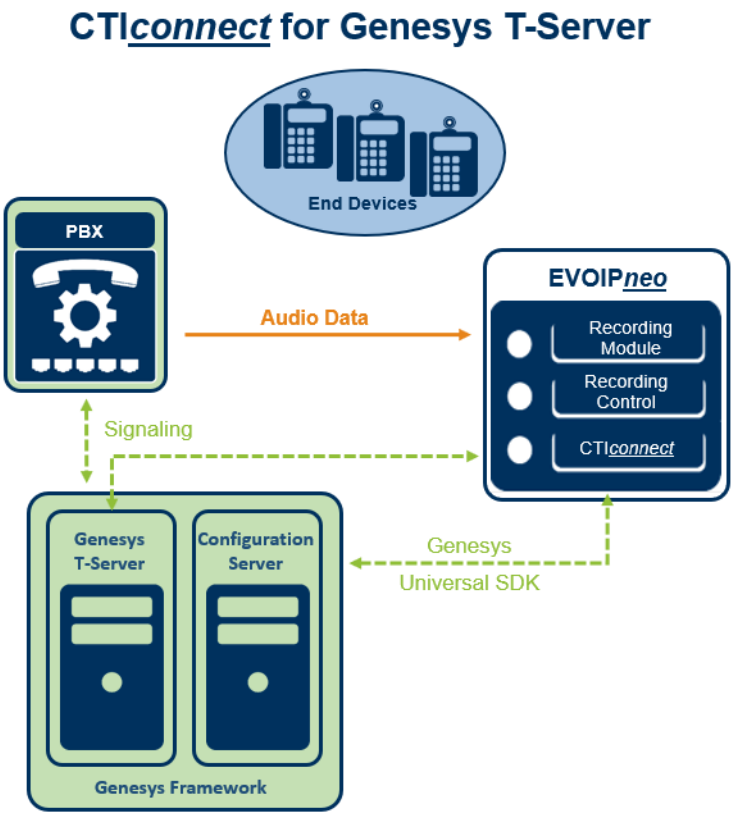


Fig. 277: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

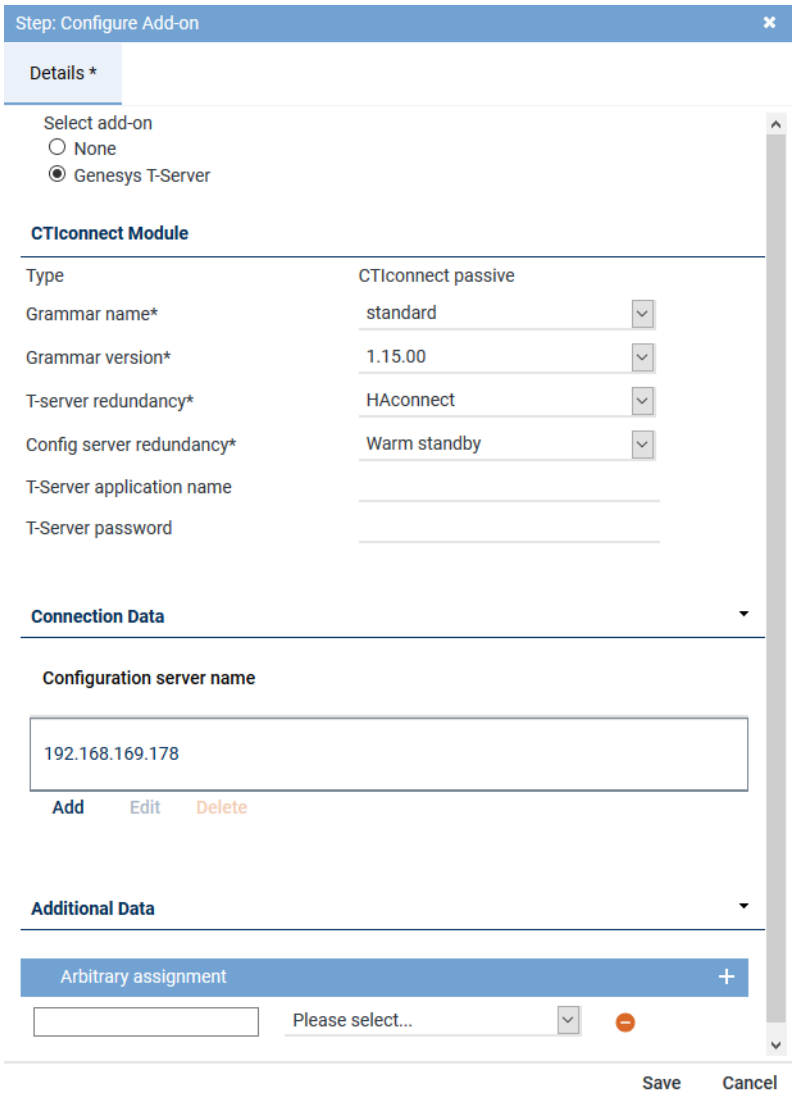


Fig. 278: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 64: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

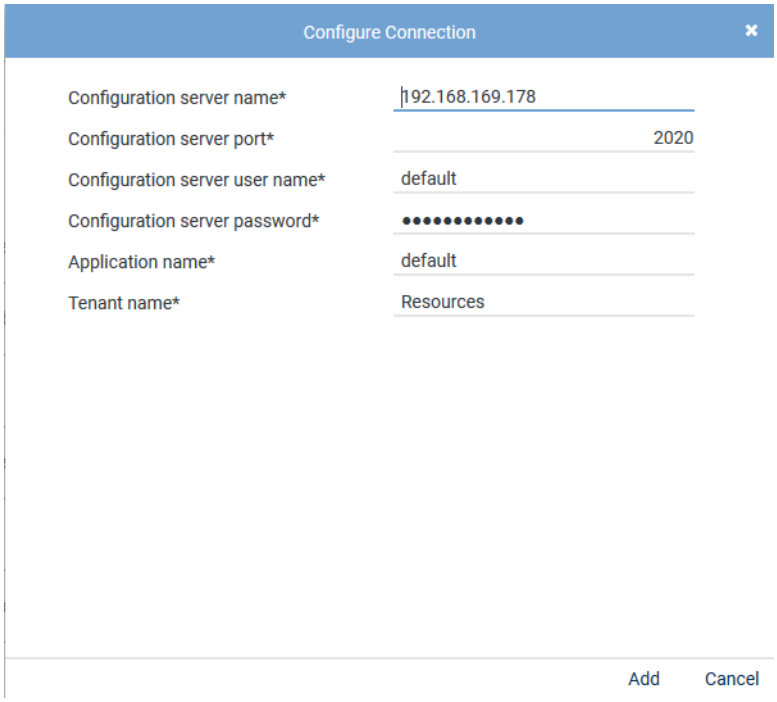


Fig. 279: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 65: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

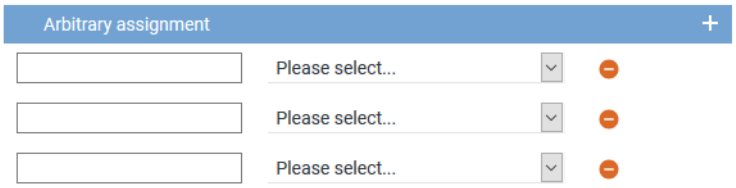


Fig. 280: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

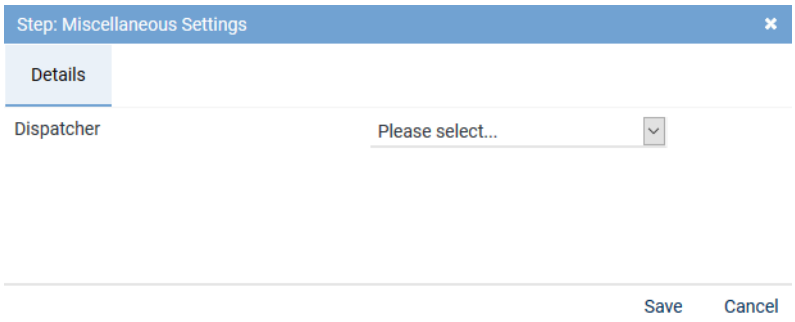


Fig. 281: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

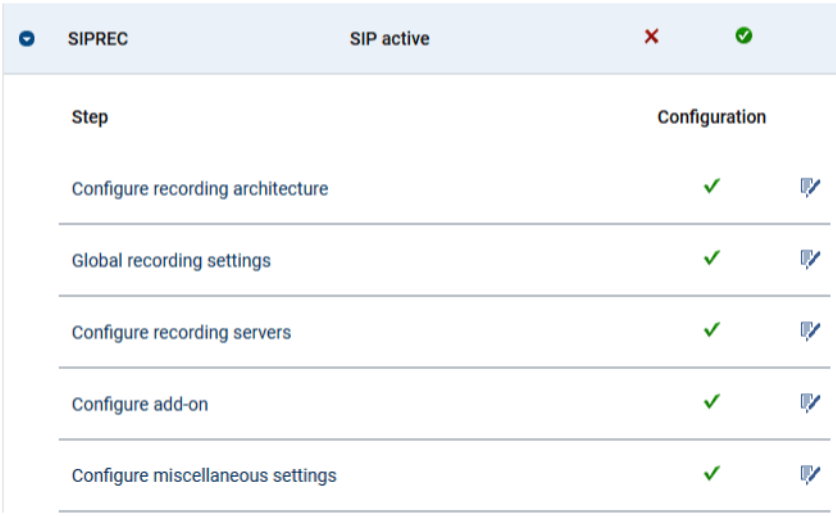


Fig. 282: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

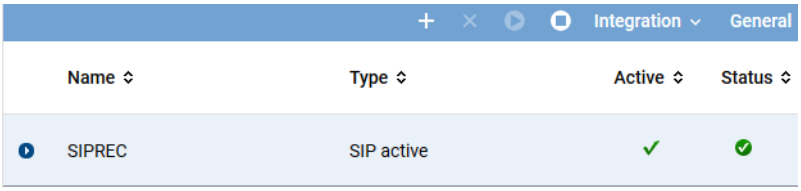


Fig. 283: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

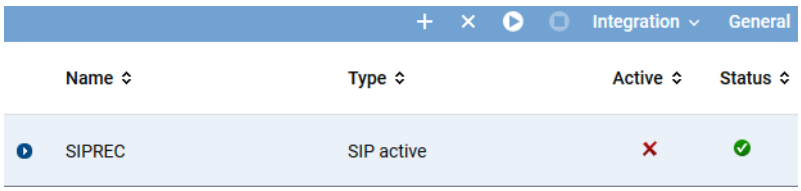


Fig. 284: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.2.5 Configure recording solution Multi-Server Failover

7.1.2.5.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

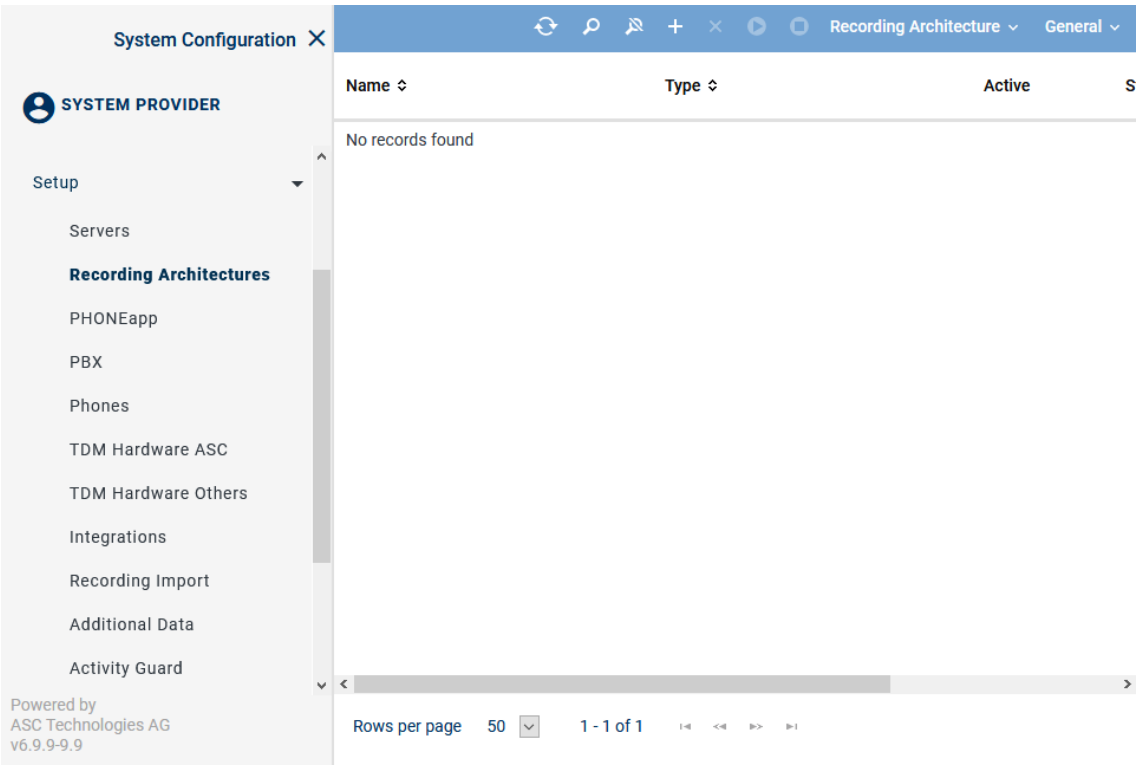


Fig. 285: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 286: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Create recording architecture Multi-Server Failover

If there are several recording servers which are supposed to take over the tasks of another recording server in case of an error, you have to create a recording architecture of the type *Multi-Server Failover* .

1. To create a new recording architecture, click on the icon + *(Create)* in the toolbar of the main view.
   ⇨ The window *New Recording Architecture* appears.

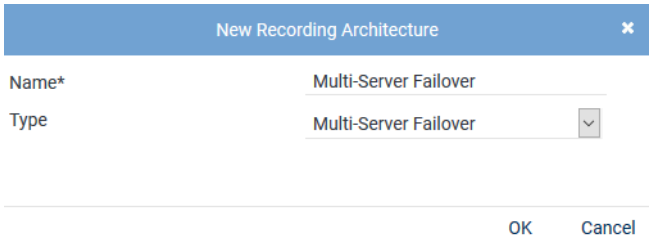


Fig. 287: Create recording architecture - Multi-Server Failover

2. In the entry field *Name*, enter a descriptive name for the recording architecture.
3. From the drop-down list *Type*, select the recording architecture type *Multi-Server Failover* .
   NOTICE! The drop-down list only displays the supported recording architecture types.

4. Click on the button *OK*.
   ⇨ Your entries now appear in the detail view.

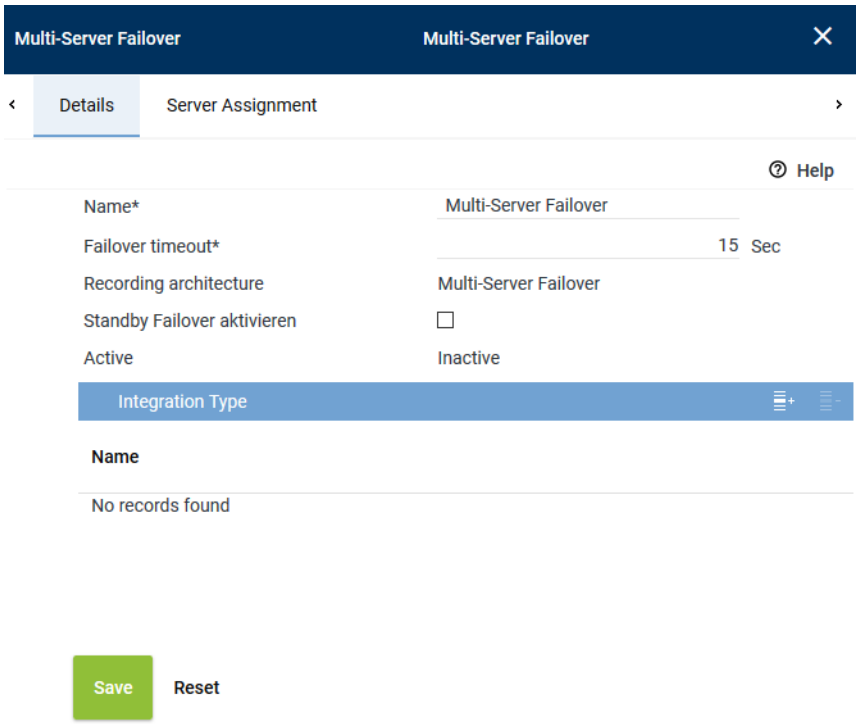


Fig. 288: Recording architecture - tab Details - Multi-Server Failover

As standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For further information about the configuration of failover architectures, see chapter "Standby management for failover architectures", p. 373.

Failover timeout	Enter a timeout of a minimum of 15 seconds after which the failover process is supposed to start. Depending on the system architecture it may make sense to configure a longer timeout period. The timeout defines the elapse time until the failover process starts. If the status returns to *OK* within this time, then the failover process is not triggered. **NOTICE!** Check these parameters after an update and set the timeout to 15 seconds, if required.
Activate standby failover	Activate this option if you would like to ensure that the system switches back to the primary server in case of an error of the standby server. **NOTICE!** There is no check whether the primary database is working properly before switching back. As a result it is possible that both databases are in an undefined state. **NOTICE!** After switching back to the original primary server from the standby server, this option is deactivated. If the switching process is supposed to be carried out automatically in the event of a new error, you must activate this option again.
Active	Shows the status of the recording architecture.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 289: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for Multi-Server Failover

1. Click on the tab *Server Assignment* to assign the recording components to the corresponding recording servers for the *Multi-Server Failover* recording architecture.

Group field Recording Control and CTI*connect*

In this group field, you can configure recording control You can configure two different server for this purpose or select the same server.

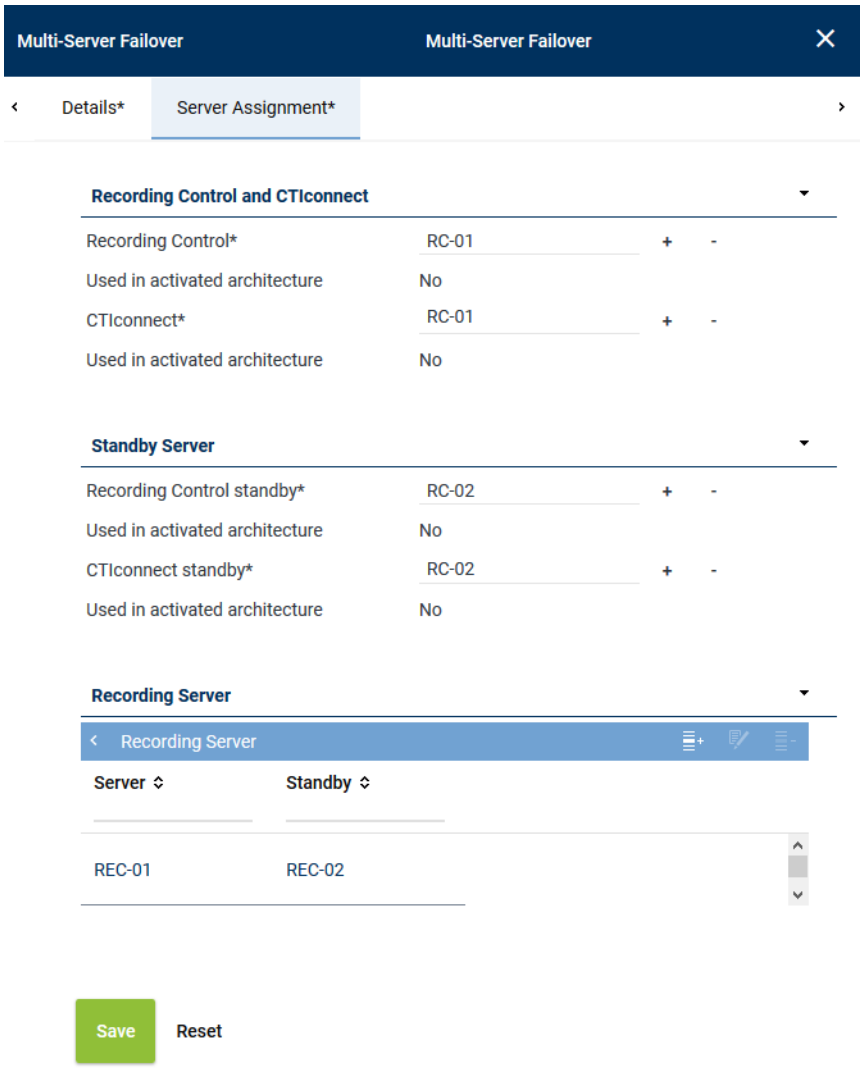


Fig. 290: Recording Architecture - tab Server Assignment

1. Click on the button + behind the entry field *Recording control*.
   ⇨ The window *Servers* appears.

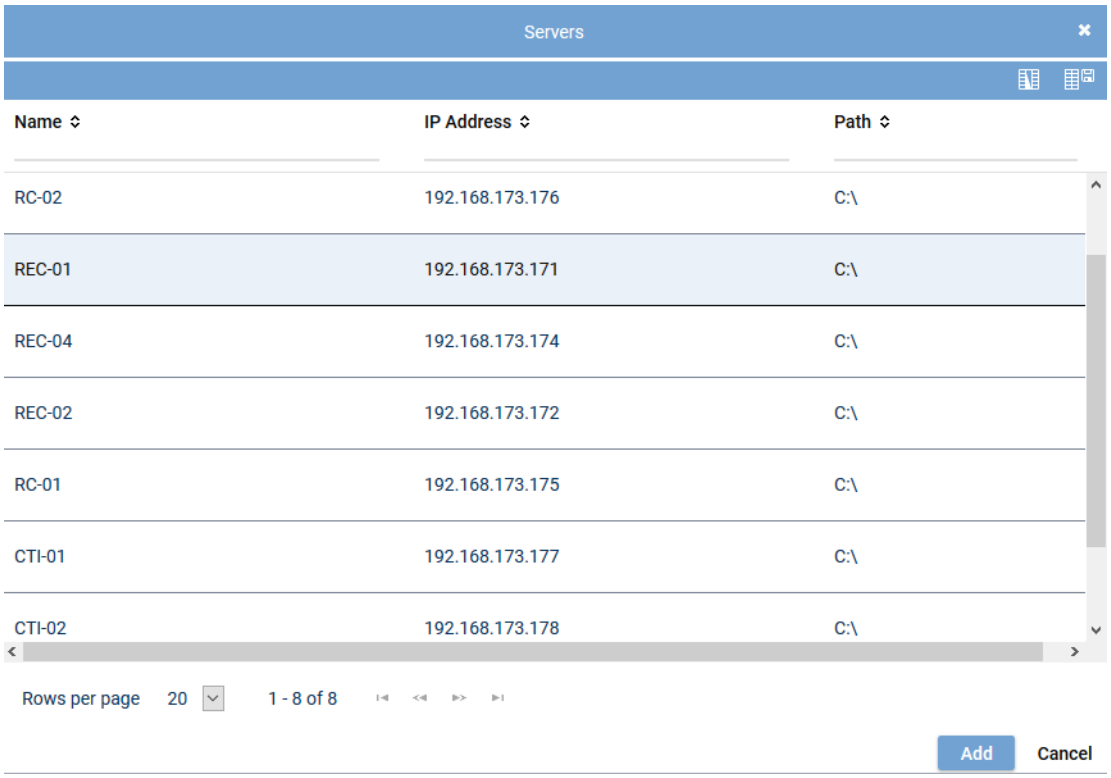


Fig. 291: Recording Architecture - assign server - example

2. Select the server for the *recording control module*.
3. Click on the button *Add*.
   ⇨ The name of the server now appears in the detail view.
4. To delete an assignment, click on the button - .

ⓘ A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the CTI*connect module* in the entry field CTI*connect*.

Group field Standby Server

1. Click on the button + behind the entry field *Recording control*.
2. Select the standby server for the *recording control module*.
3. Click on the button *Add*.
   ⇨ The name of the server now appears in the detail view.
4. Click on the button + behind the entry field *CTIconnect*.
5. Select the standby server for the *CTIconnect module*.
6. Click on the button *Add*.
   ⇨ The name of the server now appears in the detail view.

Group field Recording Server

1. In the table headline *Recording Server*, click on the icon .
   ⇨ The following window appears:

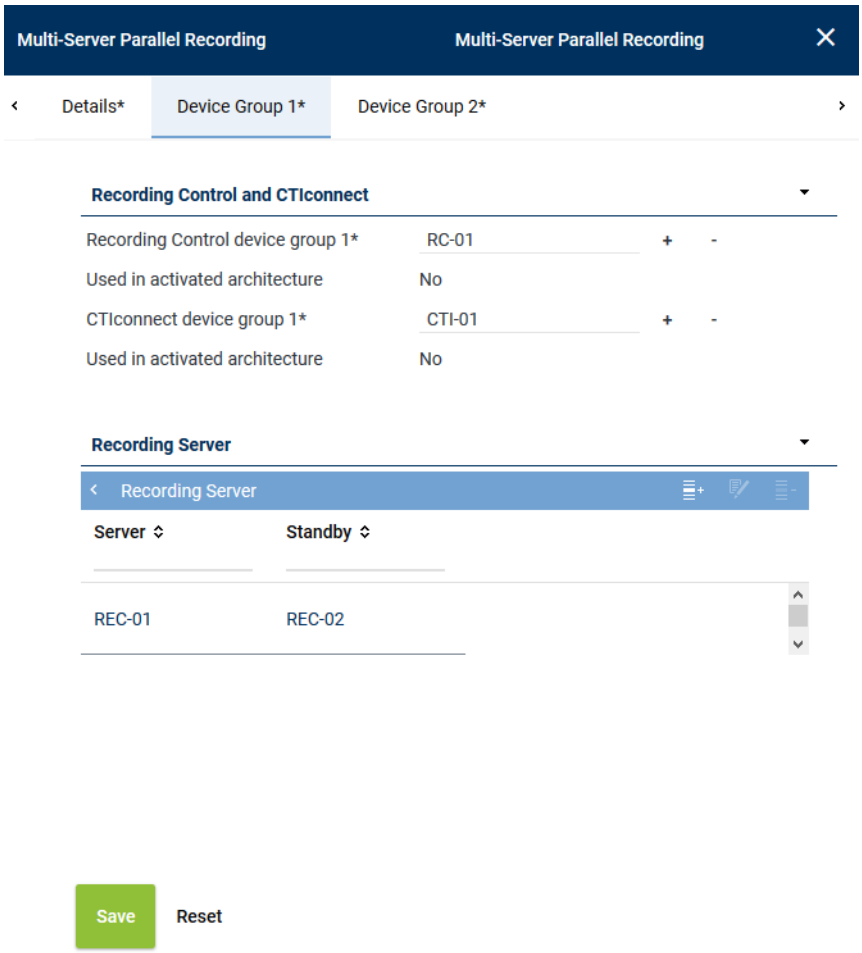


Fig. 292: Add Recording Server

2. As described in the previous steps, go to the entry field *Primary server* and click on the icon + to select the primary server on which the recording is supposed to run.
3. In the entry field *Standby server*, click on the icon + to select the standby server which is supposed to take over recording in case of an error.
4. Select the recording type you would like to use for these servers by activating the check box.

ⓘ You can activate several recording types if the integration has been designed for this and if you have installed the respective licenses.

5. Click on the button *OK* to close the window.
   ⇨ The name of the server now appears in the detail view.
6. To edit the assignment subsequently, click on the icon .
   To delete an assignment, click on the icon .
7. If you would like to add further recording servers, repeat the steps described above.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the tool-bar becomes active.
3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

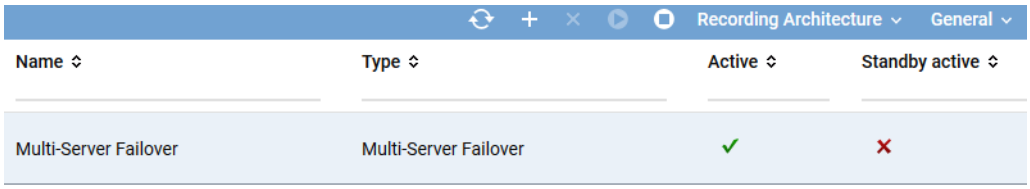


Fig. 293: Recording architecture - activate recording architecture

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.

ⓘ The recording architecture must have been activated so that the integration can be configured.

ⓘ For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See chapter "Standby management for failover architectures", p. 373.

ⓘ If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.5.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

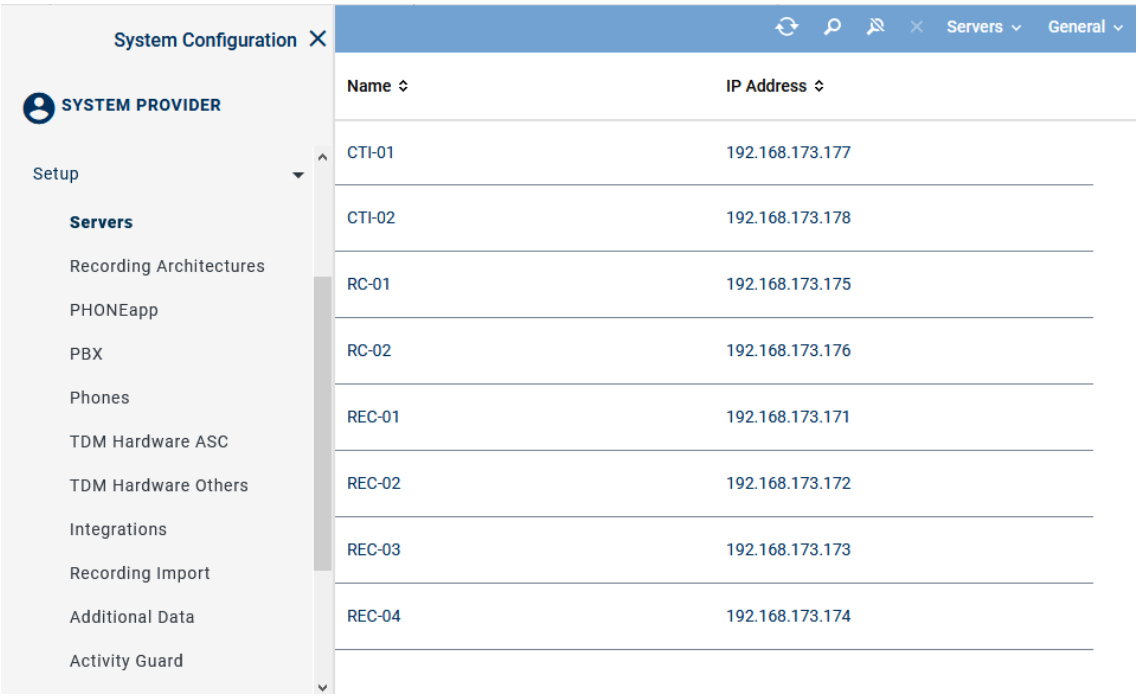


Fig. 294: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.

Path	Shows the path of the server.
Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 295: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.
Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 254.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.

   ⇨ The window *Server Locations* appears.

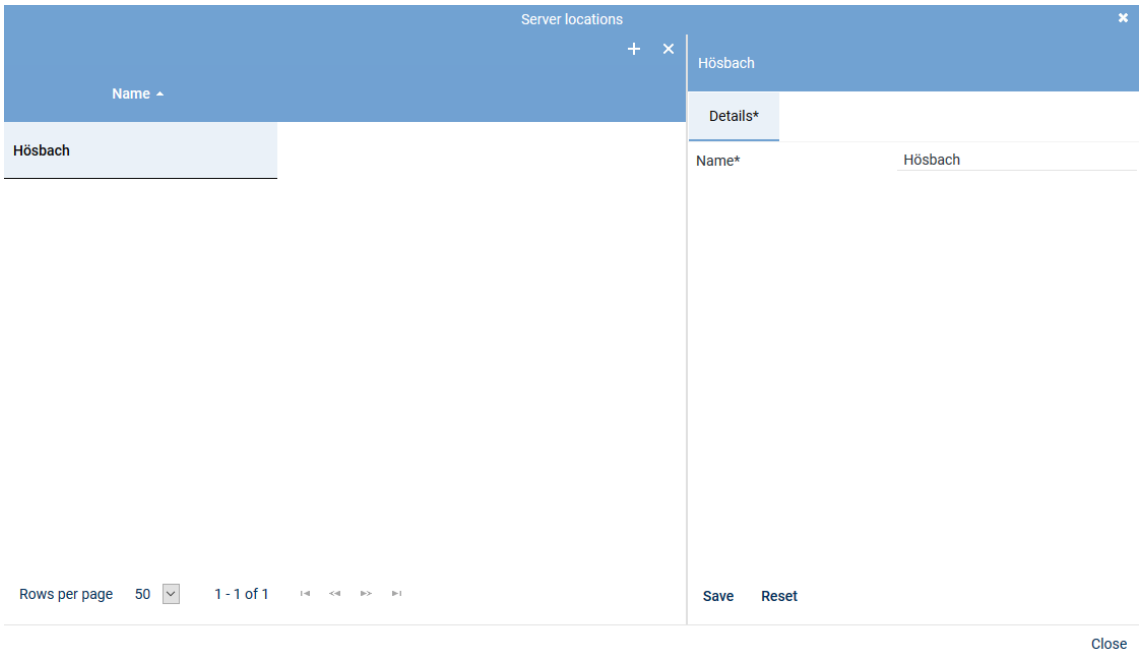


Fig. 296: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

ⓘ A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.

   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

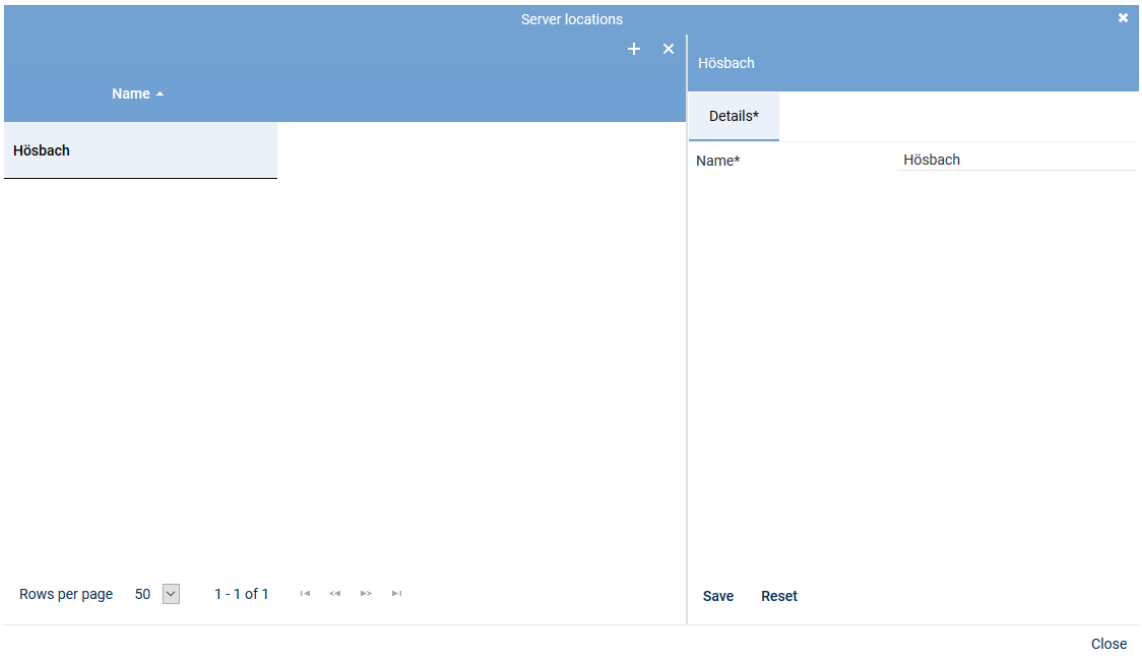


Fig. 297: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

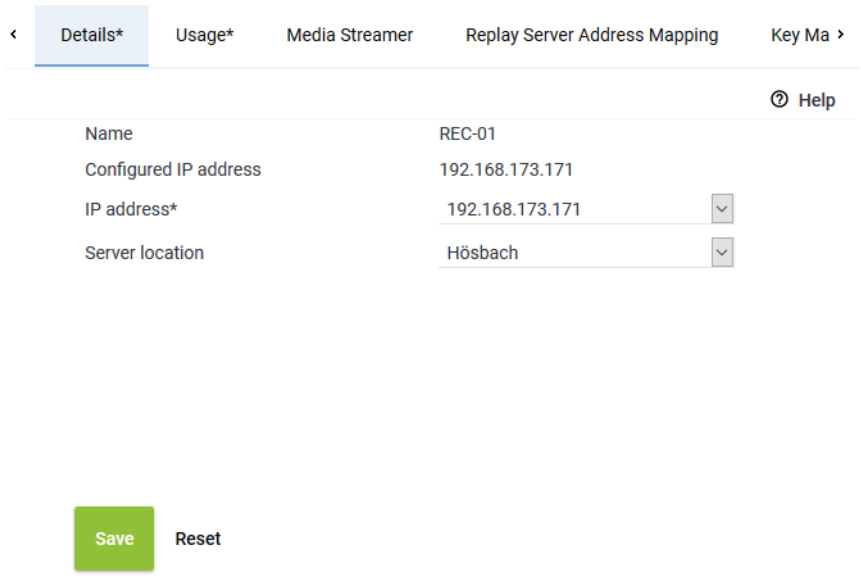


Fig. 298: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.

4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

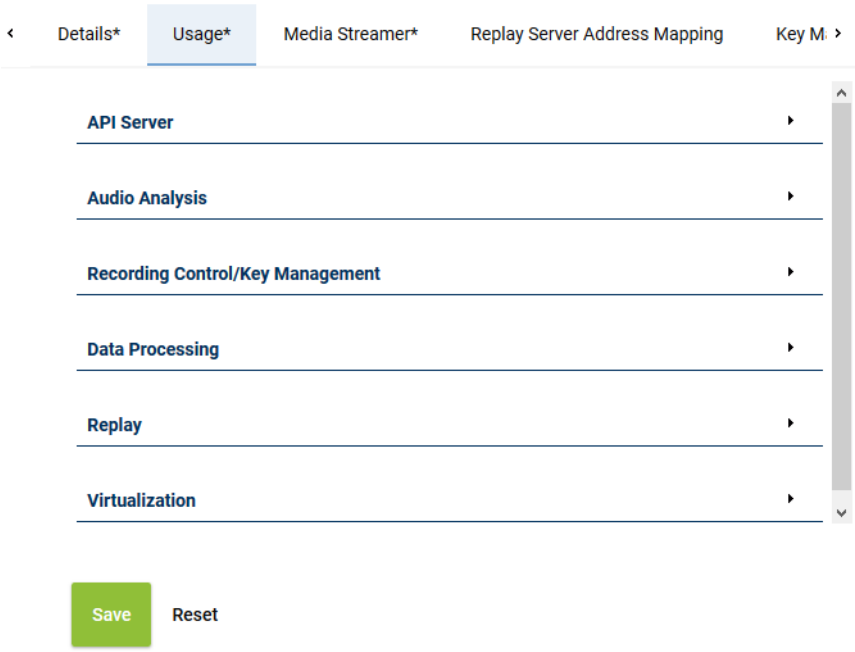


Fig. 299: Servers - tab usage

Group field API Server

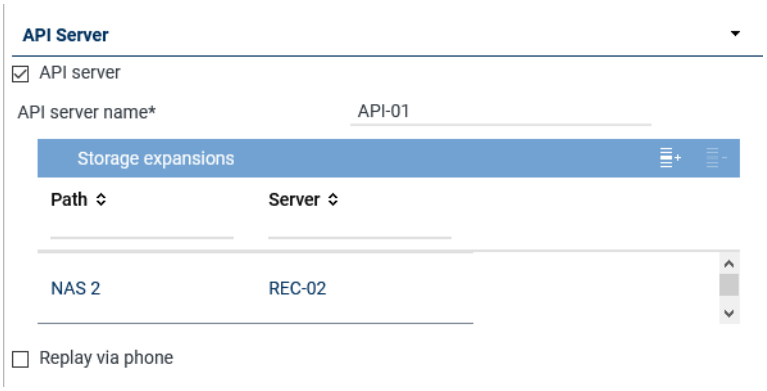


Fig. 300: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server.

Parameter	Value/Description
	☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 268.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List *Storage expansions*	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 259. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list. If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 266. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

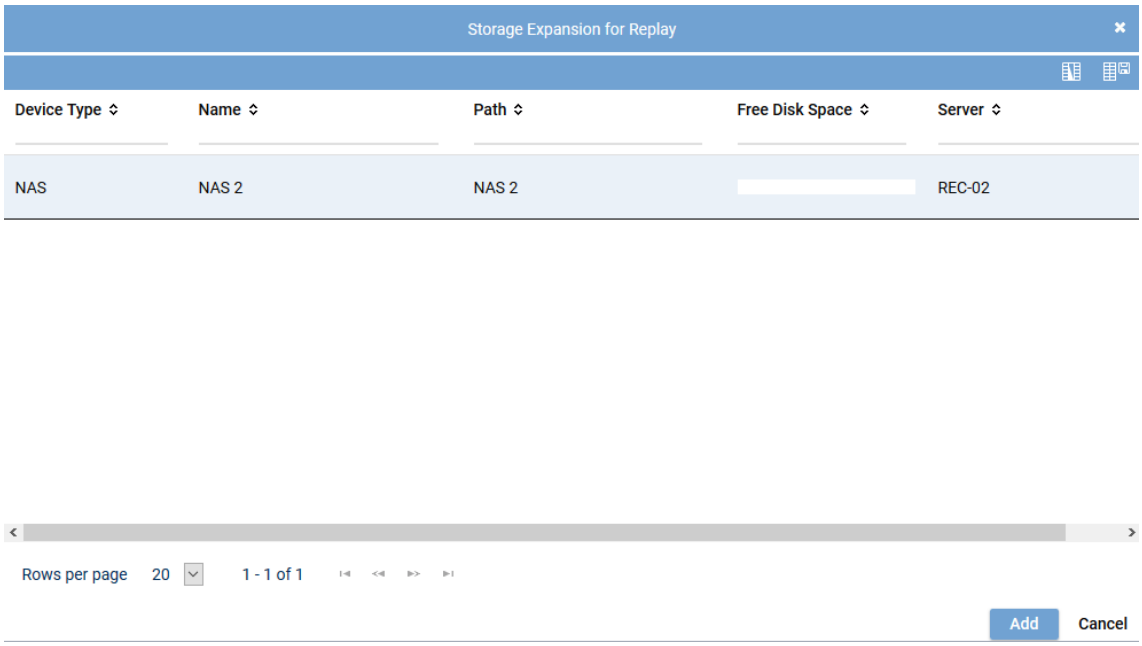


Fig. 301: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

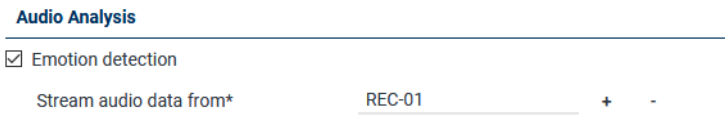


Fig. 302: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 66: Configure audio analysis

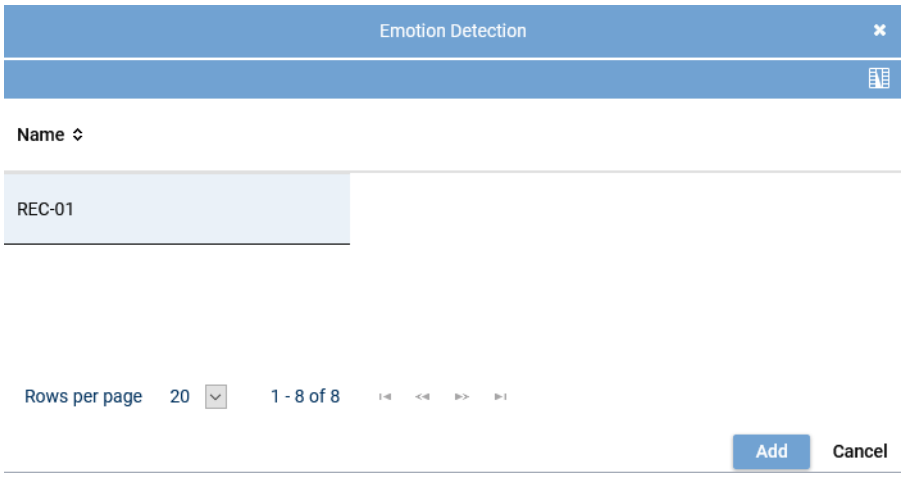


Fig. 303: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

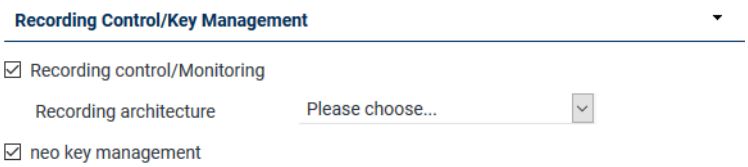


Fig. 304: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 67: Configure recording control/key management

Group field Data Processing

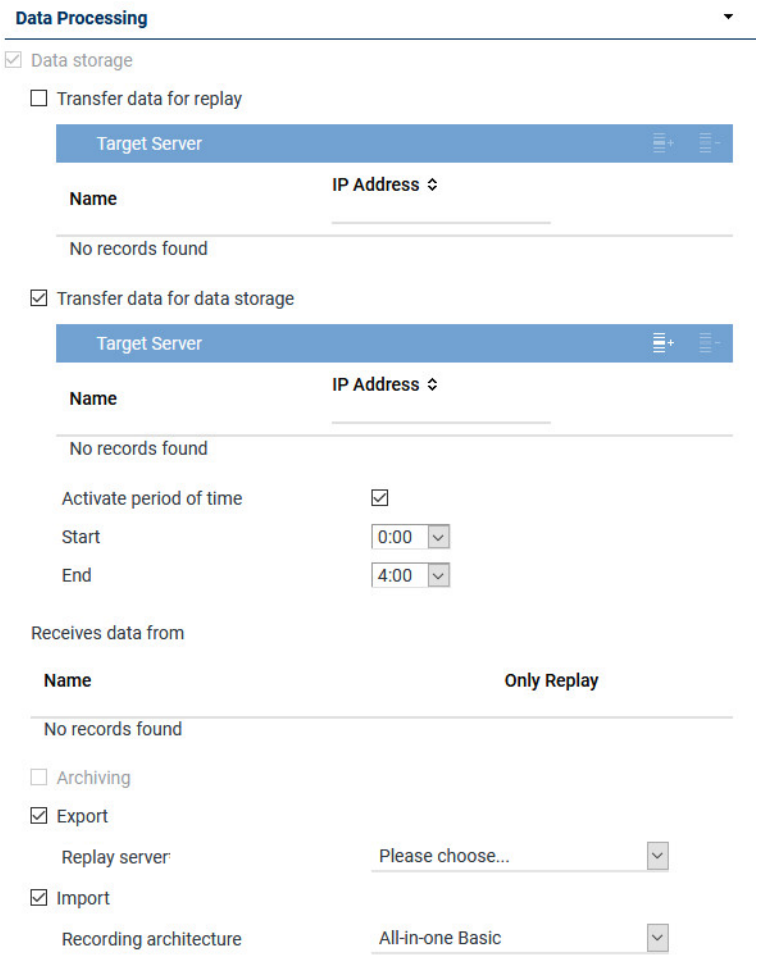


Fig. 305: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 263. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be trans-

Parameter	Value/Description
	ferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 263. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.

Parameter	Value/Description
	NOTICE! If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 68: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 306: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

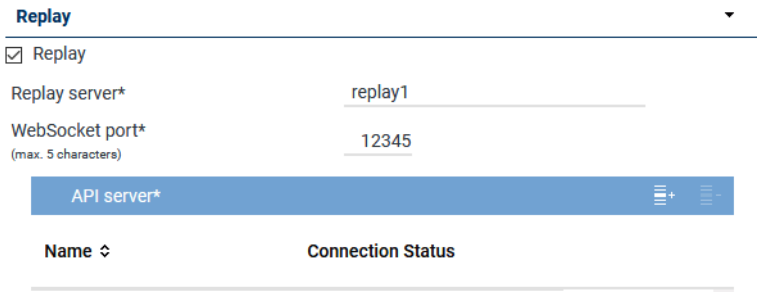


Fig. 307: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 264. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 69: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.

- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

Fig. 308: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 257.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 309: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management.

Parameter	Value/Description
	• *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 70: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

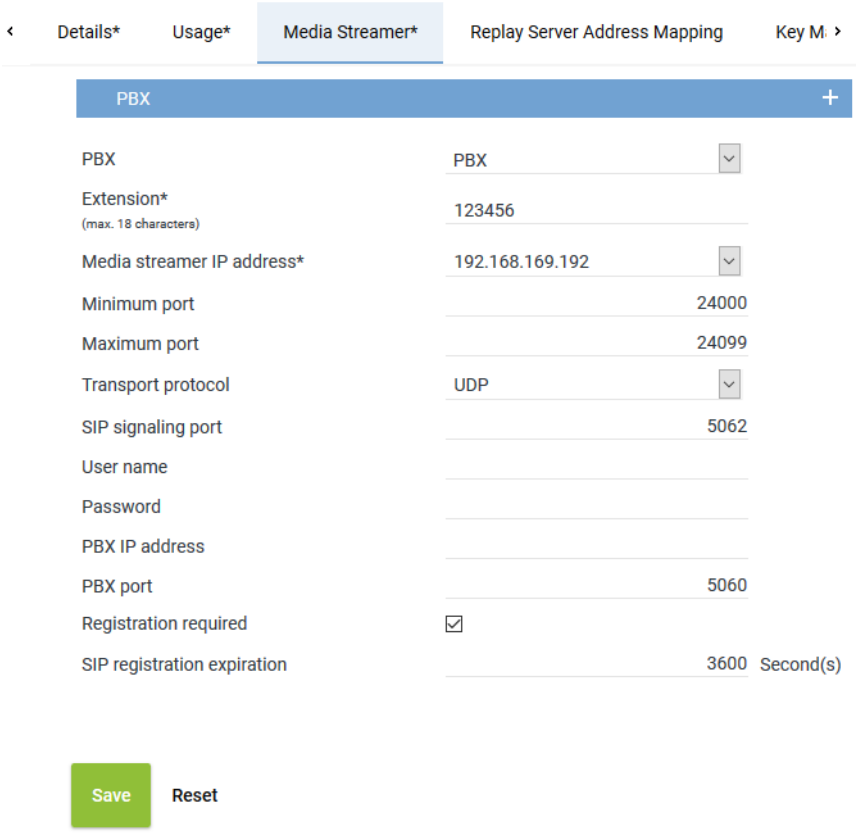


Fig. 310: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.

	If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 272.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number. A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

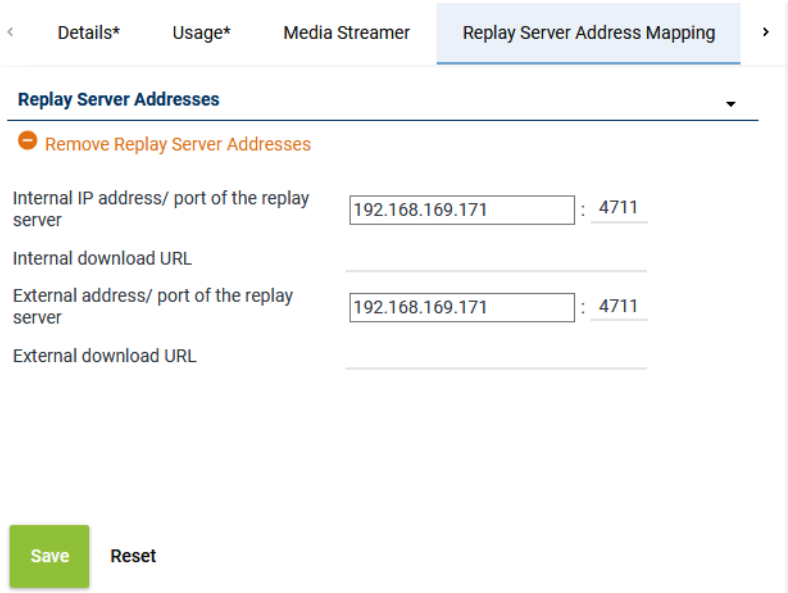


Fig. 311: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

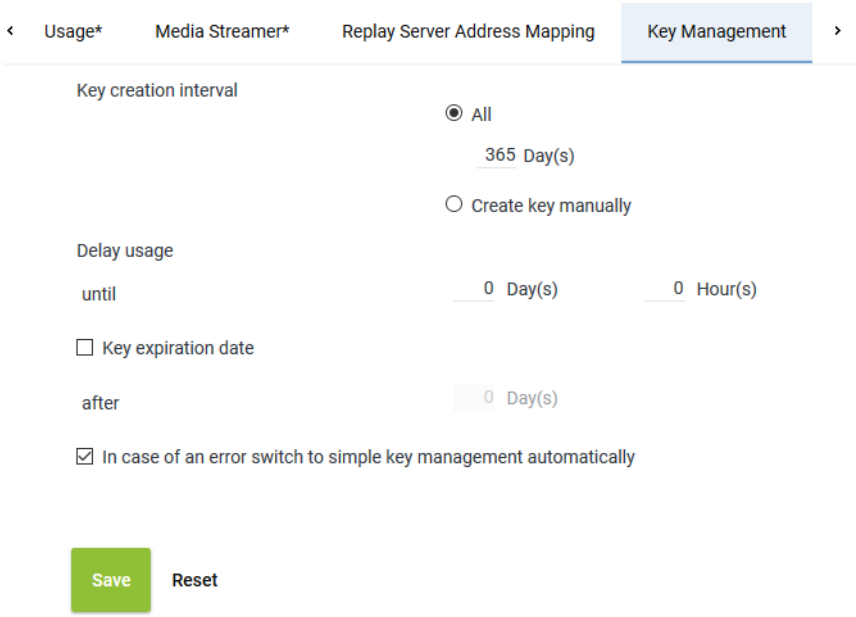


Fig. 312: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.

Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid. ☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

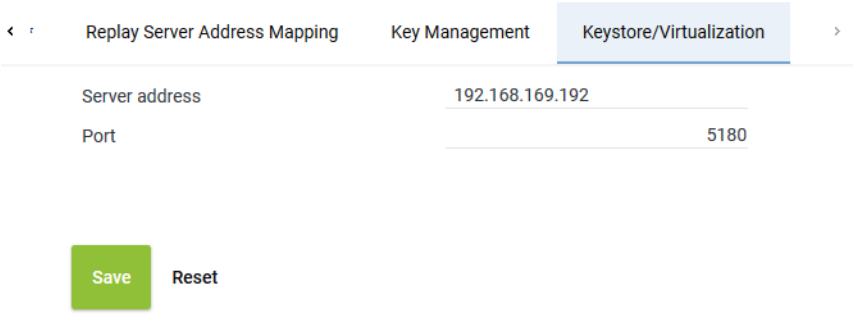


Fig. 313: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management:

	IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.5.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

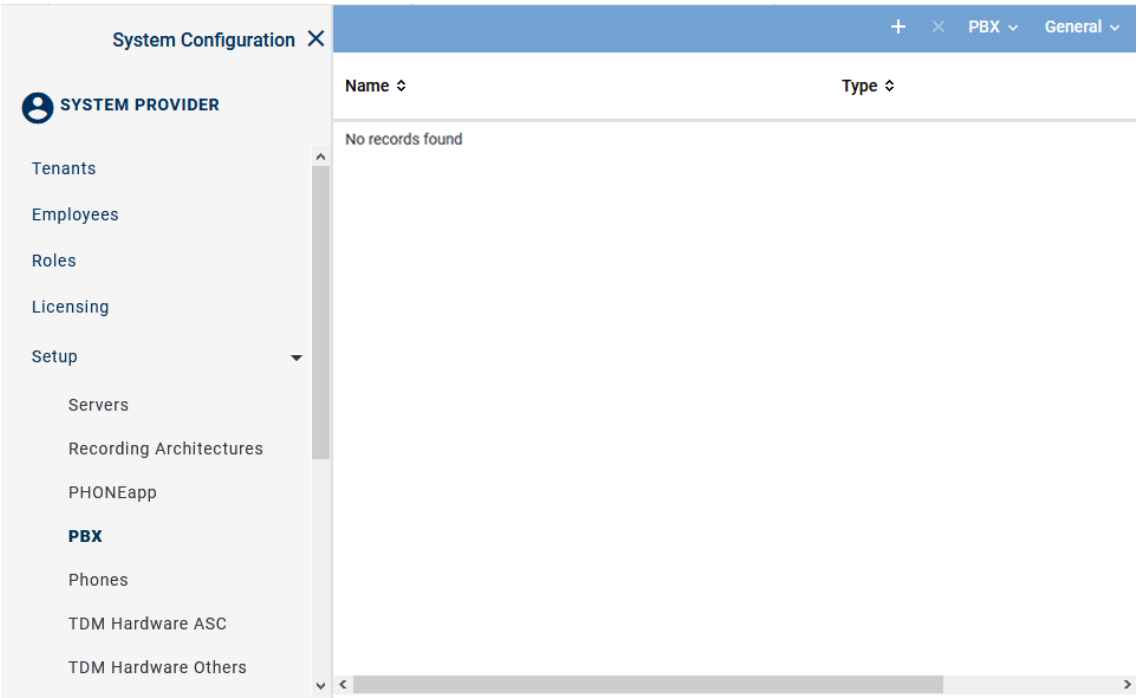


Fig. 314: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 315: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.

PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

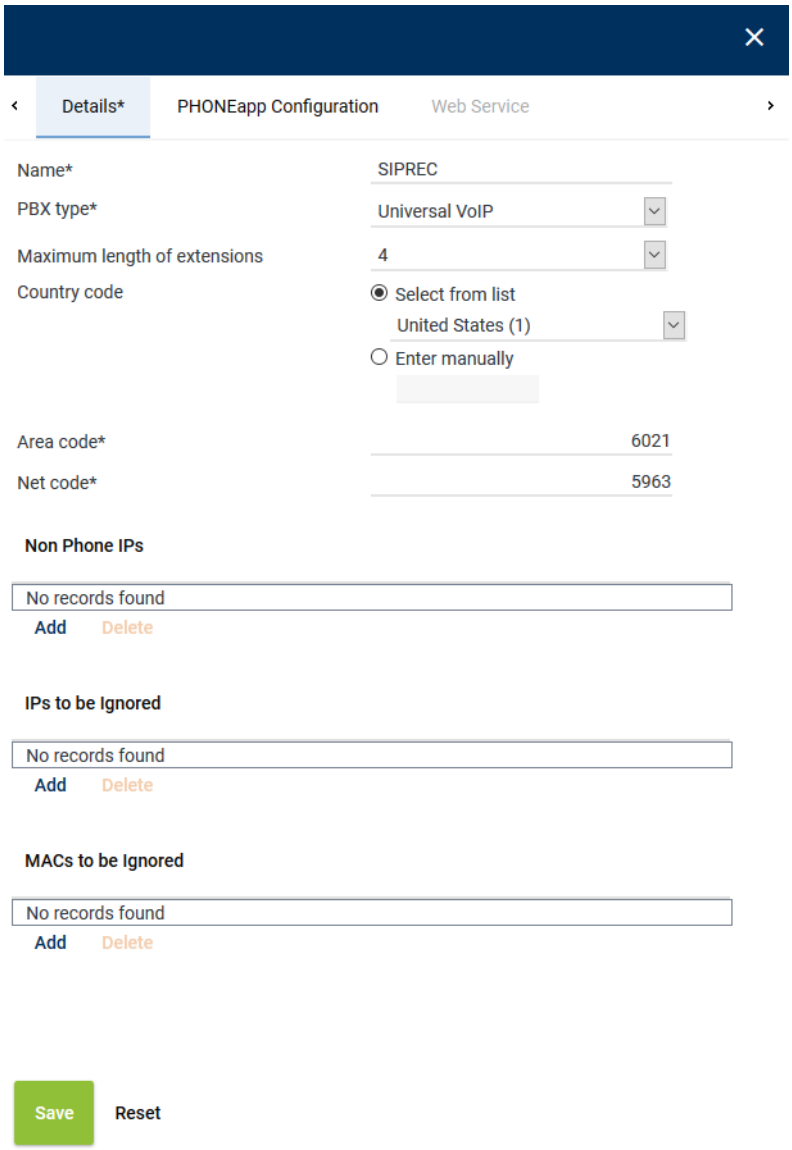


Fig. 316: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list* Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 71: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 72: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.5.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

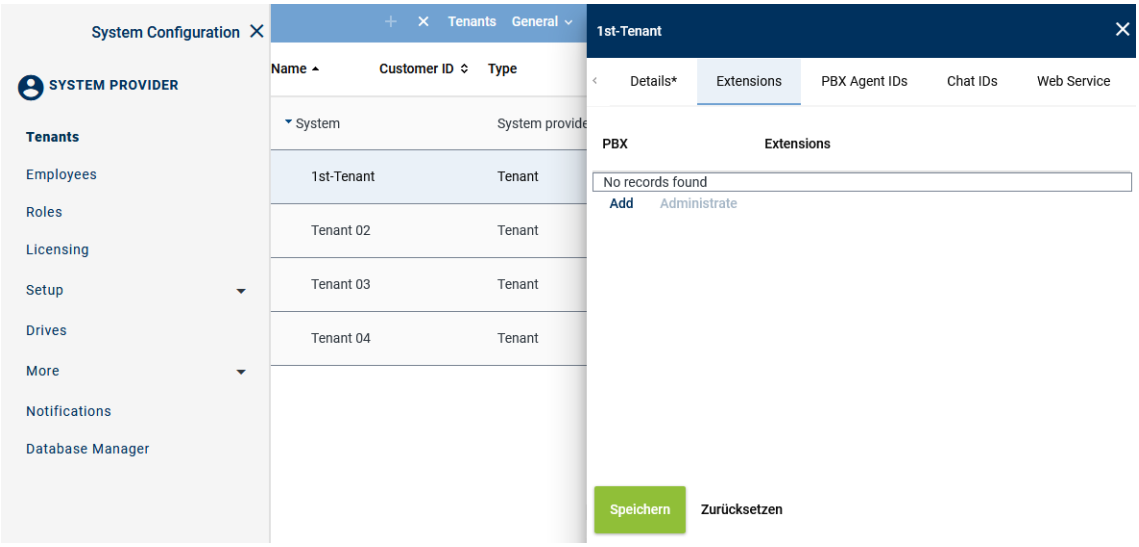


Fig. 317: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.

⇨ The following window appears:

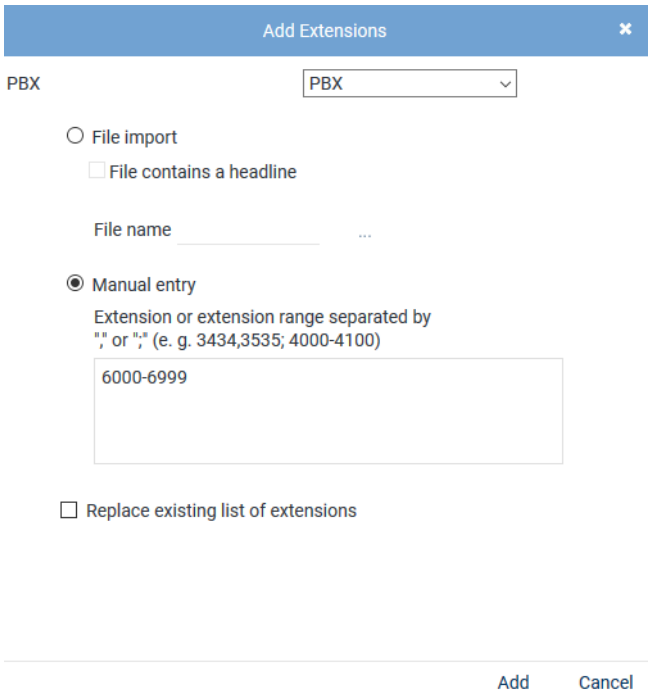


Fig. 318: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT* • *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually.

	To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

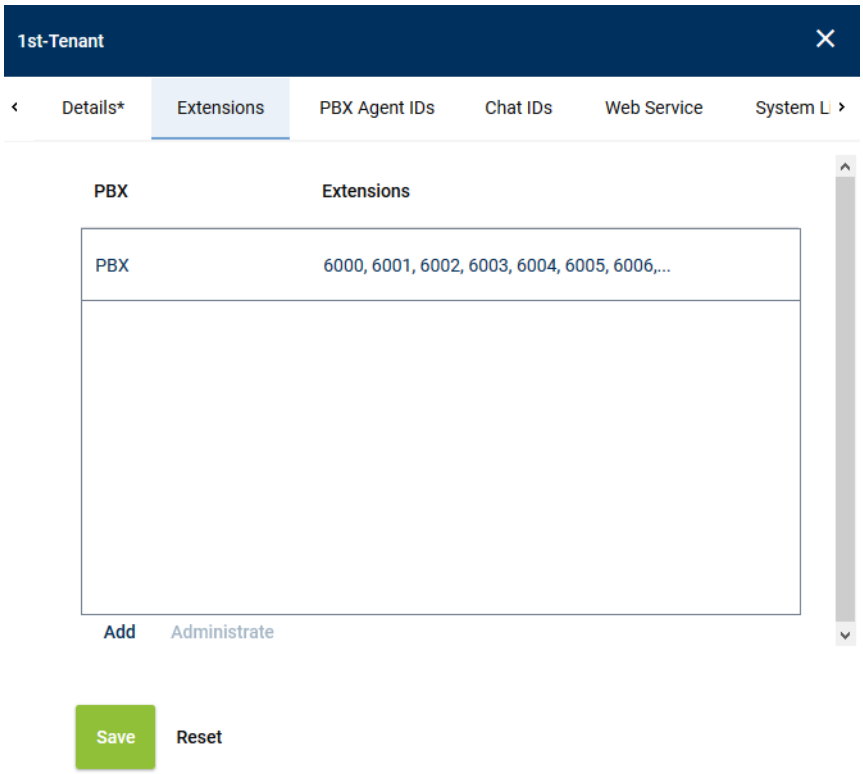


Fig. 319: Remove extensions

2. Click the button *Administrate*.

3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 320: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

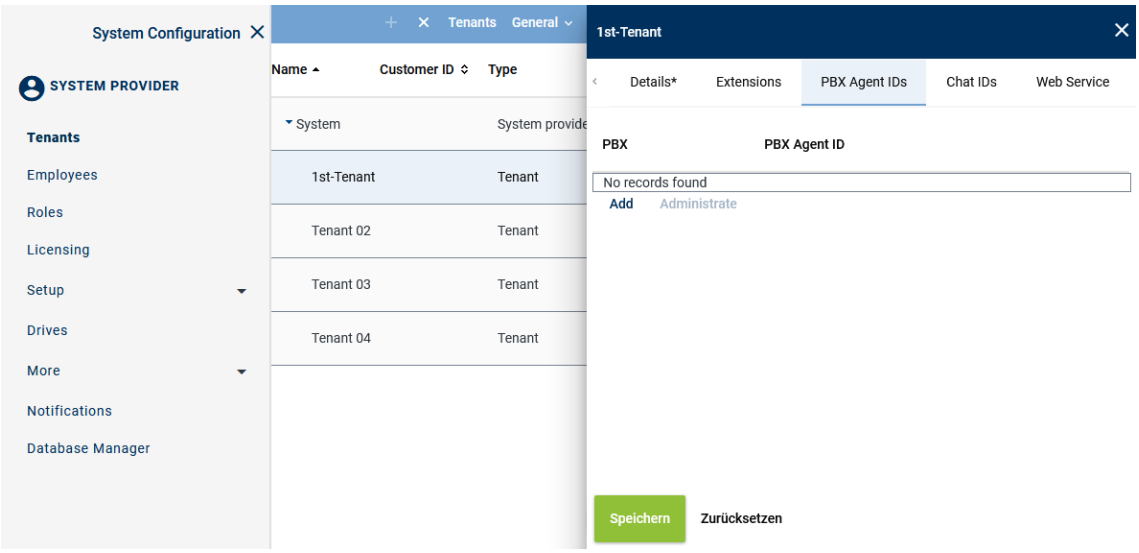


Fig. 321: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

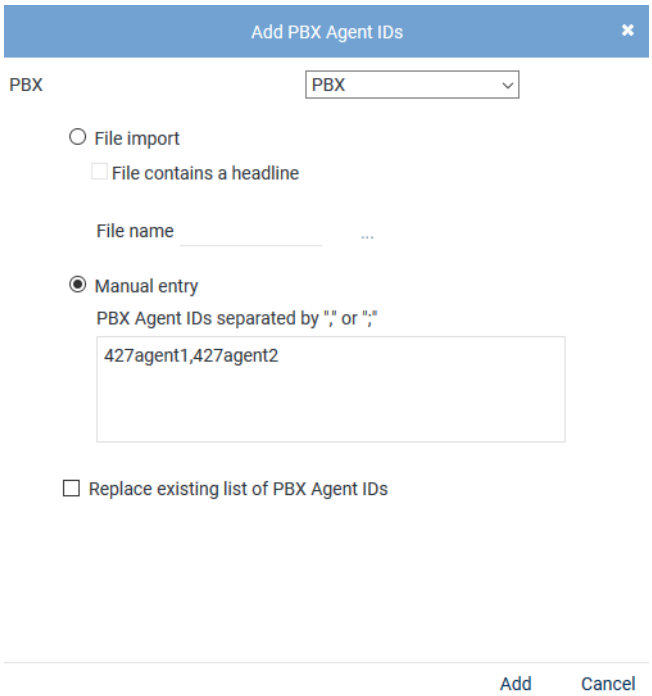


Fig. 322: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline

	Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

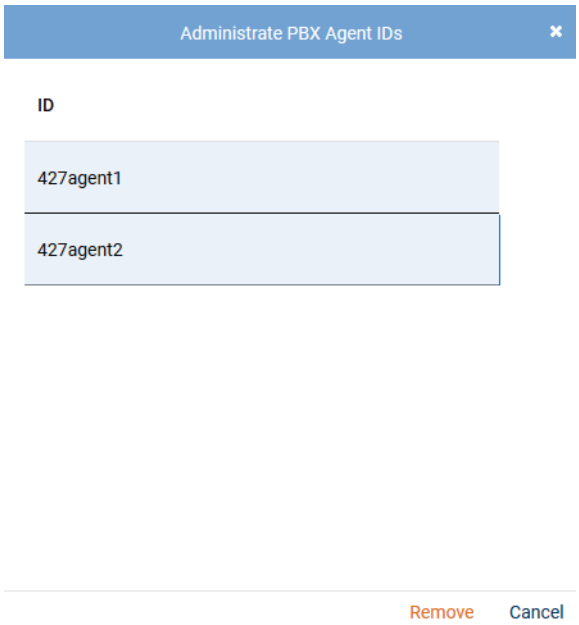


Fig. 323: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.5.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

> In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

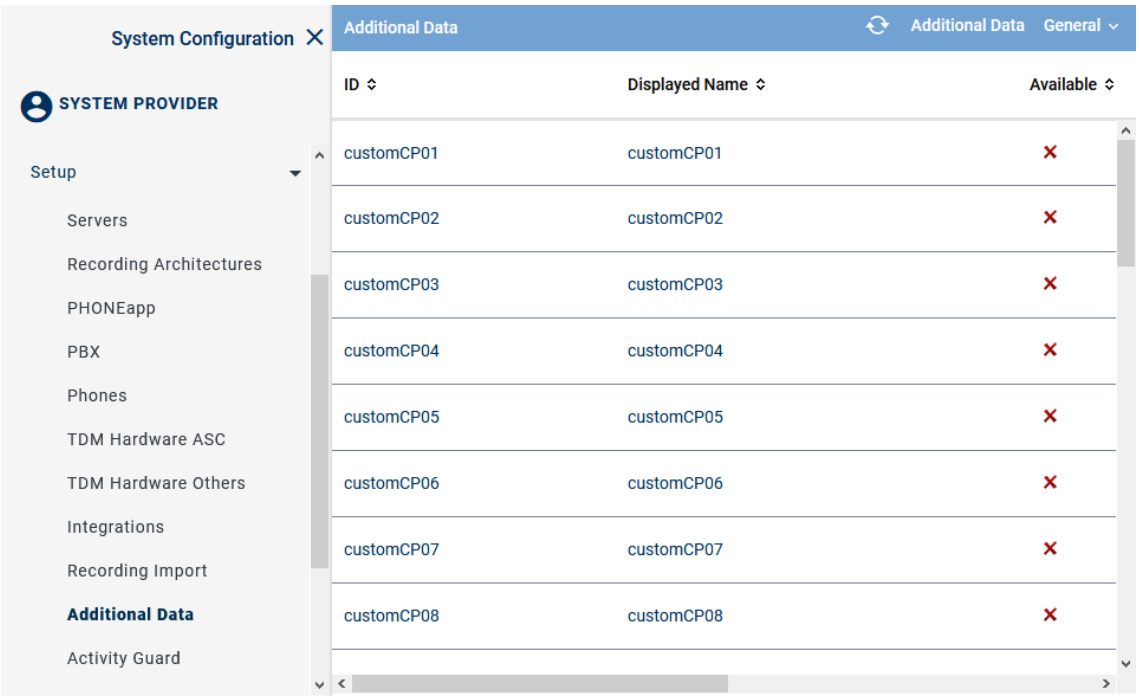


Fig. 324: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

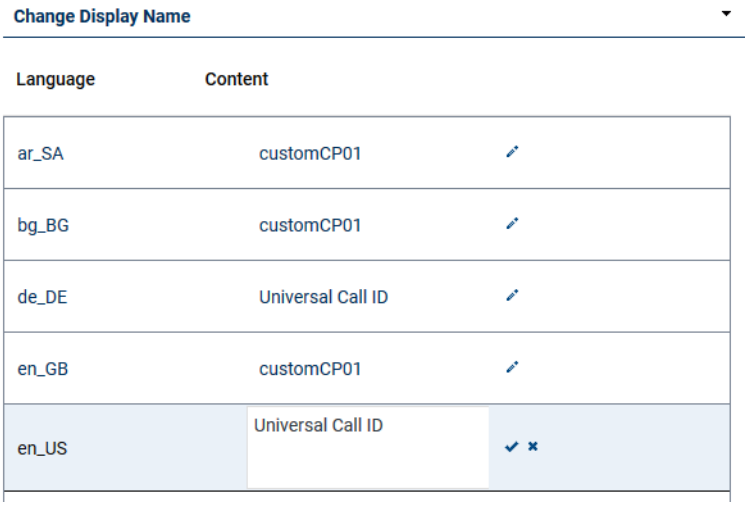


Fig. 325: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 326: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.5.6 Create integration for Multi-Server Failover

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

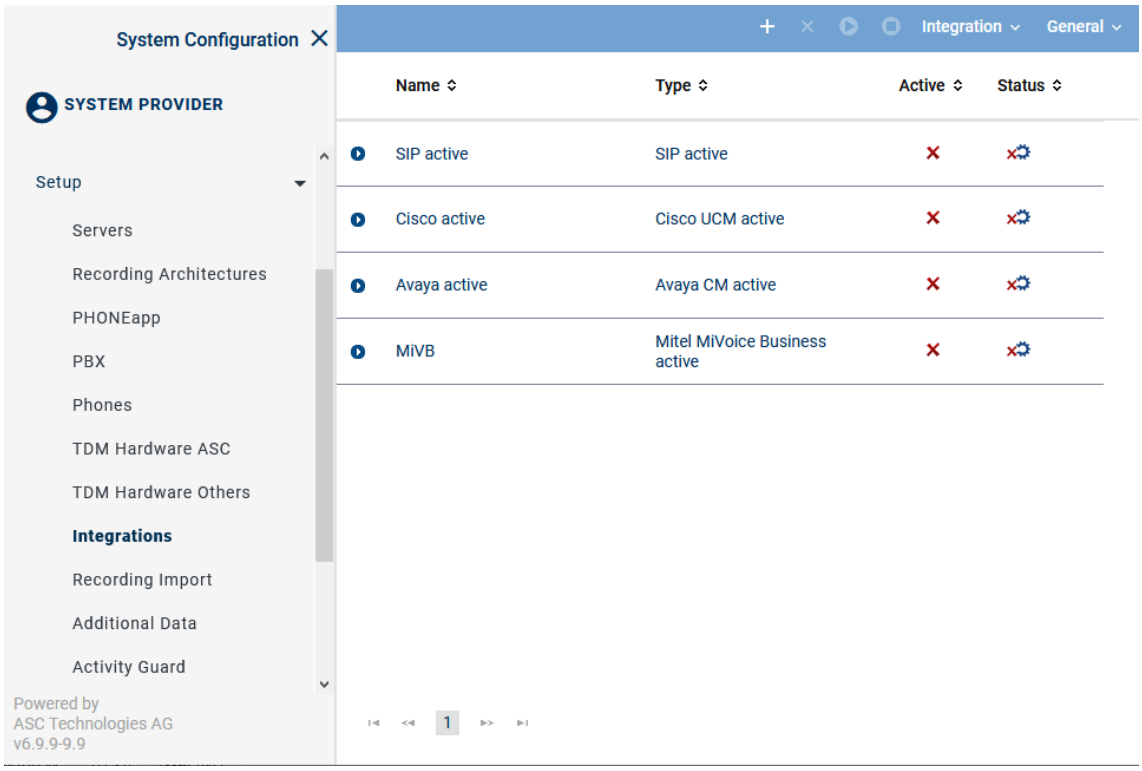


Fig. 327: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 328: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
✗	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

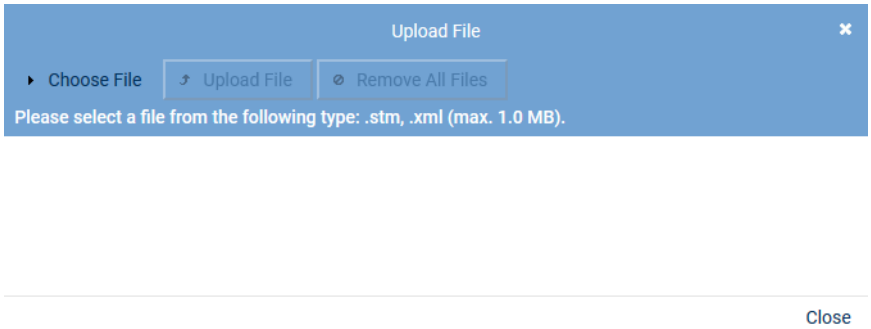


Fig. 329: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

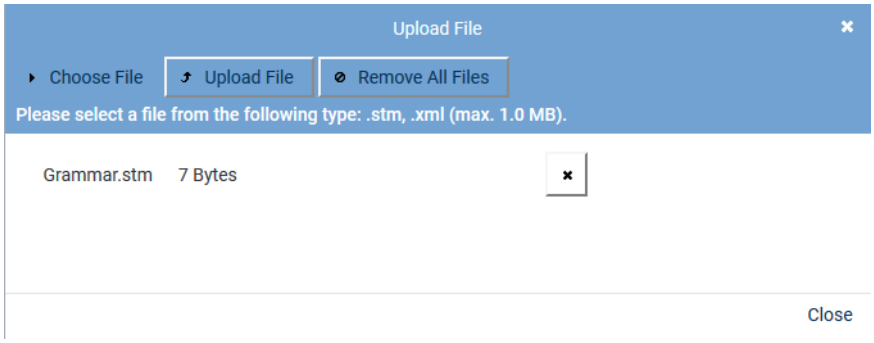


Fig. 330: Upload grammar

5. To remove a selected file from the list, click on the button × *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 331: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 73: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 332: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for Multi-Server Failover

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

Fig. 333: Assign recording architecture - Multi-Server Failover

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

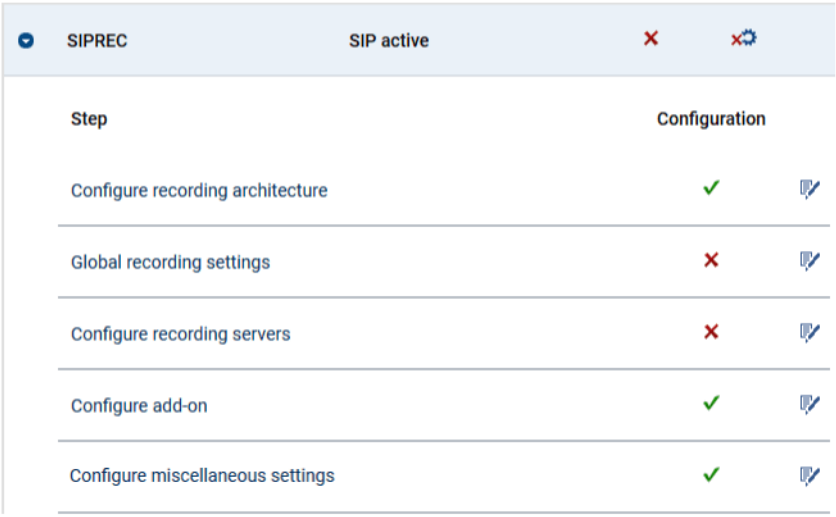


Fig. 334: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

Fig. 335: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for Multi-Server Failover

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.

   ⇨ The window *Step: Global Recording Settings* appears.

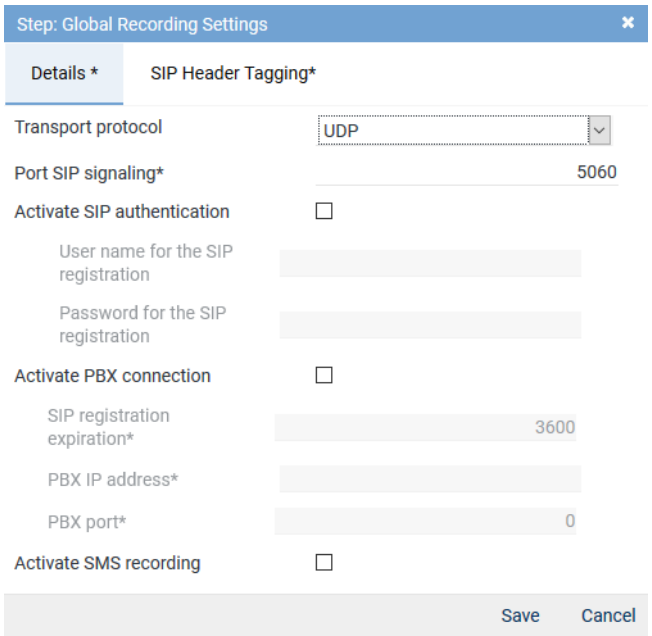


Fig. 336: Configuration step - Global Recording Settings - All-in-one Basic Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	Select the transport protocol *UDP* for the SIP signaling between the recording server and the PBX.
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*
Activate SIP authentication	Deactivate this option for this recording solution.

Parameter	Value/Description
Activate SMS recording	This function is not supported in this recording solution.

Tab. 74: Global recording settings

3. To save the entries, click on the button *Save*.
   To discard entries, click on the button *Cancel*.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

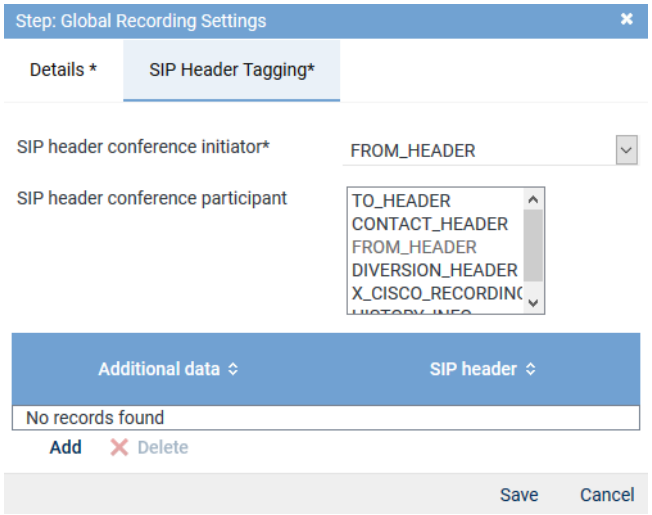


Fig. 337: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.
   ⇨ The window *SIP Additional Data* appears.

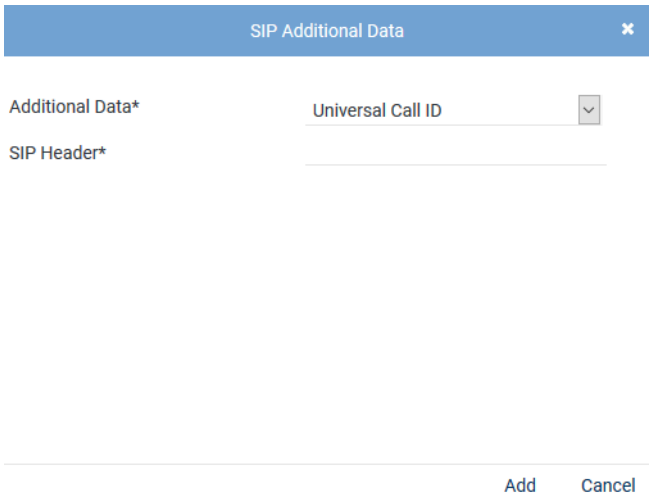


Fig. 338: SIP Additional Data

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted. To have ASC configure the mapping file, contact your distribution partner.

Tab. 75: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for Multi-Server Failover

To guarantee that recording works properly when switching servers in case of failover with several servers, you must configure a port range for each recording server. The range may be the same for all recording servers. Make sure, though, that the port range lies within the range of ports activated in the firewall, refer to the installation manual Installation requirements in chapter Communication matrix.

This configuration takes place in the configuration step *Configure recording servers*.

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

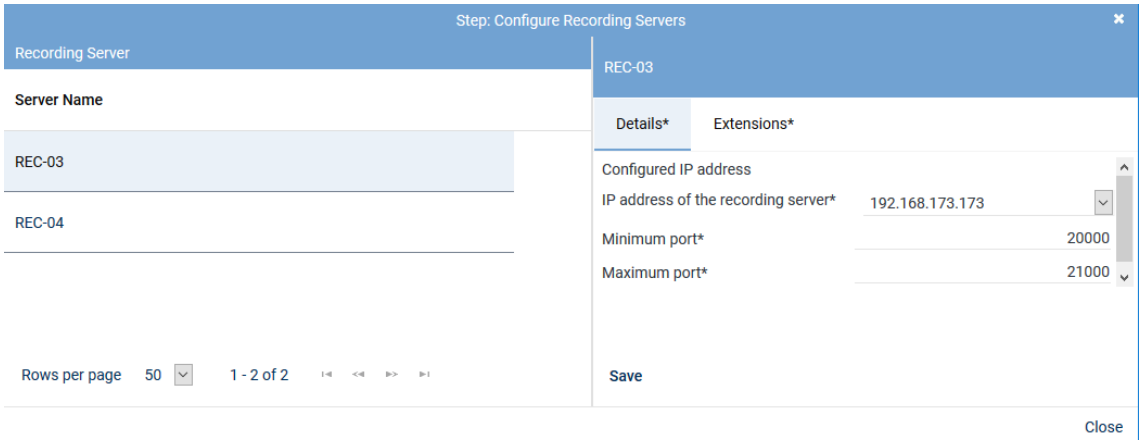


Fig. 339: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.

Parameter	Value/Description
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 76: Configure recording servers

For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.

In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Tab Extensions

1. Click on the tab *Extensions*.

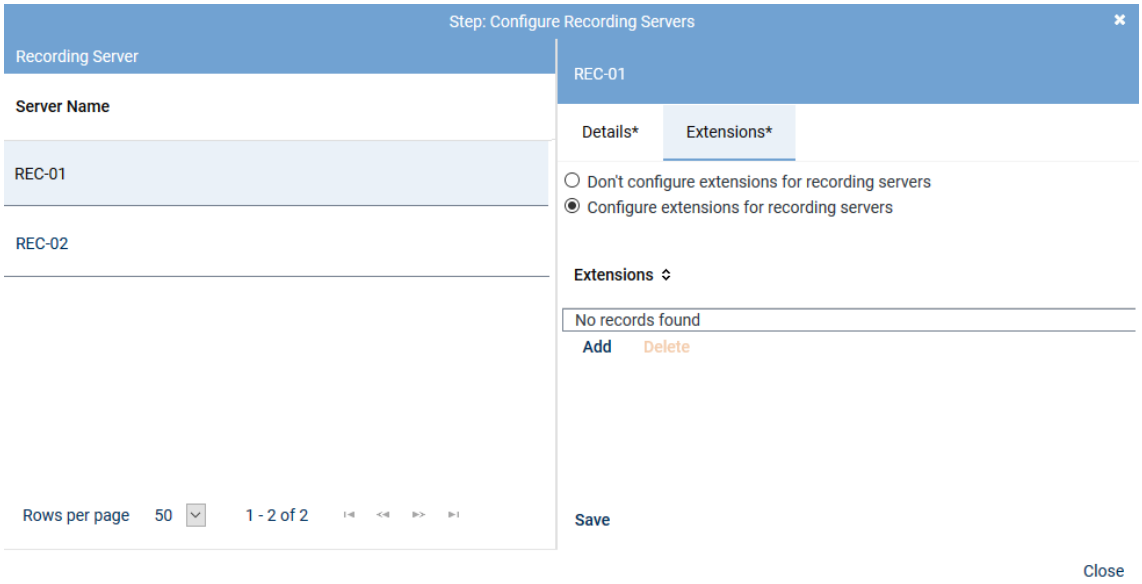


Fig. 340: Tab Extensions

The following options are available:

Configure no extensions for recording servers	Activate this option if you have not configured the extensions for the recording server in the PBX.
Configure extensions of the recording server	Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

2. To add extensions, click on the button *Add* in the table *Extensions*.

   ⇨ The window *Add Extensions* appears.

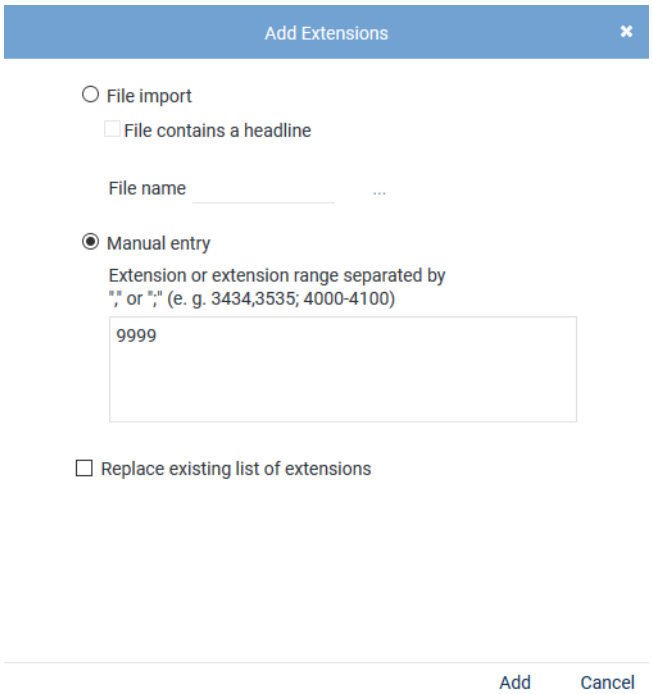


Fig. 341: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

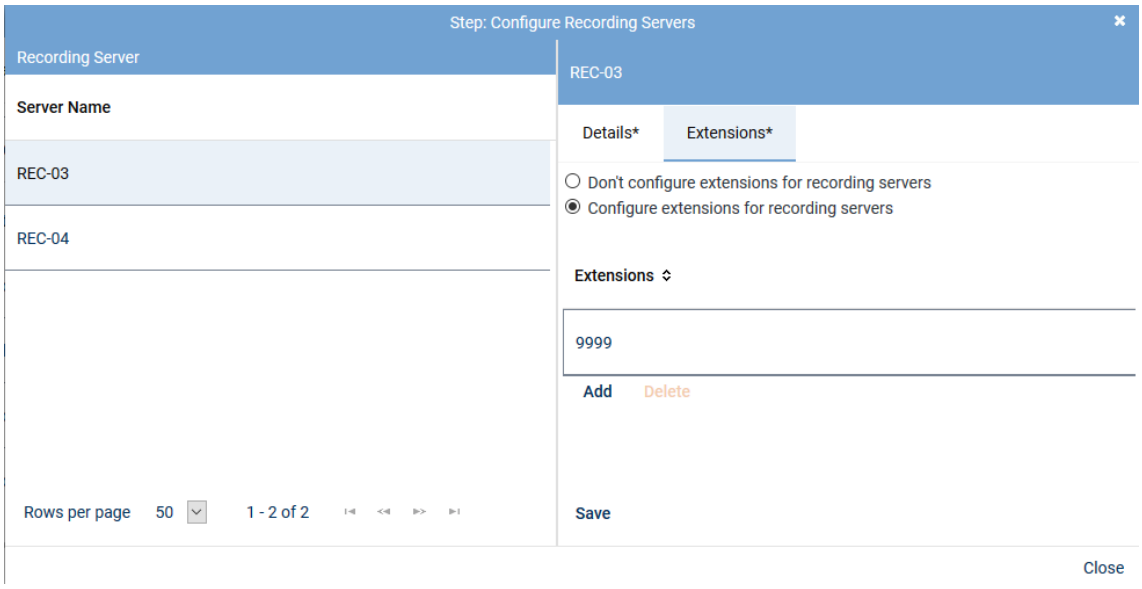


Fig. 342: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.
8. Click on the button *Save*.

9. Click on the button *Close* to finish this configuration step.

Configure add-on

The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

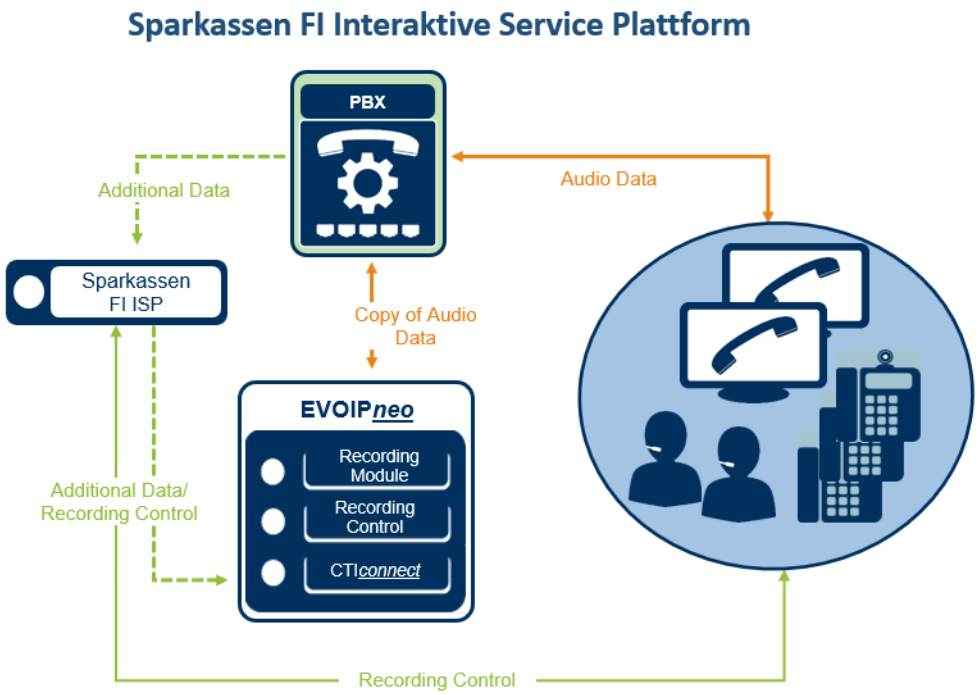


Fig. 343: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

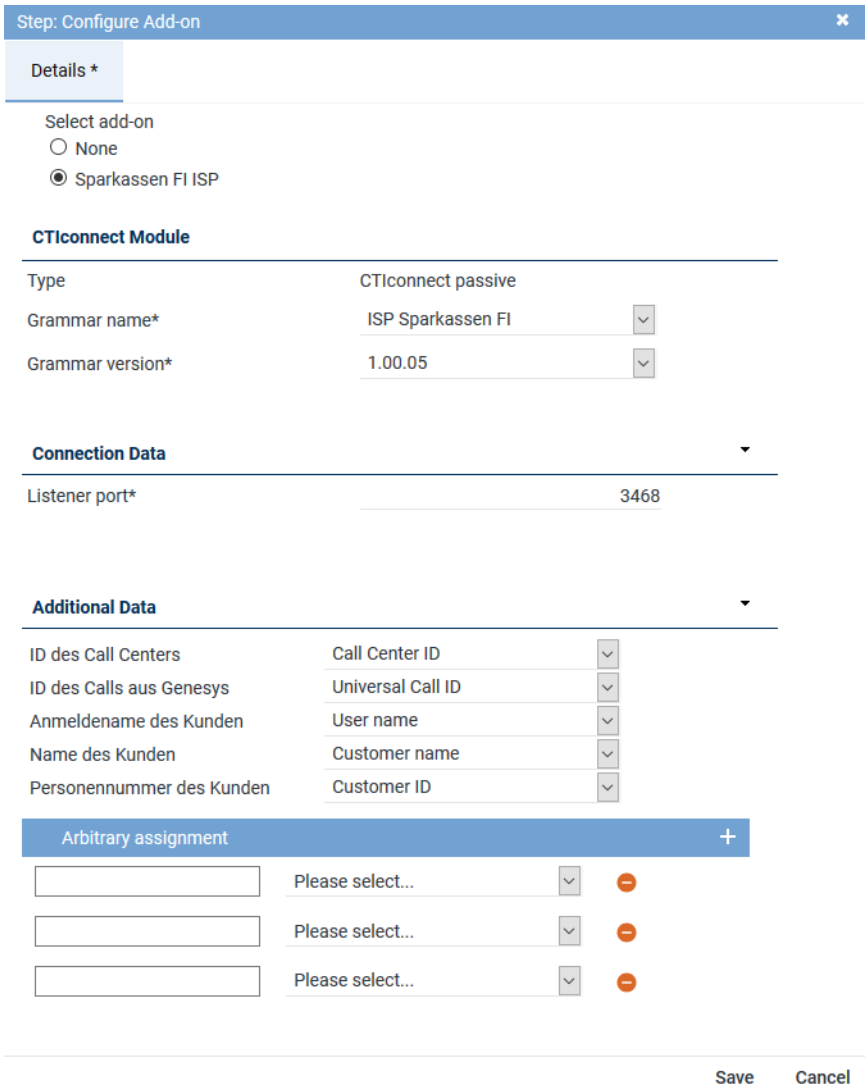


Fig. 344: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 77: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 285.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 78: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

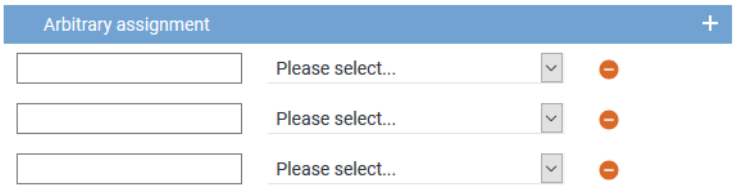


Fig. 345: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.

   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

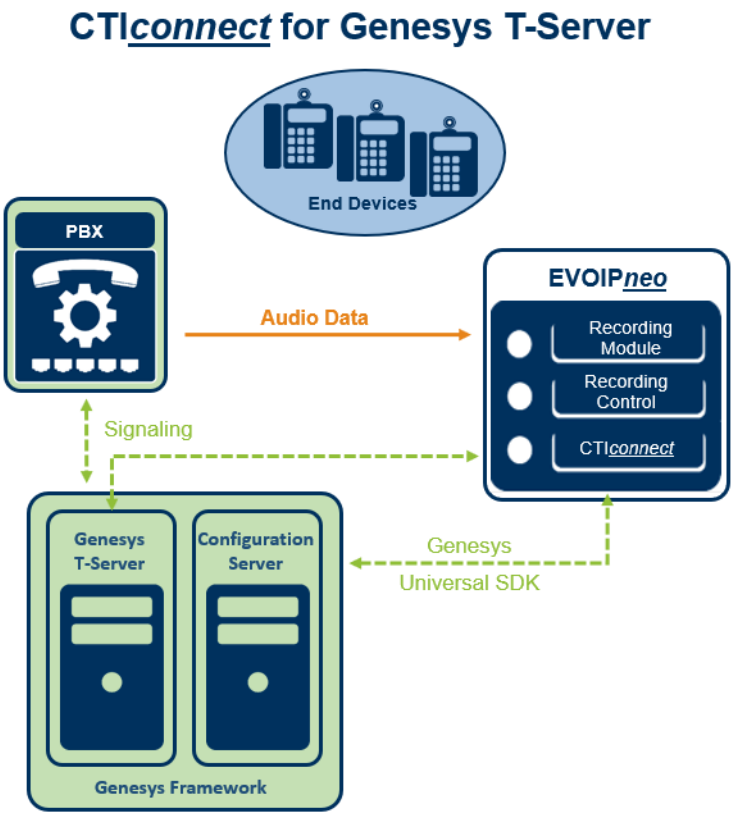


Fig. 346: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

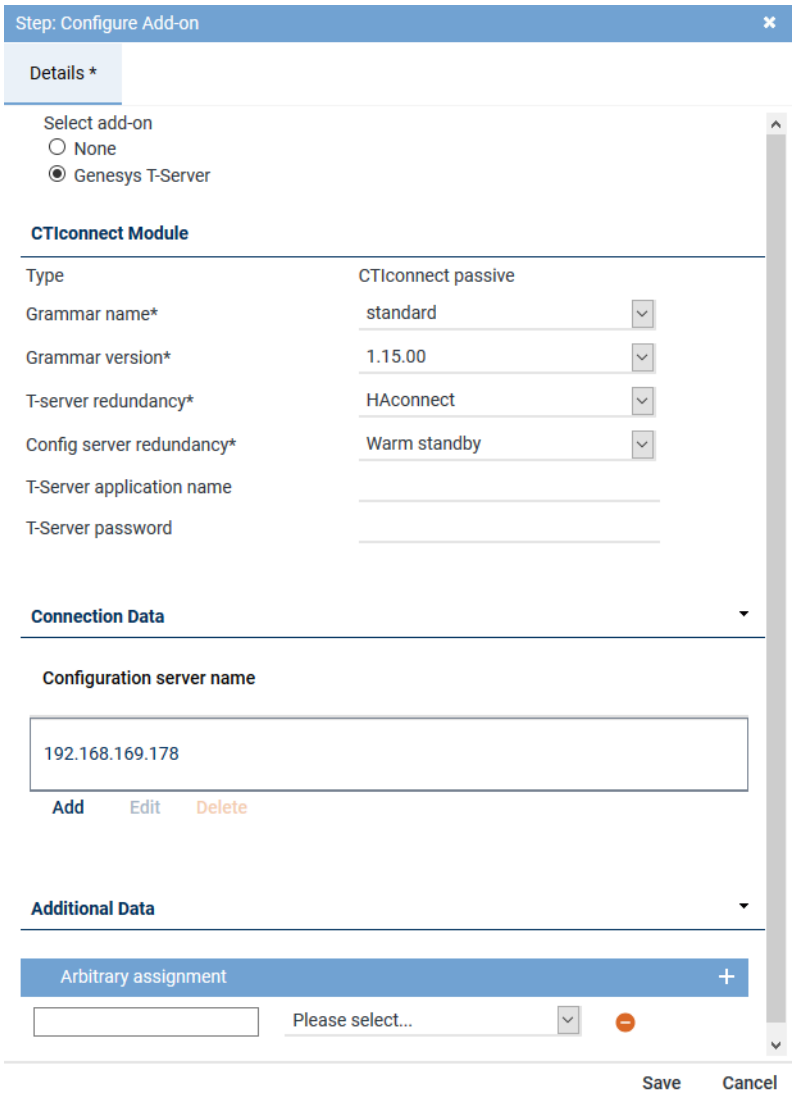


Fig. 347: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 79: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

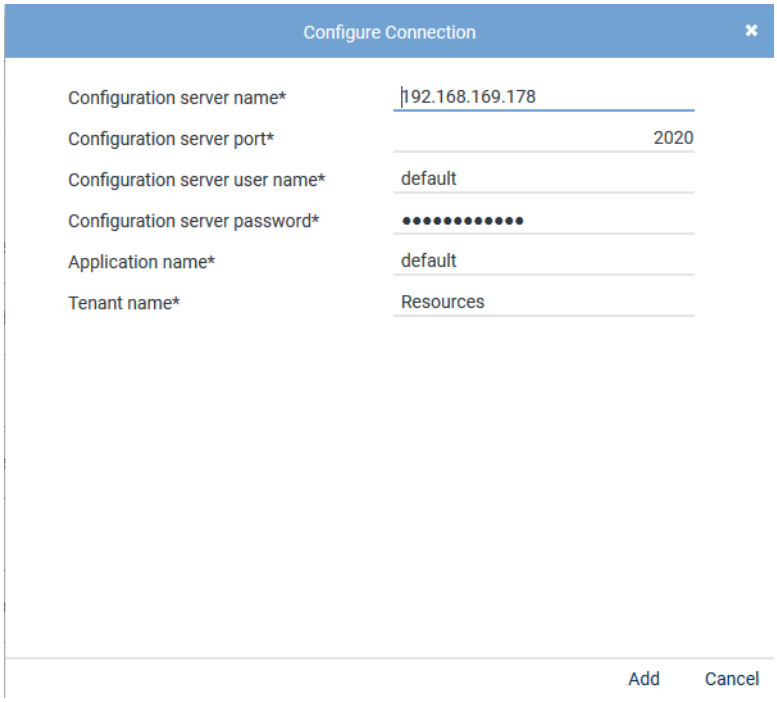


Fig. 348: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 80: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

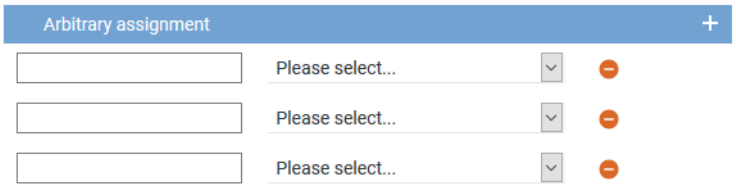


Fig. 349: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

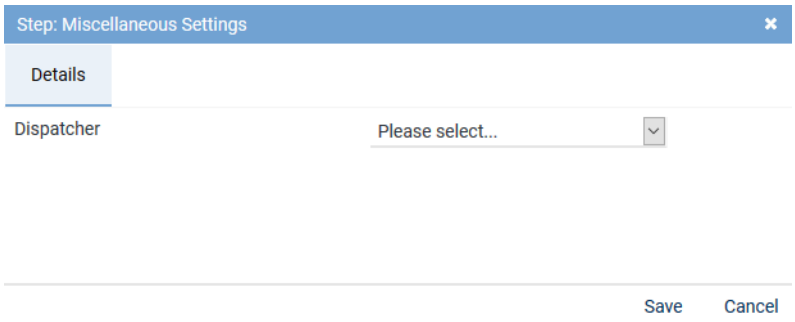


Fig. 350: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

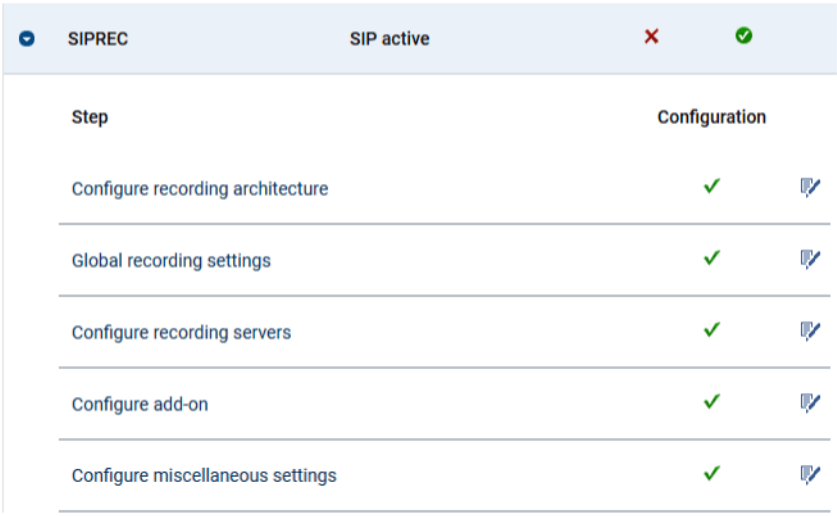


Fig. 351: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

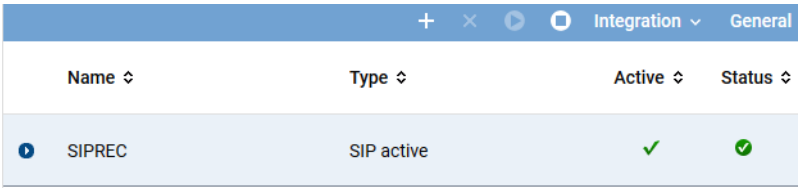


Fig. 352: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

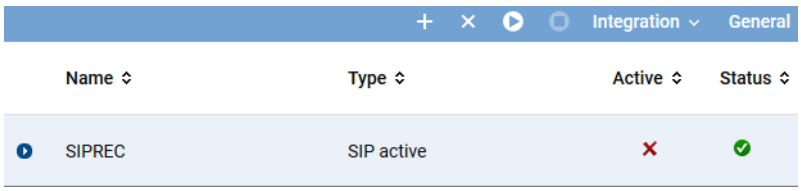


Fig. 353: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.2.6 Configure recording solution Multi-Server Parallel Recording

7.1.2.6.1 Create recording architecture

Start the configuration in the Recording Architectures module because an activated recording architecture is required for further configuration.

The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.

1. Select the menu item *Setup* > *Recording Architectures* in the navigation bar.
   ⇨ The following window appears:

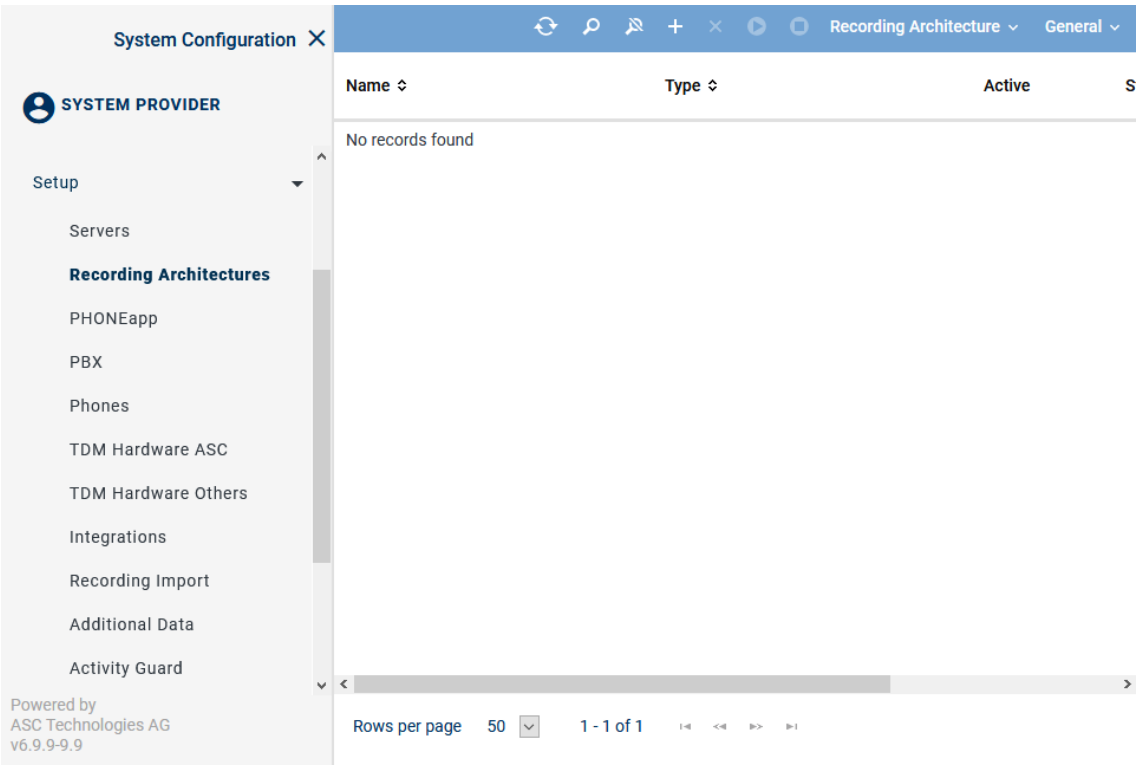


Fig. 354: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon *(Deactivate)* in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon *(Activate)* in the toolbar.
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
Creation Date	Date on which the recording architecture was installed.
Updated	Date on which the settings of the recording architecture were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

Fig. 355: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Create recording architecture Multi-Server Parallel Recording

If there are several recording servers which are supposed to record the same trunks in parallel, you must create a recording architecture of the type *Multi-Server Parallel Recording*.

1. To create a new recording architecture, click on the icon + *(Create)* in the toolbar of the main view.
   ⇨ The window *New Recording Architecture* appears.

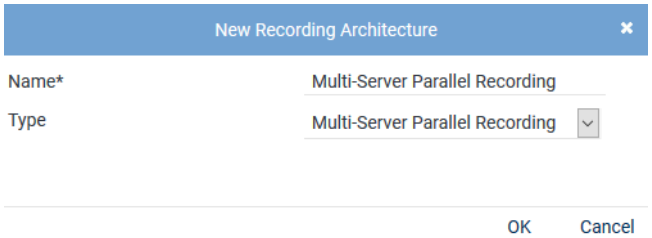


Fig. 356: Create recording architecture - Multi-Server Parallel Recording

2. In the entry field *Name*, enter a descriptive name for the recording architecture.

3. From the drop-down list *Type*, select the recording architecture type *Multi-Server Parallel Recording*.
   NOTICE! Only the supported recording architecture types are displayed in the drop-down list.
4. Click on the button *OK*.
   ⇨ The entries now appear in the detail view.

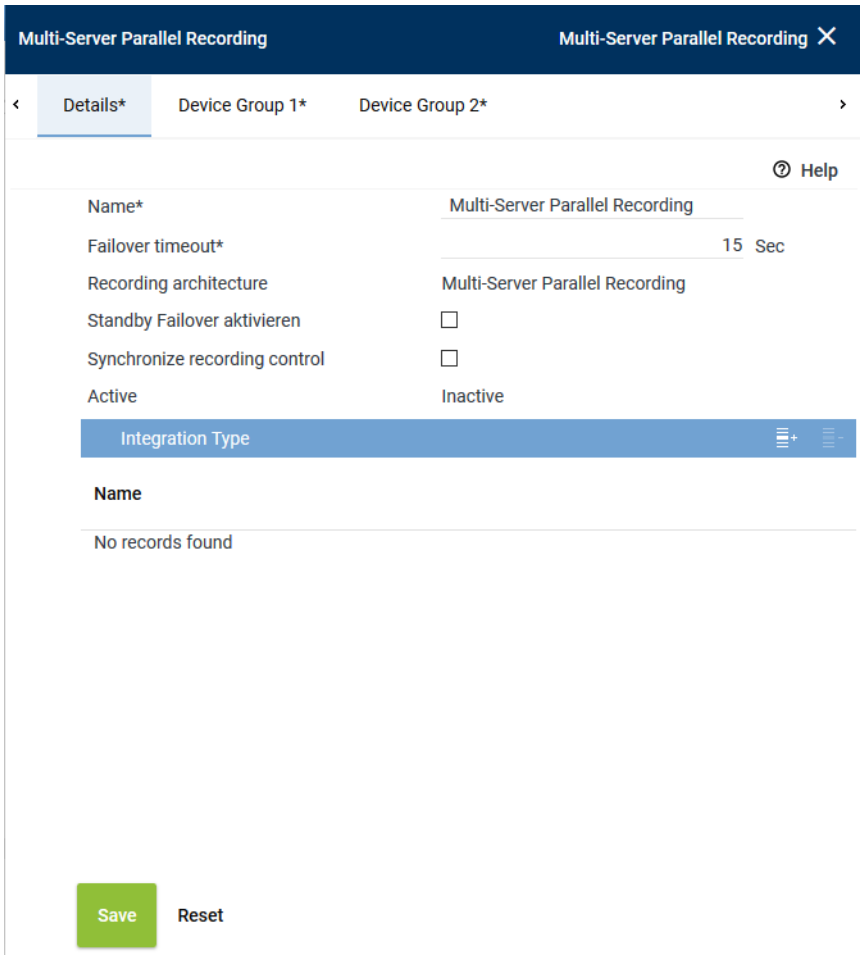


Fig. 357: Recording architecture - tab Details - Multi-Server Parallel Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For more information about the configuration of failover architectures, see chapter "Standby management for failover architectures", p. 373.

ⓘ Set the failover timeout to a minimum of 15 seconds until the failover process is initiated. Depending on the system architecture it may be useful to set the timeout even higher. The timeout defines how long to wait until the failover process is started. If the state switches back to *OK* within this time, the failover process is not initiated.

5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see chapter "Synchronization of recording control", p. 365.

NOTICE! If you have activated the option *Synchronize recording control*, only one set of data is generated in the database but audio data is recorded on both recording servers. This methods makes duplicate detection impossible. Ensure that there is enough storage capacity for twice the amount of data.

If you do not want to synchronize recording control, you can configure duplicate detection, see chapter "Duplicates in parallel recording architectures", p. 369.

Add integration type

1. Click on the icon *(Add)* in the toolbar of the list *Integration Type*.
   ⇨ The window *Integration Type* appears.

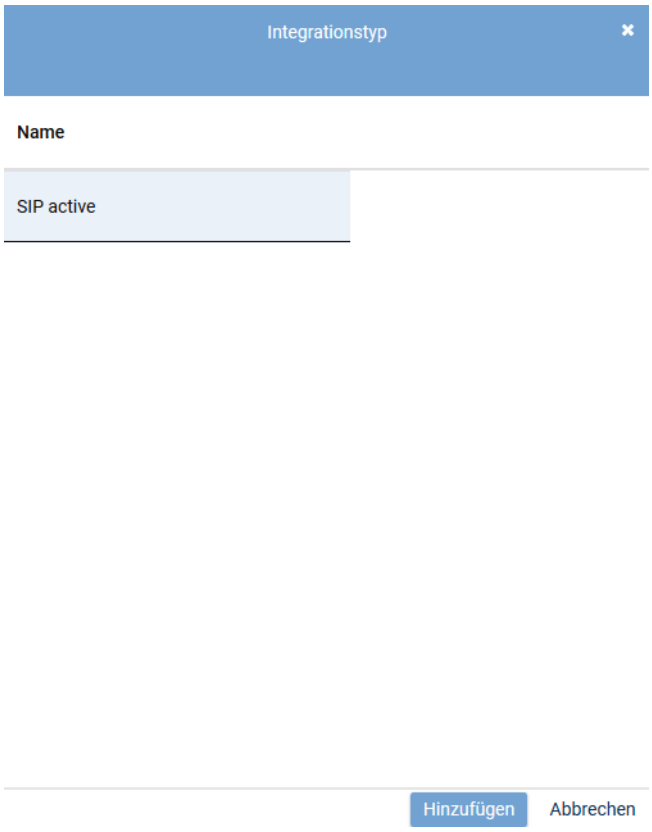


Fig. 358: Select integration type

Only those integration types are displayed which have a license in the system and which support the selected architecture type.

Any number of integration types can be assigned to a recording architecture.

2. Select *SIP active* from the list of the available integration types and click on the button *Add*.
   ⇨ The name of the integration type now appears in the list in the detail window.

Assign server for Multi-Server Parallel Recording

In the architecture type *Multi-Server Parallel Recording* a tab for the configuration of the different servers appears for each device group.

Tab Device Group 1

1. Click on the tab *Device Group 1* to configure the distribution of the recording components for the first device group.

Group field Recording Control and CTI*connect*

In this group field, you can configure recording control. You can configure two different servers or the same server for this.

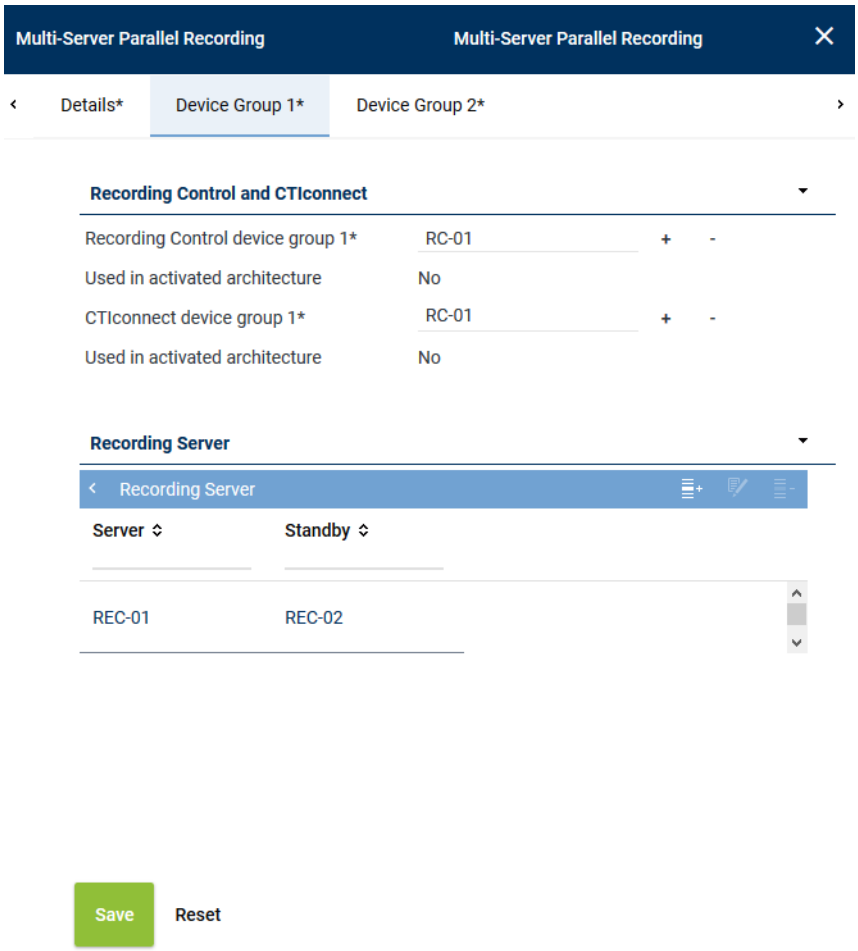


Fig. 359: Recording architecture - server assignment device group 1

1. Click on the button + next to the entry field *Recording Control* to assign a server.
   ⇨ The window *Servers* appears.

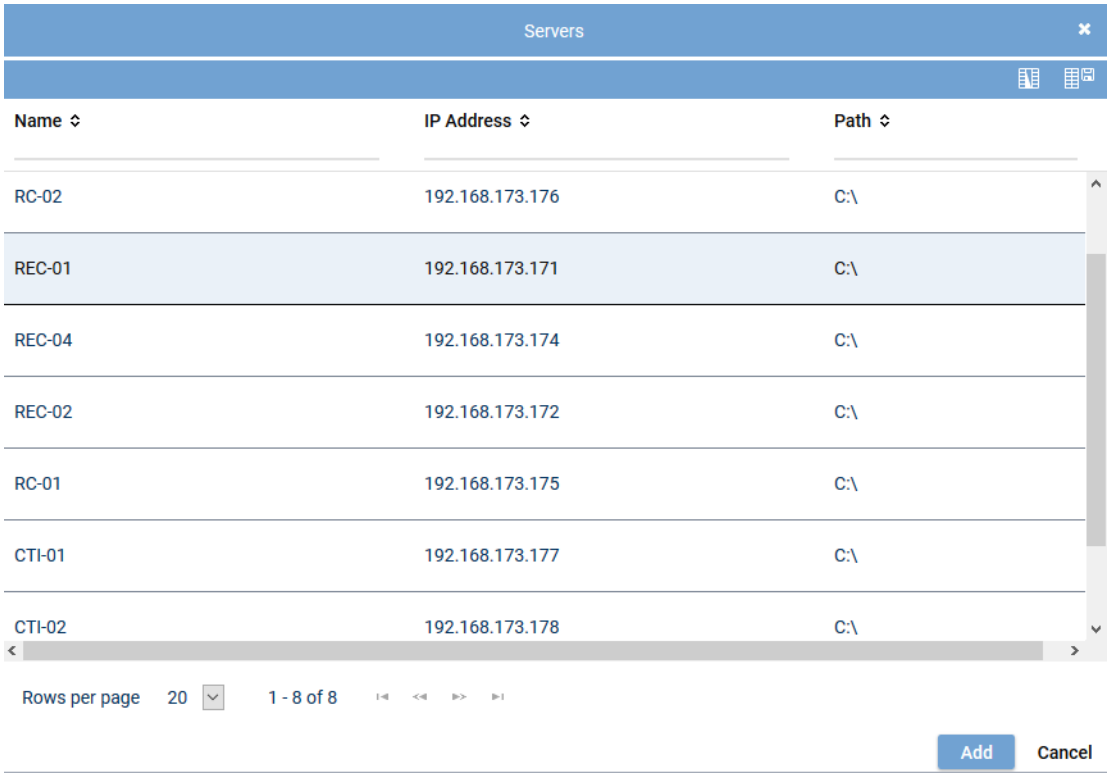


Fig. 360: Recording architecture - assign server - example

2. Select the server for the *Recording Control module*.
3. Click on the button *Add*.
   ⇨ The name of the server appears in the detail view.
4. To delete an assignment, click on the icon - .

A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the CTI*connect module* in the entry field CTI*connect*.

Group field Recording Server

1. Click on the icon in the table headline Recording Server to add a recording server and the standby server.
   ⇨ The following window appears:

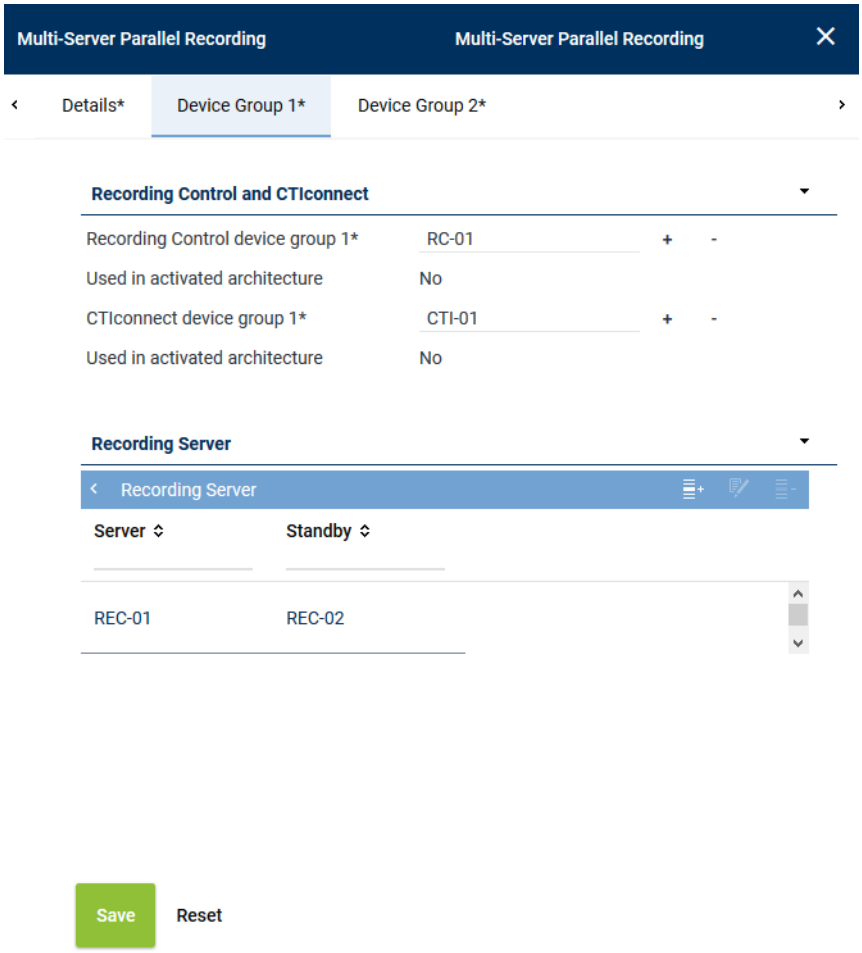


Fig. 361: Add recording server

2. Following the steps described above, go to the entry field *Primary server* and click on the icon + to select the primary server where recording is supposed to be active.
3. In the entry field *Standby server*, click on the icon + to select the standby server which is supposed to do the recording in case of an error.

4. Tick the check box to activate the recording type you would like to use for this server.
   NOTICE! You can activate several recording types if the integration supports them and if the corresponding licenses have been installed.
5. Click on the button *OK* to close the window.
   ⇨ The name of the server appears in the detail view.
6. To edit the assignment subsequently, click on the icon .
   To delete an assignment, click on the icon .
7. If you would like to add additional recording servers repeat the steps described above.

Tab Device Group 2

1. Click on the tab *Device Group 2* to configure the distribution of the recording components for the second device group.
2. Proceed as described in the configuration of tab *Device Group 1*.

In the same device group, you can select the same server for both recording components. For device group 2, you cannot use a server which is already used in device group 1.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon *(Activate)* in the toolbar becomes active.
3. To activate the recording architecture, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

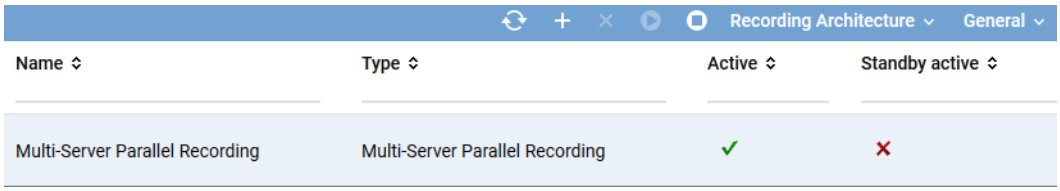


Fig. 362: Recording architecture - activate recording architecture - example

4. To deactivate the recording architecture, if required, click on the icon *(Deactivate)*.
   ⇨ In the column *Active*, the icon ✗ *(Inactive)* appears.

The recording architecture must have been activated so that the integration can be configured.

Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see chapter "Configure duplicate detection", p. 369.

If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.6.2 Configure server

Each server in your network on which the *neo* software has been installed is recognized automatically as a server of the recording system and displayed in the Servers module. In the Servers module, you can configure the purpose of the servers of your recording system.

1. In the navigation bar, select the menu item *Setup* > *Servers*.
   ⇨ The following window appears:

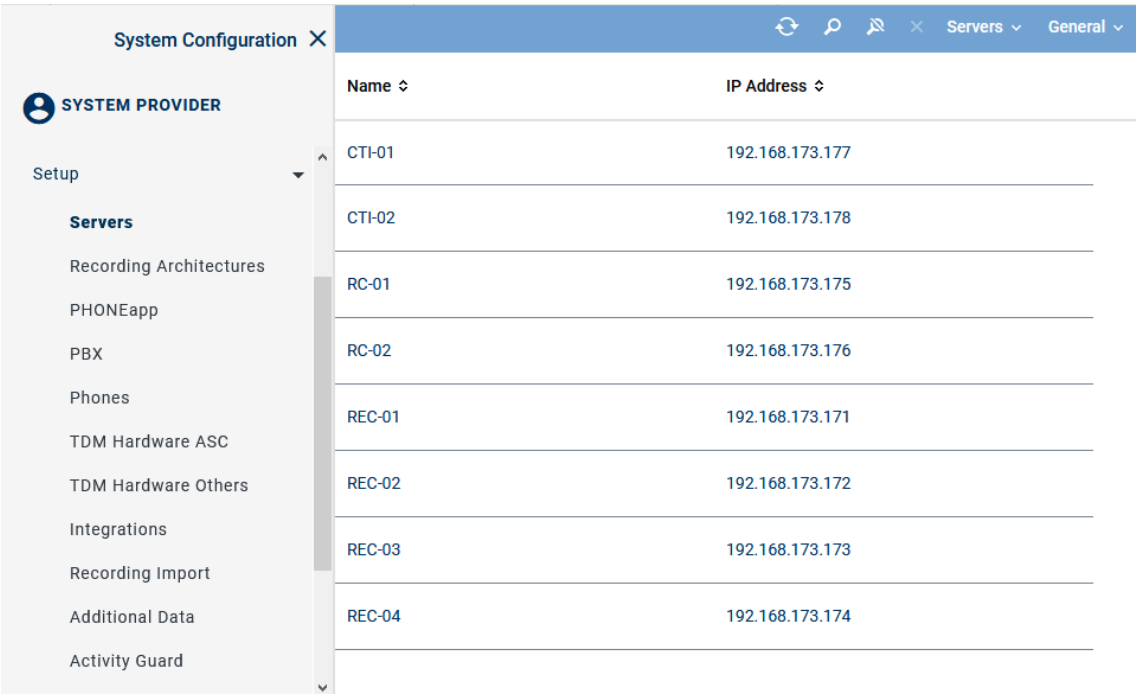


Fig. 363: Servers - main view

Depending on the configuration of the columns, the following information is displayed in the main view:

Name	Shows the name of the server.
IP Address	Shows the IP address of the server.
Path	Shows the path of the server.
Creation Date	Date on which the server was installed.
Updated	Date on which the settings of the server were updated for the last time.

NOTICE! Hidden columns can be added by clicking on the menu item *General* > *Adjust Table*.

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 364: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.

Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 312.
	Administrate NTP Server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Administrate server locations

You can create and manage a list of server locations. In the tab *Details*, you can assign locations to the servers.

Add server locations

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.

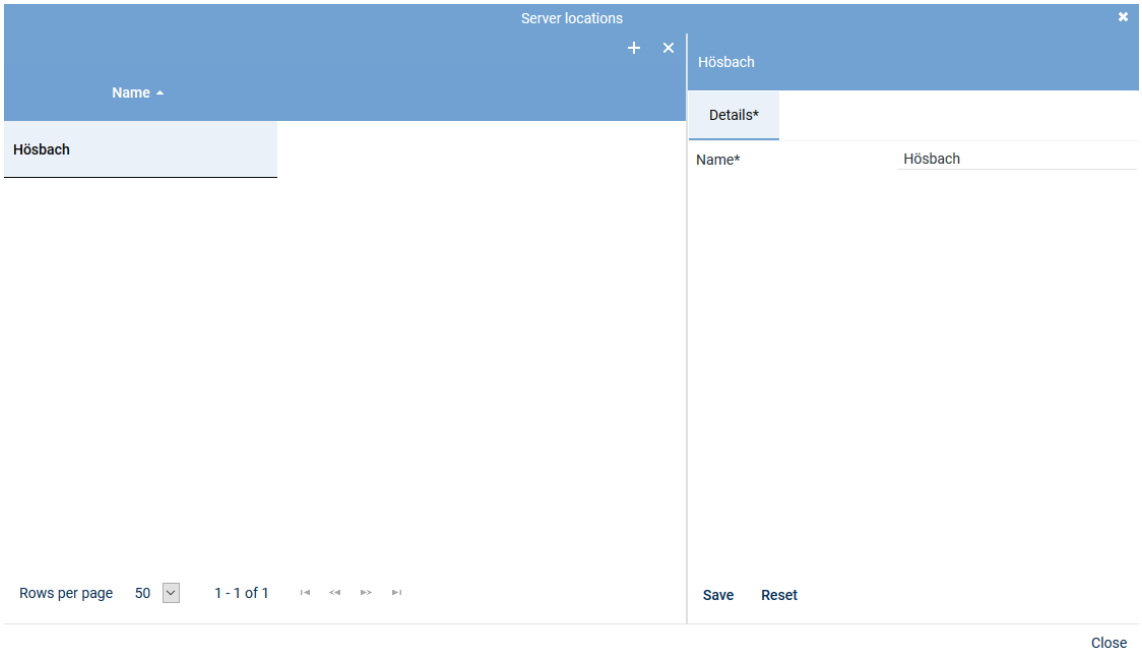


Fig. 365: Add server locations

2. Click on the icon + *(Create)* in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.

4. To save the entry, click on the button *Save*.
   To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

Delete server location

A server location can only be deleted when it has not been assigned. To be able to delete a server location, you must first delete possible assignments.

1. Click on the menu item *Servers* > *Administrate Server Locations* in the toolbar of the main view.
   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

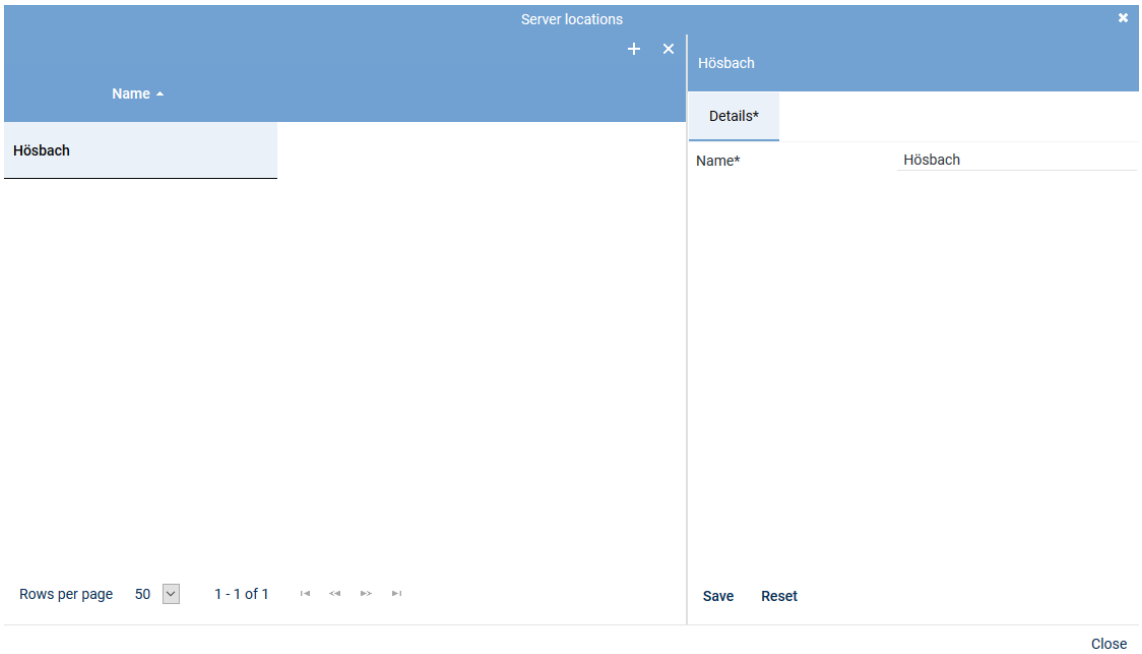


Fig. 366: Delete server location

3. Click on the icon ✕ *(Delete)* in the toolbar of the window.
4. To delete further locations, repeat the last 2 steps.
5. To close the window, click on the button *Close*.

Tab Details

1. To configure the server, select the entry of the corresponding server in the main view.
   ⇨ In the detail view, the tab *Details* appears.
   The information *Name* and *Configured IP address* has already been entered during the installation and is displayed for your information only.

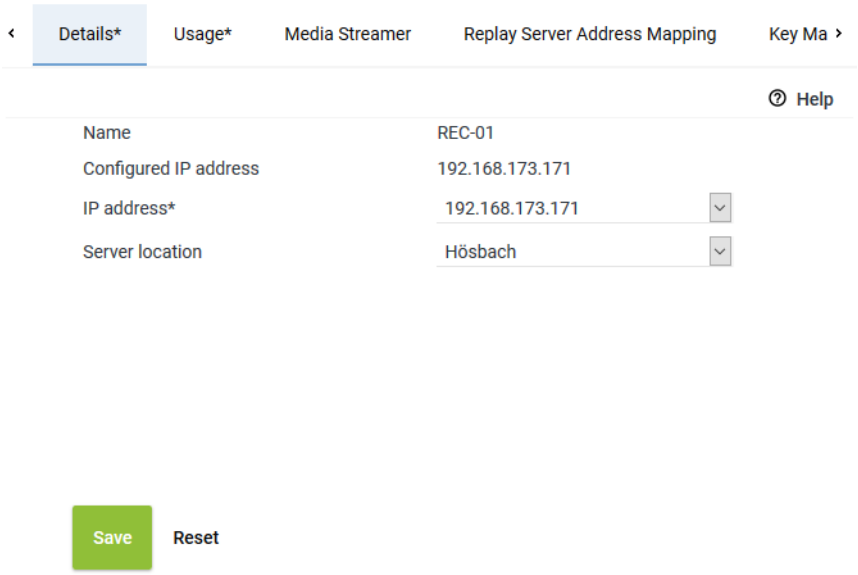


Fig. 367: Servers - tab Details

2. From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
3. Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.
4. Click on the button *Save* if the entries are correct.

Tab Usage

1. Click on the tab *Usage* to configure the intended purpose.

As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

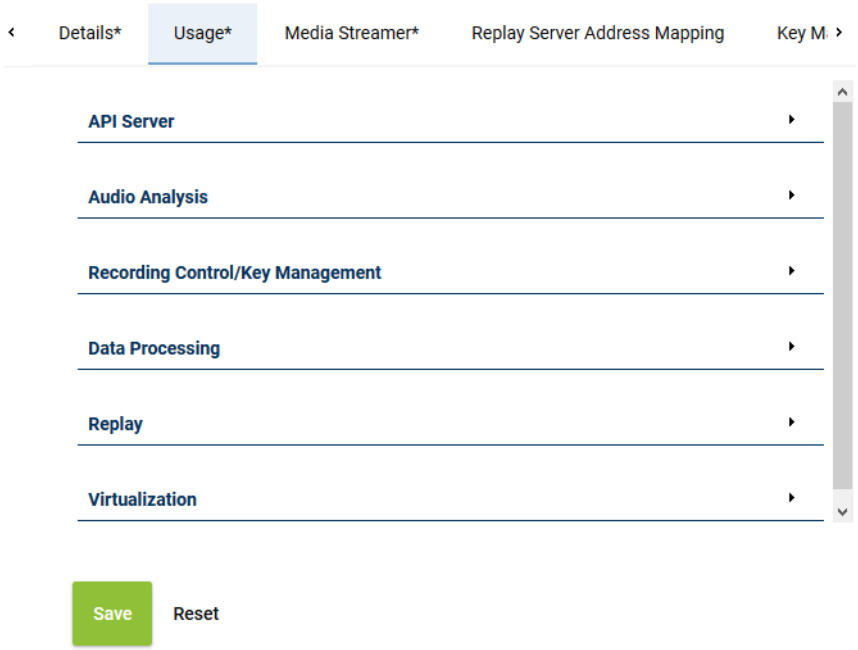


Fig. 368: Servers - tab usage

Group field API Server

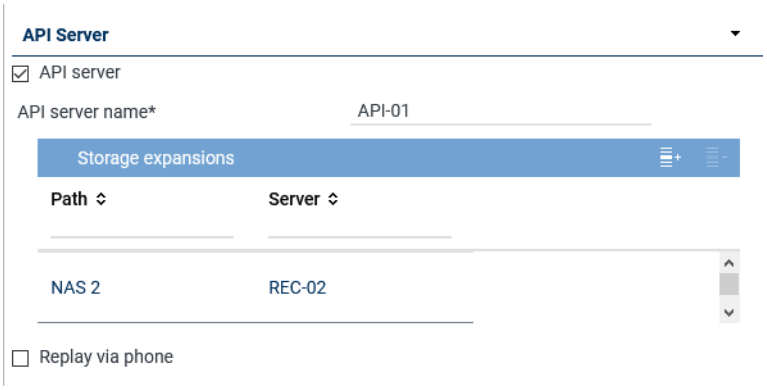


Fig. 369: Group field API Server

The ASC API Server is a service within the *neo* software.

The ASC API Server offers the interface for the client applications to communicate with the *neo* system.

Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

Parameter	Value/Description
API server	Activate the check box to start the ASC API Server. ☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 325.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List Storage expansions	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add storage expansions, see chapter "Add storage expansion for replay", p. 316. • By clicking on the icon *(Remove)*, you can remove storage expansions from the list.

Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone. **NOTICE!** In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 323. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

1. Click on the icon *(Add)* in the toolbar of the list.
2. Select 1 or several storage expansions.
   If you would like to select several storage expansions or revoke a selection, click on the respective line while holding the [Ctrl] key down.

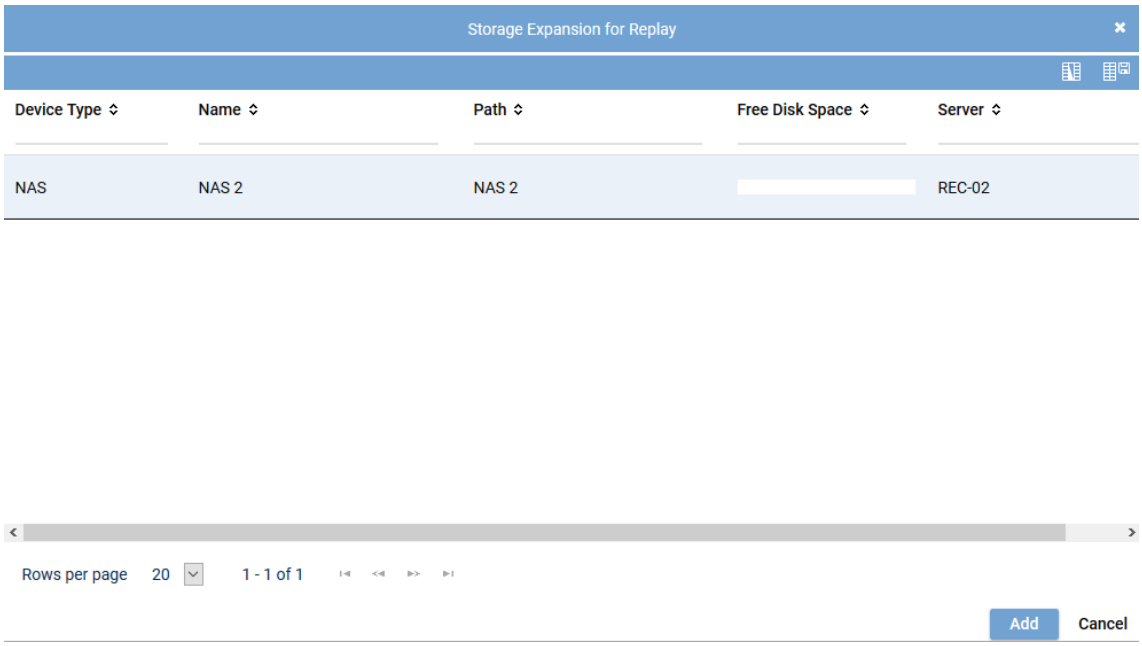


Fig. 370: Select storage expansion

3. To apply the selected storage expansions, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Audio analysis

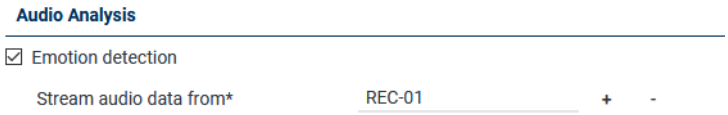


Fig. 371: Group field Audio Analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the emotion detection function. ☐ = Function has not been activated.
Stream audio data from	If the function emotion detection has been activated, the parameter to select the respective server becomes active. • Click on the button + to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.

Tab. 81: Configure audio analysis

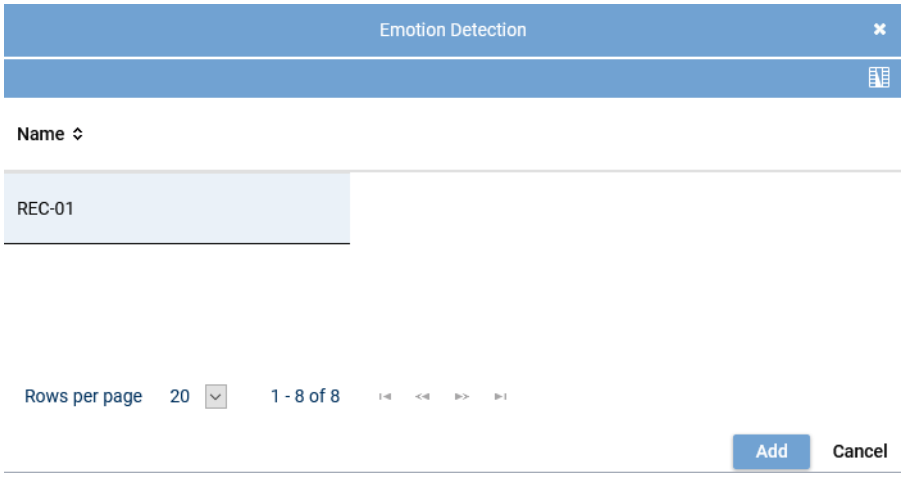


Fig. 372: Select server for emotion detection

1. Click on the button *Add* to apply the selected server.

Group field Recording Control/Key Management

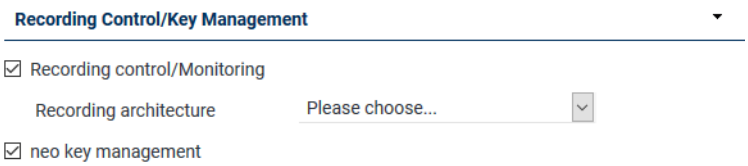


Fig. 373: Group field Recording Control/Key Management

Parameter	Value/Description
Recording control/Monitoring	Activate the check box if you would like to use CLIENT*command* or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated. • Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
neo key management	This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box *Key management*. The function can only be activated if the license *ASC_KEY_MANAGEMENT* is available. For more information about the configuration of key management refer to the administration manual *Configuration server and recording architectures* and to the installation manual *Installation Dongle Manager*.

Tab. 82: Configure recording control/key management

Group field Data Processing

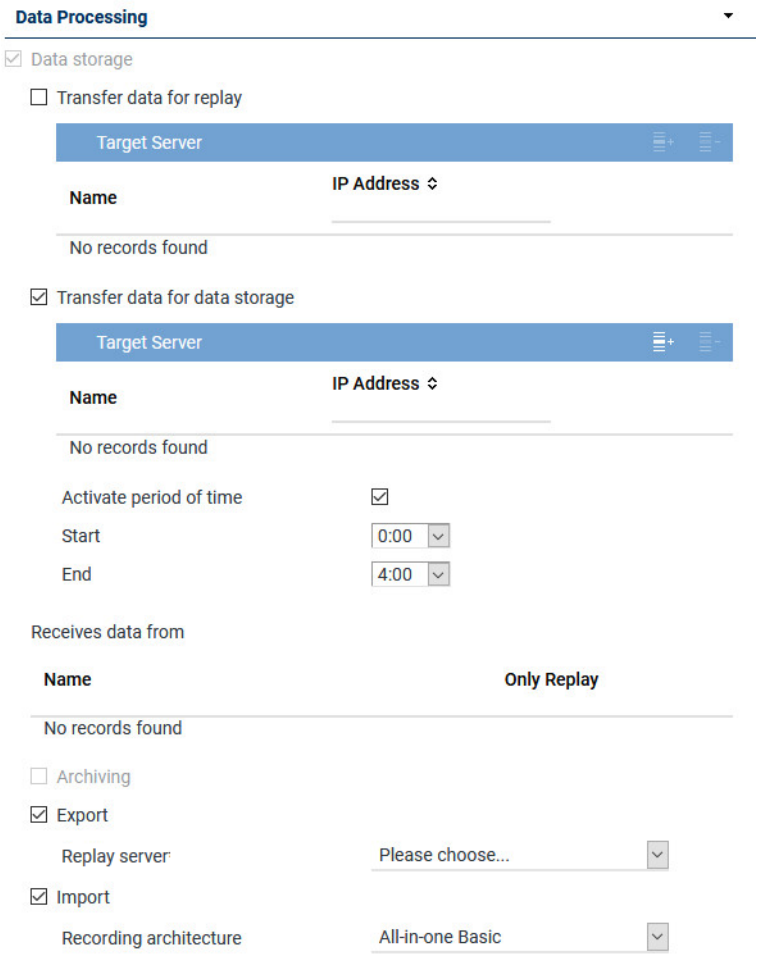


Fig. 374: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to make additional functions of data processing available for editing.
Transfer data for replay	Activate the check box if you would like to transfer the data to another server for replay purposes only. If the function has been activated, you can add a server to the list *Target Server* to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 320. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer the data to be saved on another server. If the function has been activated, you can select a server in the list *Target Server* to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function *data storage* has been activated. The data is copied to the target server and saved there. • By clicking on the icon *(Add)*, you can add the target servers, see chapter "Add target server to a list", p. 320. • By clicking on the icon *(Remove)*, you can remove target servers from the list. **NOTICE!** Only those servers are displayed for which the function *data storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • *Activate period of time* ☑ = Function activated. The fields to enter a time become active. Select the time for from − to by means of the rotating field. • *Activate period of time* ☑ = Function not activated. **NOTICE!** Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed. **NOTICE!** For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.
Receive data from	This table displays servers which transfer data to this server. The column *Name* displays the server name from which data is transferred. The column *Only Replay* displays the purpose of the transfer: ✓ = Data is transferred for replay only. ✗ = Data is transferred for data storage.

Parameter	Value/Description
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server. • *Replay server* From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers. **NOTICE!** For the export from *neo* to *neo*, you do not have to select a replay server.
Import	Activate the check box *Import* so that the imported data can be saved on this server. • *Recording architecture* From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function. **NOTICE!** If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 83: Data storage

Add target server to a list

1. In the toolbar of the list *Target Server*, click on the icon *(Add)*.
2. Select the server from the list to which you would like to transfer the data.
   If you would like to select several servers or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Fig. 375: Select server

Only those servers are available on which the function *Data storage* has been activated.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Replay

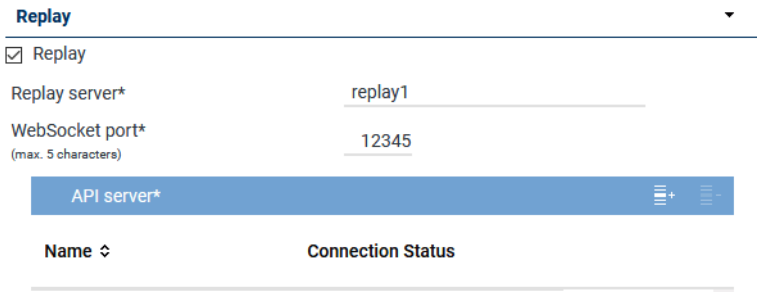


Fig. 376: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings:

Parameter	Value/Description
	• By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 322. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 84: Configure replay

Search and replay functions

To be able to use the search and replay functions via LCR as well as to use replay via phone, you have to create the users with the respective access rights in the application System Configuration in the Employees module. For information about the configuration refer to the administration manual *User management* for tenants.

Add API server to a list

The replay server required the services of an API server. The configuration must be as follows:

- If the replay server runs on a server with a local API server, it must not necessarily be assigned as the replay server always addresses the local API server first.
- If the replay server runs on a separate server, you must assign at least one API server that the replay server can address.
- If several API servers are available in the network, you can assign further API servers in addition to the local API server. The assigned API servers are addressed in order. For this reason, the local API server should always be first in the list.

1. To assign an API server, click on the icon *(Add)* in the toolbar of the list *API Server*.
2. Select the server from the list on which the API service is running.

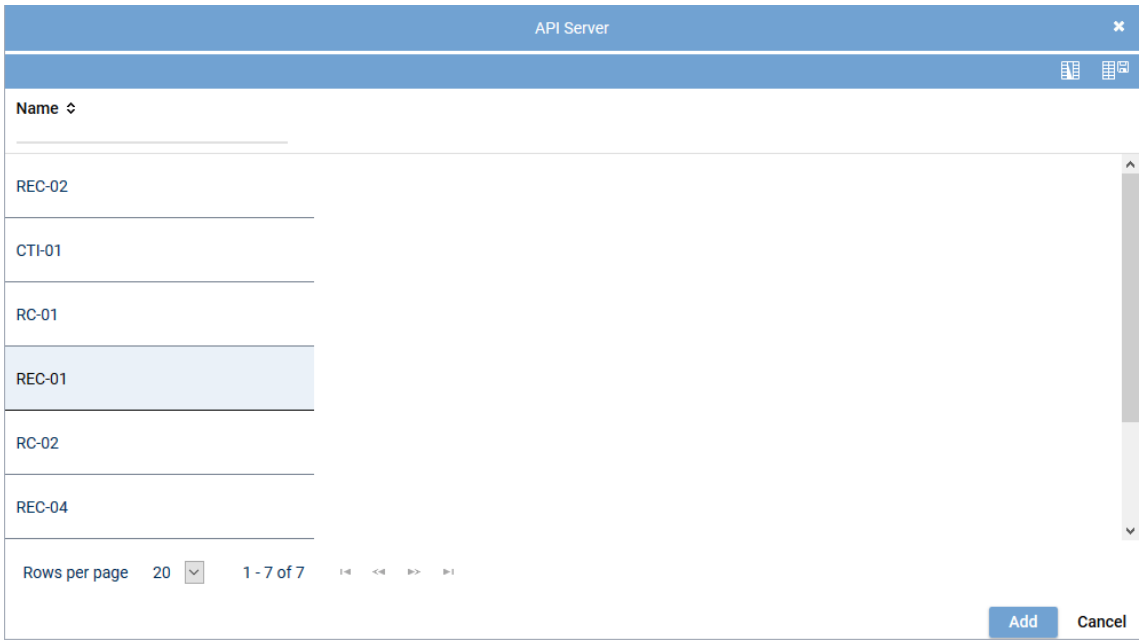


Fig. 377: Select server

Only those servers are available on which the API service has been installed and activated. See chapter "Group field API Server", p. 315.

3. To apply the selected servers, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

Group field Virtualization

Fig. 378: Group field Virtualization

Parameter	Value/Description
VM without Trusted License	This functionality can only be activated if the system runs in a virtual environment and if no *TRUSTED_VIRTUALIZATION* license has been installed. When you tick the check box *VM without Trusted License*, the tab *Keystore/Virtualization* becomes active and must be completed. There, you can configure the following options: • *licensing.asc.de* If you enter this domain, there is no key management. • *IP address of the DongleMan* If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 85: Configure virtulization

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

For *virtualization* without an Internet connection, a Trusted License is required.

1. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab Media Streamer

1. Click on the tab *Media Streamer* in the detail view.

In this tab, you can configure the Media Streamer for the functionalities *Replay via phone* and *Last Call Repeat Facility*.

The tab *Media Streamer* is only active if the function *Replay via phone* has been activated in the tab *Usage*.

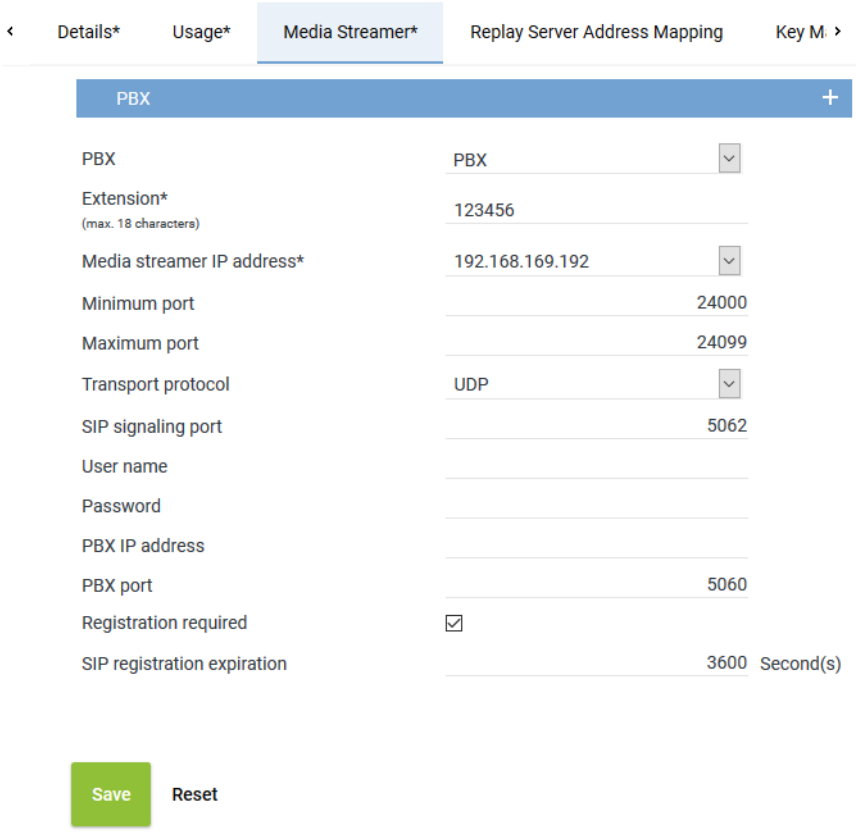


Fig. 379: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system. If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 330.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.
Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange. Enter an even number.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. Enter an uneven number.

	A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses. **NOTICE! The port range must not have less than 64 ports.**
Transport protocol	From the drop-down list, select the transport protocol type you would like to use for the SIP communication. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

1. Click on the tab *Replay Server Address Mapping* in the detail view.

In this tab, you can configure the replay server address mapping. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.

ⓘ The tab *Replay Server Address Mapping* is only active if the function *Replay* has been enabled in the tab *Usage*.

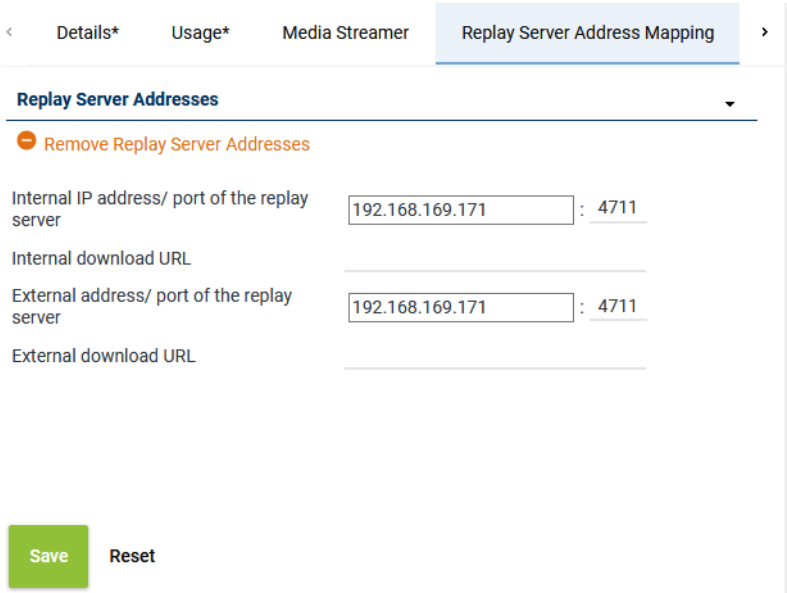


Fig. 380: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

Internal IP address/ port of the replay server	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
Internal download URL	Enter the URL and the port of the replay server under which the Replay module can be reached internally, e. g.: `https://example.company.com:4711/`
External address / Port of the replay server	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network. When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.
External download URL	Enter the URL and the port under which the Replay module can be reached via the browser from outside the local network, e. g.: `https://example.company.com:4711/` When entering the external address take into consideration whether the SSL certificate has been issued for an IP address or a DNS address. In the latter case, entering the DNS name is mandatory; otherwise the certificate check in the replay application will fail.

If you would like to remove the addresses, click on the icon ✕ in the title bar of the group field.

ⓘ If address mapping has been configured, the Replay module receives the configured address and the configured port.

If address mapping has not been configured, the Replay module receives the IP address and the default port *4040* as entered in the tab *Details*.

ⓘ To allow the users of the respective tenant to access the replay server via the browser, an internal address and/or an external IP address or a DNS name must be configured in the Tenants module.

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

1. Click on the tab *Key Management* in the detail view.

In this tab, you can configure the settings for the *neo* key management. This tab is only active if you have installed the corresponding license and enabled the function *neo Key Management* in the tab *Usage*.

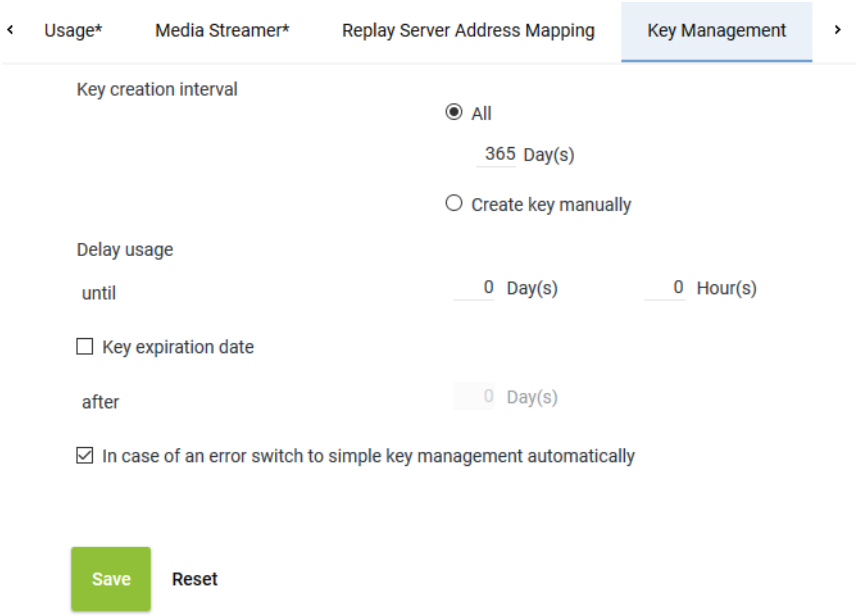


Fig. 381: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.
Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid.

	☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it. **CAUTION!** All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

On top of the settings in this tab, each tenant who would like to use the *neo* key management has to define individual settings in his own user management (Tenants module).

For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Keystore/Virtualization

1. Click on the tab *Keystore/Virtualization* in the detail view.

In this tab, you can configure the connection data to the service *DongleMan* for key management and authentication of the VMware.

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

For key management there are the following options:

- *Dongle*
  You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.
  In this case, no separate configuration is required.
  In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*
  In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*
  NOTICE! License Management does not support encryption.

For licensing, there are the following options:

Without Internet access:

- *Dongle*
  Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.
  In this case, no separate configuration is required.
- *Trusted Virtualization License*
  Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.
  In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*
  You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.

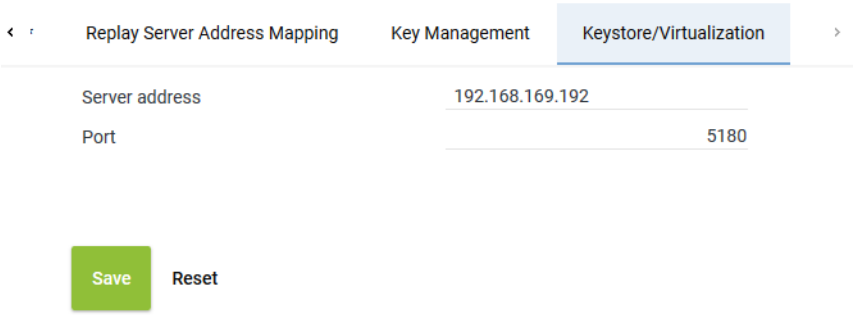


Fig. 382: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for the connection. • If you use the hardware with neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service *DongleMan* has been installed. • If you use the VM without neo key management, you can authenticate the VM via ASC License Management System, too. In this case, enter the following address: *licensing.asc.de* • If you use the VM with *TRUSTED_VIRTUALIZATION* license and neo key management: IP address of the server where the service *DongleMan* has been installed.
Port	Enter the port for the connection. *5180* = Dongle Manager *8181* = ASC License Management System

For detailed information about how to configure virtualization and key management refer to the administration manual *Encryption of recordings*.

1. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.6.3 Create PBX

The PBX can either be configured via the PBX module or via the Integrations module.

In this configuration step, the parameters for the PBX are configured, e. g. the name, the area code and the net code.

1. Select the menu item *Setup* > *PBX* in the navigation bar.
   ⇨ The following window appears:

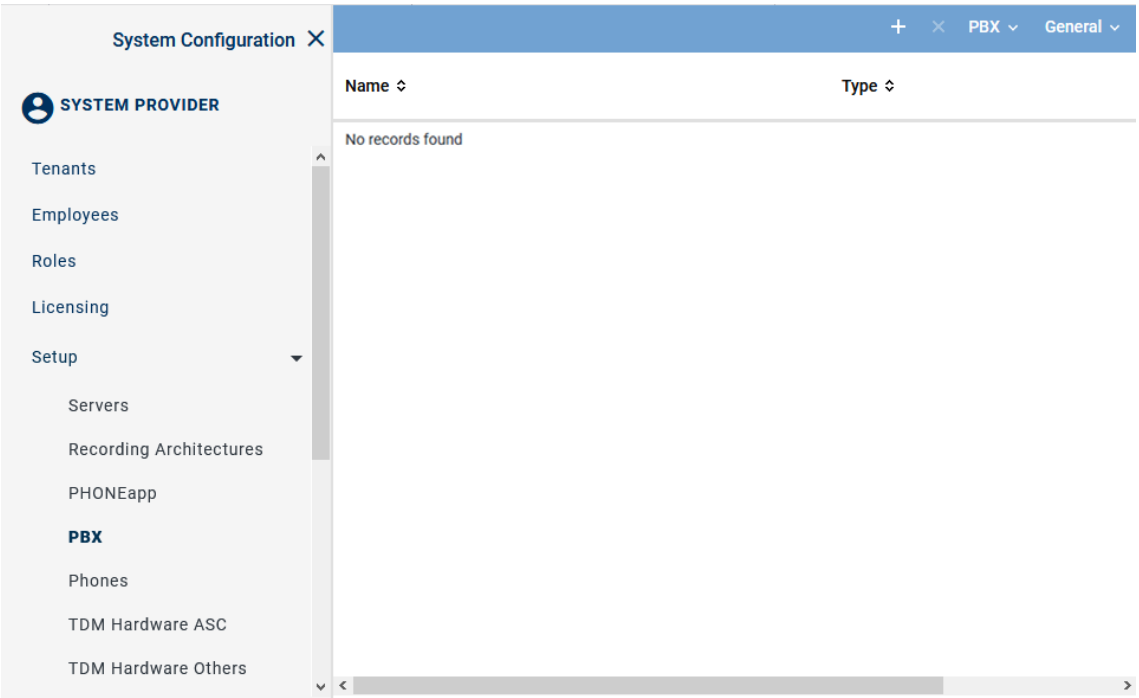


Fig. 383: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 384: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	General Help	Opens the online help.

Module Help	Opens the module-specific online help.

For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

Create new PBX

1. Click on the icon + *(Create)* in the toolbar of the main view of the PBX module.
   ⇨ In the detail view, the tab *Details* appears.

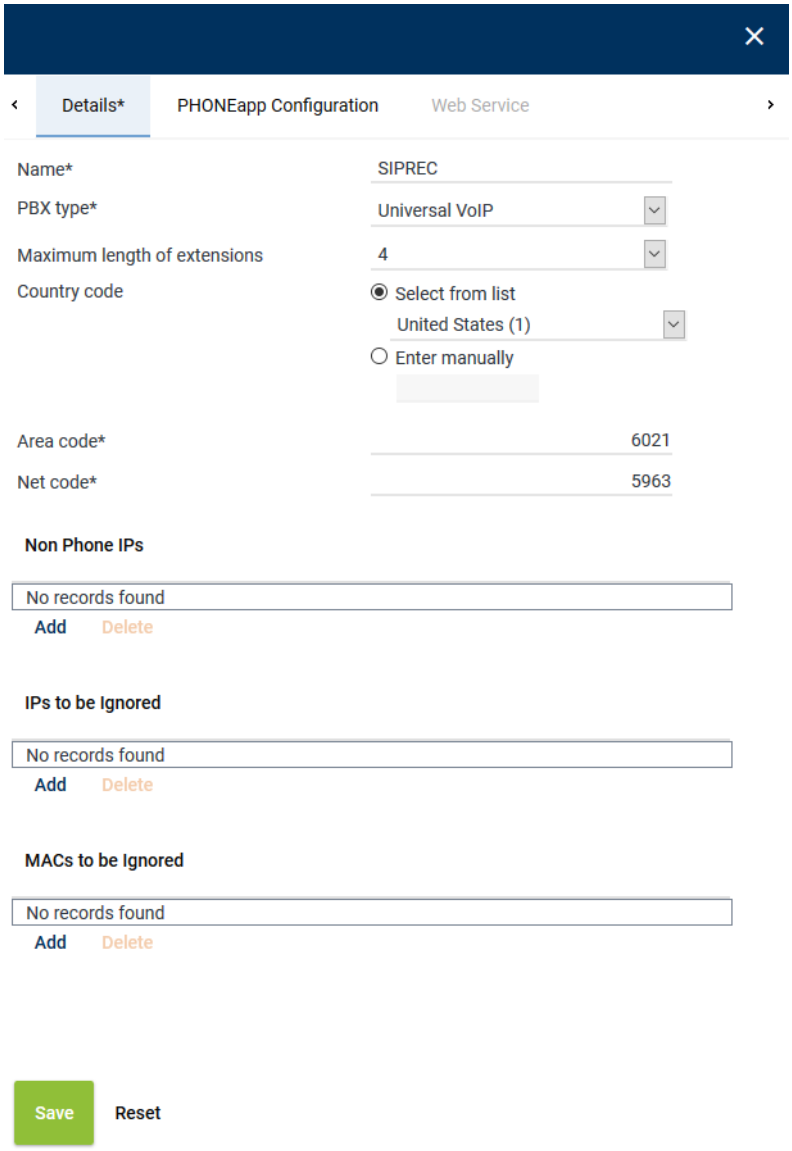


Fig. 385: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code: • *Select from list*

Parameter	Value/Description
	Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 86: Create PBX

If you would like to display the complete phone number, e. g. if you use more than one PBX, several area codes, or if you would like to record mobile phones, you have to configure the value *0* in the following parameters:

Parameter	Value/Description
Maximum length of the extensions	Enter the number *0* in the field maximum length of the extensions to display the complete phone number.
Area code	Enter the number *0* as area code to display the complete phone number.
Net code	Enter the number *0* as net code to display the complete phone number.

Tab. 87: PBX parameters with complete phone number

3. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

7.1.2.6.4 Assign recording resources

Resources for tenants

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities. For information about the configuration of chat systems refer to the respective manual.

Assign extensions to tenants

If you would like to assign resources based on extensions, you can assign the tenant the extensions intended for recording in the Tenants module.

1. Select the menu item *Tenants* in the navigation bar.

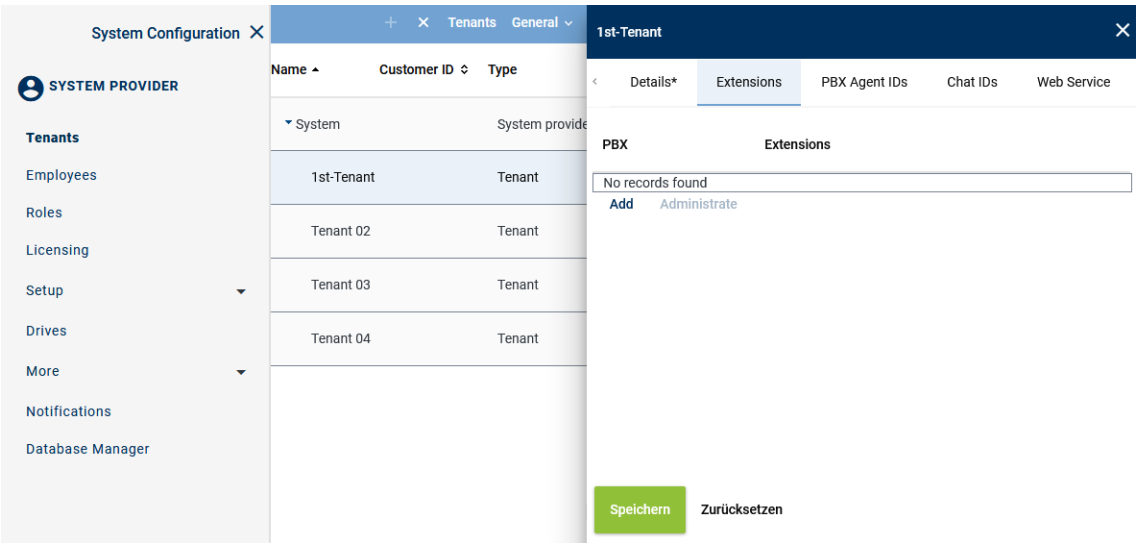


Fig. 386: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.
   ⇨ The following window appears:

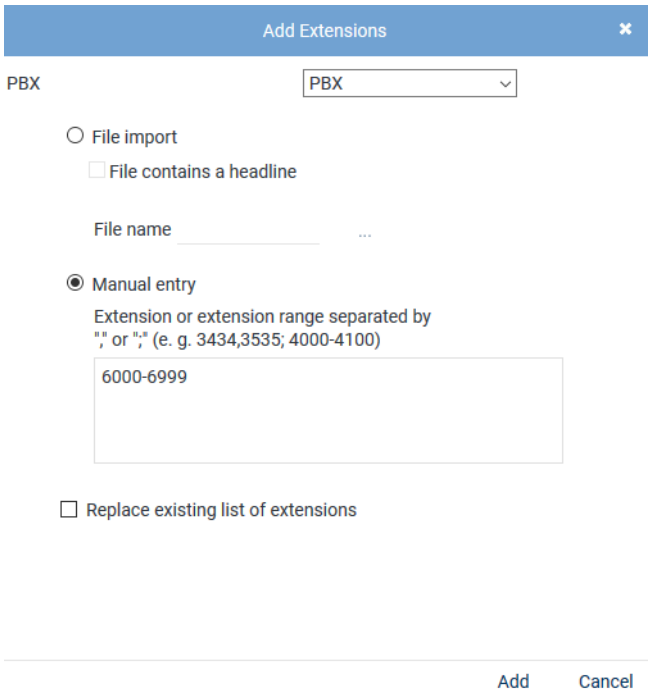


Fig. 387: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT*

	• *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually. To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove extensions

1. In the list, select the PBX for which you would like to remove the assigned extensions.

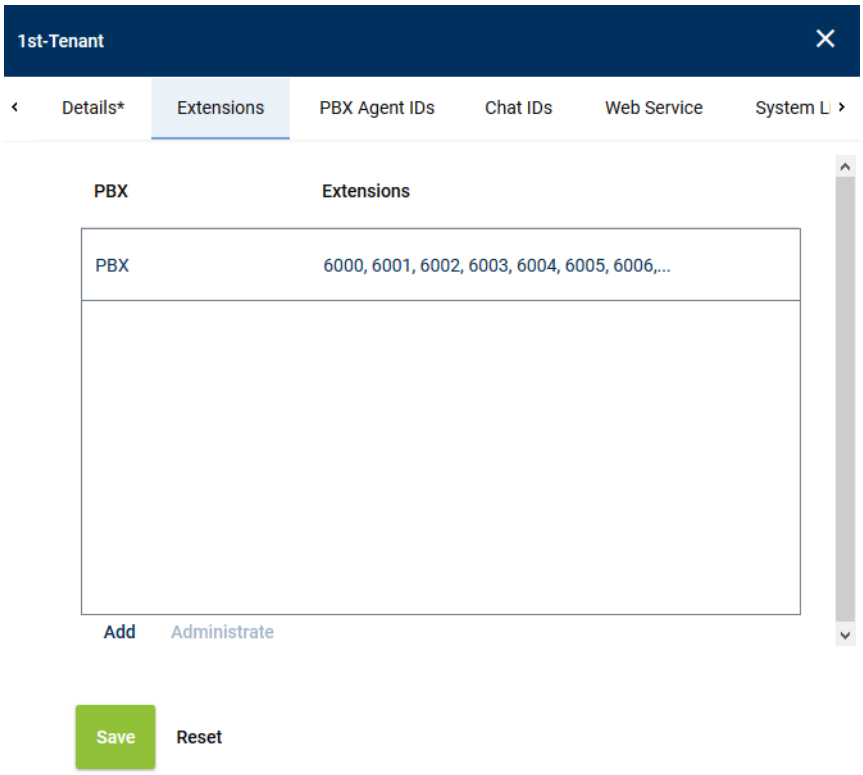


Fig. 388: Remove extensions

2. Click the button *Administrate*.
3. Select one or several extensions you would like to remove from the assignment.
   To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Fig. 389: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

Assign PBX Agent IDs to tenants

If the information about PBX Agent IDs is delivered by the PBX, you can make an assignment by means of the PBX Agent IDs. In this case, you can assign the respective tenant the PBX Agent IDs designated for recording in the Tenants module.

In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.

In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.

1. Select the menu item *Tenants* in the navigation bar.

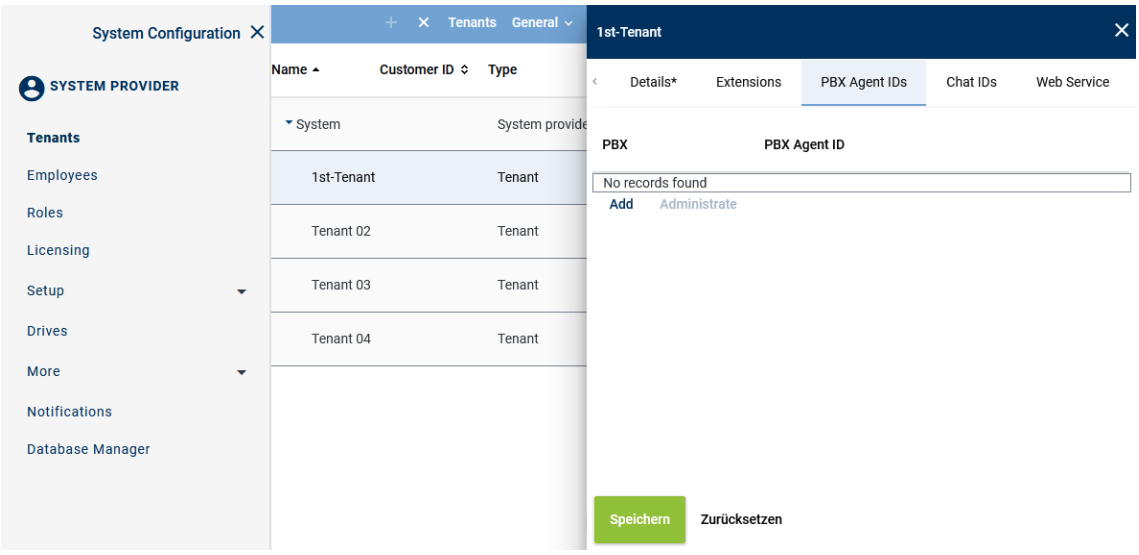


Fig. 390: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

1. In the main view, select the tenant to whom you would like to assign the PBX Agent IDs.
2. Click on the tab *PBX Agent IDs*.
3. Click on the button *Add*.
   ⇨ The following window appears:

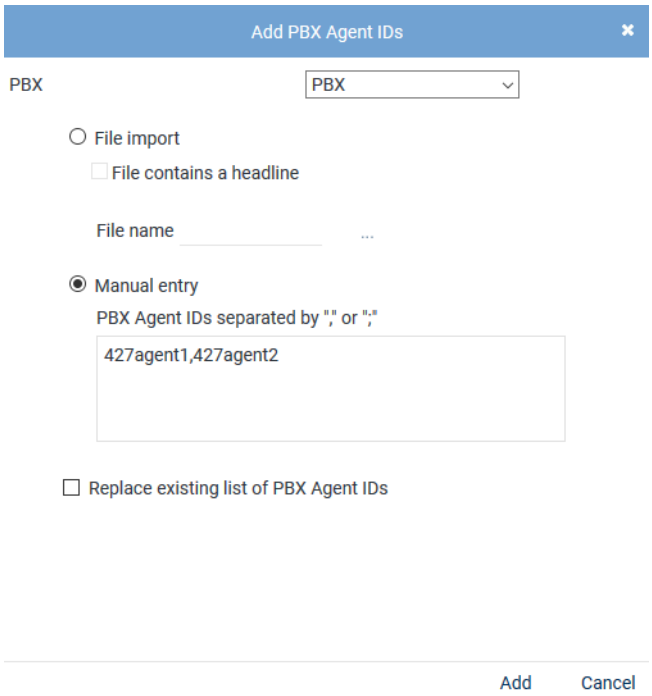


Fig. 391: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

Remove PBX Agent ID

1. In the list, select the PBX for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
   To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

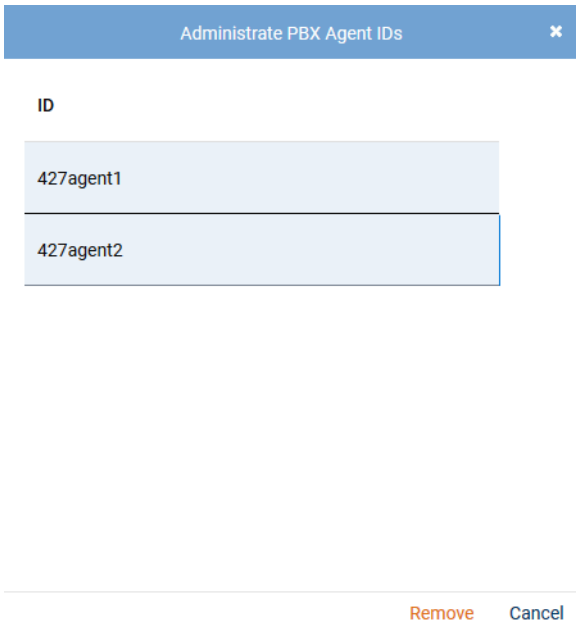


Fig. 392: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
   To cancel the process and close the window, click on the button *Cancel*.

7.1.2.6.5 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation with a protocol.

ⓘ In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured here in the Additional Data module. Only then can you map the additional data in the integration under the Global Recording Settings in the tab *SIP Header Tagging*.

For selection fields to appear in the drop-down list, they have to be configured in the Additional Data module.

1. Select the menu item *Setup* > *Additional Data* in the navigation bar.

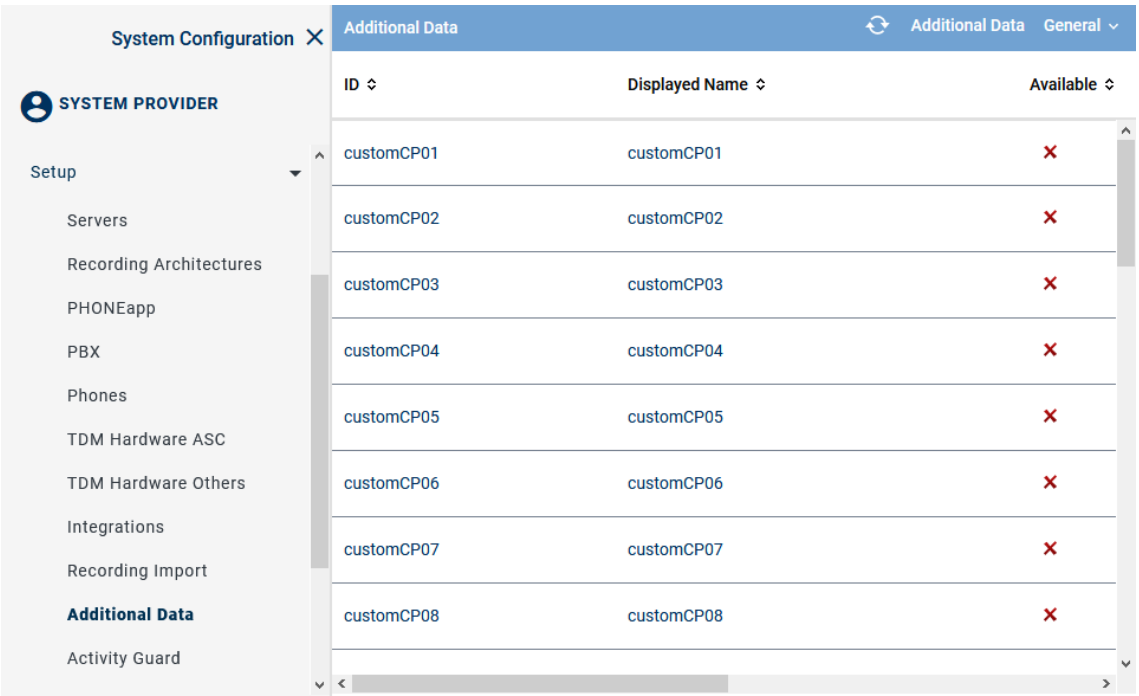


Fig. 393: Additional Data module main view

2. Select a set of data.
   ⇨ The detail view displays the information you can configure.

Change display name

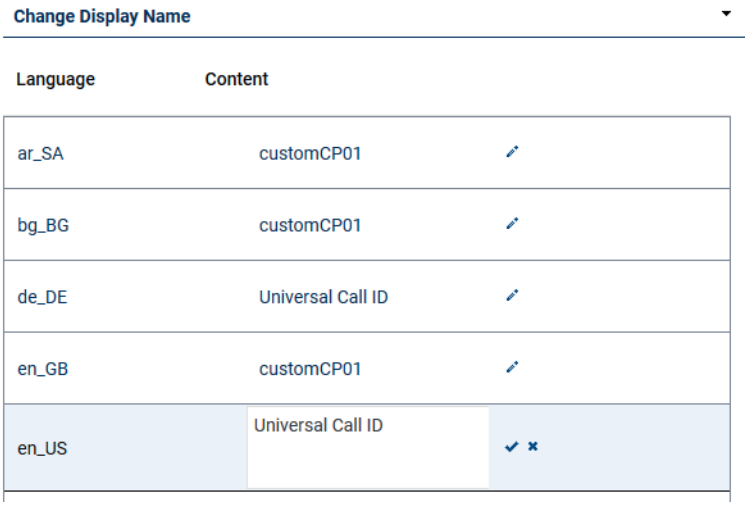


Fig. 394: Configure additional data

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Availability

Fig. 395: Additional data - configure availability

1. To make the data field available to the entire system, activate the check box of the option *Available*.
2. To make the data field in the search and replay applications editable later on, activate the check box of the option *Editable*.
3. To be able to use the data field for external recording control, activate the check box of the option *External recording control*. This option is only available if recording control has been activated in the *Servers module* in the tab *Usage*.
4. Click on the button *Save* to save the settings.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Additional data which is not delivered along with the protocol is not available for further use.

7.1.2.6.6 Create integration for Multi-Server Parallel Recording

In the Integrations module, the PBX-related recording settings are configured.

You first have to create and activate a recording architecture to be able to create a integration and to assign it here.

Depending on the recording solution, you additionally have to configure IP addresses, ports, protocols, sniffer cards, CTI connection data, phones, monitor points, and, where required, add-ons.

1. In the navigation bar, select the menu item *Setup* > *Integrations*.
   ⇨ The following window appears:

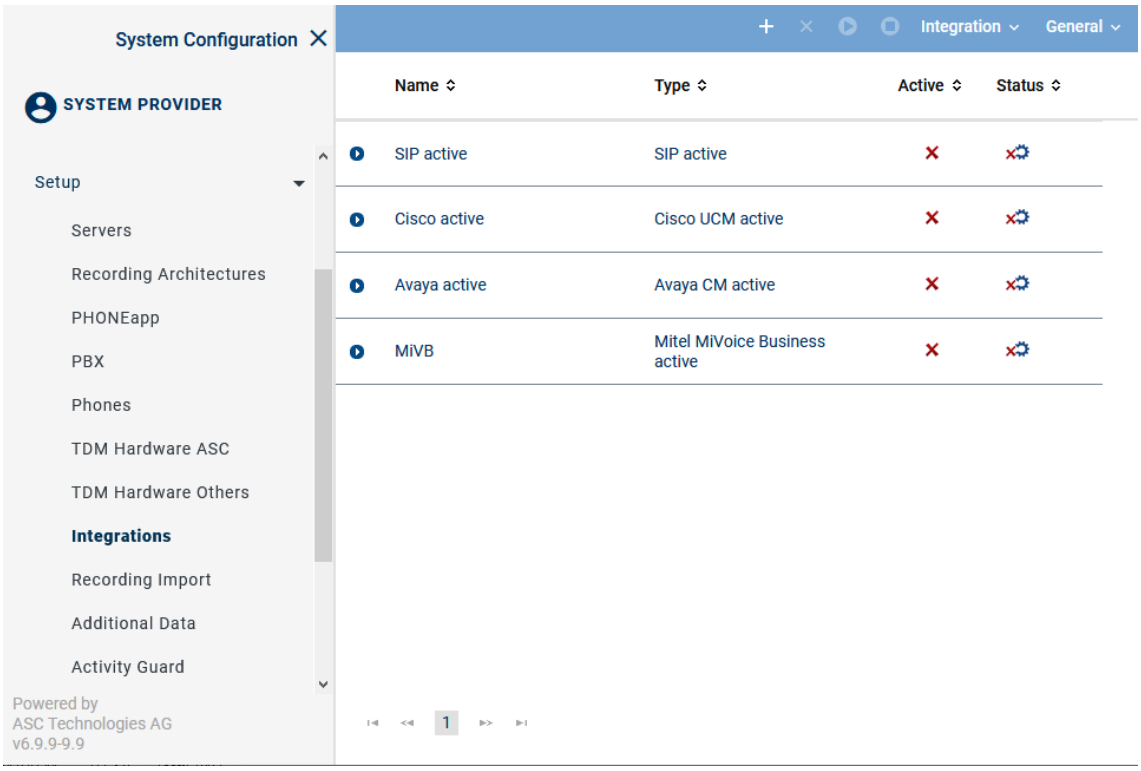


Fig. 396: Integrations - main view

In the table in the main view, the following information is displayed:

Name	Name of the integration
Type	Type of the integration
Active	Shows whether the integration has been activated and is used for the recording. ✓ = Integration is active, can be deactivated in the toolbar via the icon . ✗ = Integration is not active, can be activated in the toolbar via the icon .
Status	Shows whether the configuration has been carried out completely. = Configuration is complete. = Configuration is incomplete.

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 397: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.

Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Import grammar

Depending on the deployed PBX, conversation events are signaled differently.

A grammar recognizes and processes the events occurring during a call such as ringing, answering, consultation, hanging up. A grammar contains rules which are required to correctly translate PBX-specific call information and call states into a PBX-neutral format.

1. To import a new grammar, click on the menu item *Integration* > *Import Grammar* in the toolbar of the main view.
   ⇨ The window *Upload File* appears.

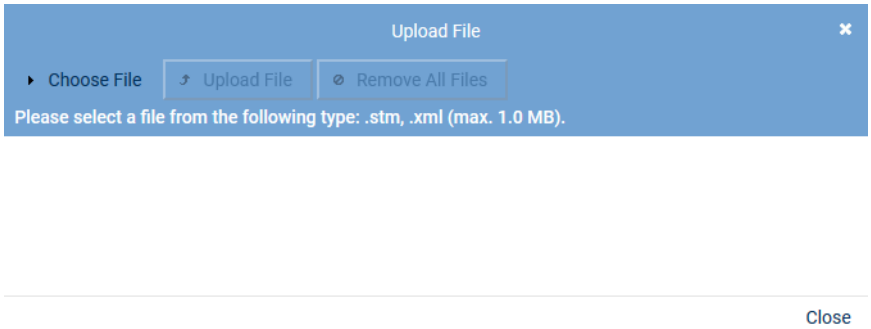


Fig. 398: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
   ⇨ The selected file appears in the window *Upload File*.

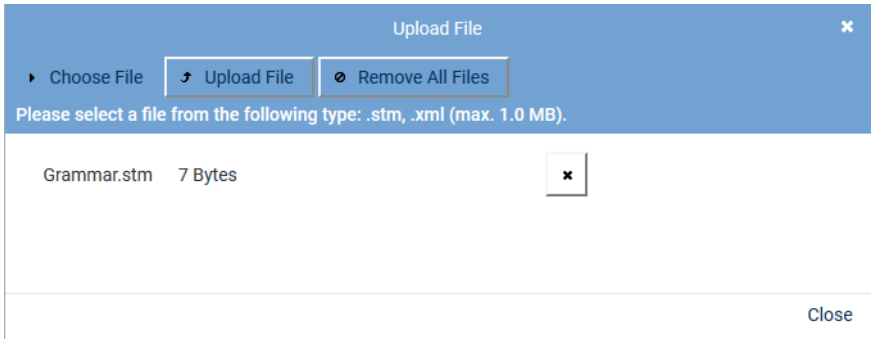


Fig. 399: Upload grammar

5. To remove a selected file from the list, click on the button × *(Remove file)* next to the respective file.
   To upload the file, click on the button *Upload File*.

⇨ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

1. Click on the icon + *(Create)* in the toolbar of the main view to create a new integration.
   ⇨ In the detail view, the tab *Integration Type* appears.

Fig. 400: Create integration type

2. Enter the following parameters:

Parameter	Value
Name	In the entry field, enter a descriptive name for the integration. This name is used as the identifier of this integration in the system.
Integration type	Select the entry *SIP active* from the drop-down list *Integration type*.

Tab. 88: Create integration type

3. To assign the PBX, click on the button + behind the field *PBX*.
   ⇨ The window *PBX* appears.

Fig. 401: Select PBX

4. Select the respective *PBX* from the list of available PBXs.
5. Click on the button *Add*.

Assign recording architecture for Multi-Server Parallel Recording

1. In the detail view on the bottom right, click on the button *Next*.
   ⇨ The tab *Recording Architecture* appears.

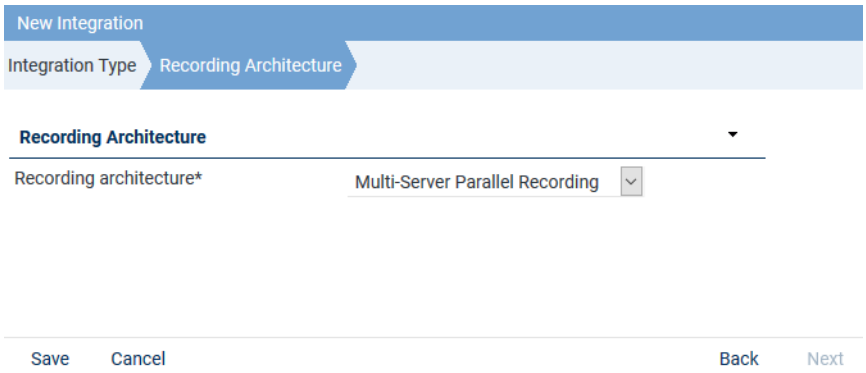


Fig. 402: Assign recording architecture - Multi-Server Parallel

2. Select the respective recording architecture from the drop-down list *Recording architecture*.

Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

3. Click on the button *Save*.
   ⇨ The integration now appears in the main view.

When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see chapter "Duplicates in parallel recording architectures", p. 369.

Configuration steps

1. To complete the configuration of the integration, click on the icon in front of the name of the new integration.
   ⇨ The following configuration steps appear:

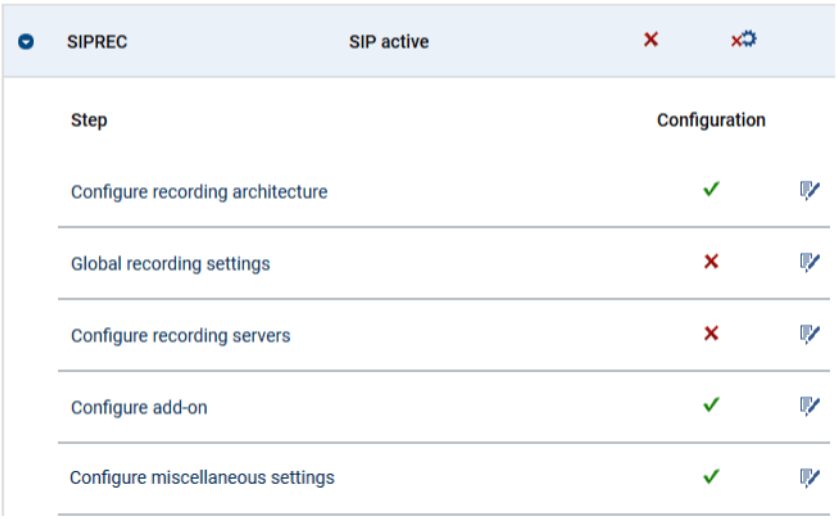


Fig. 403: Configuration steps of the integration

Configure recording architecture

The section *Configure recording architecture* has already been configured in previous steps.

1. Click on the button *(Edit configuration step)* in the line *Configure recording architecture* in the main view to show the configuration.
   ⇨ In the detail view, the configuration step appears with the information of the assigned recording architecture.

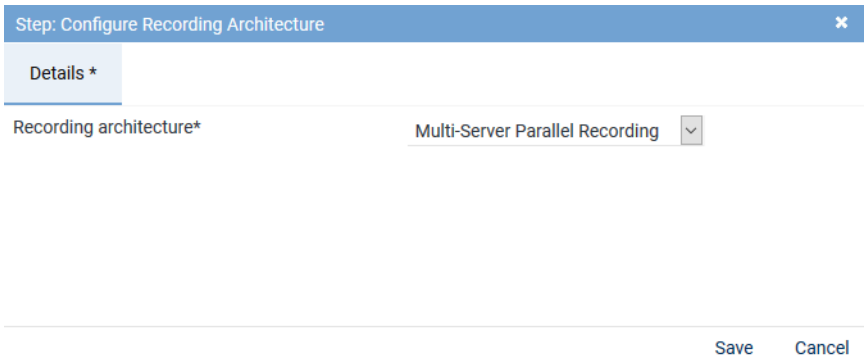


Fig. 404: Configuration step - Configure Recording Architecture

2. Click on the button *Save* to save changes and to finish the configuration step.
3. Click on the button *Cancel* to cancel the configuration step without applying changes.

Global recording settings for Multi-Server Parallel Recording

1. Click on the button *(Edit configuration step)* in the line *Global recording settings* in the main view.
   ⇨ The window *Step: Global Recording Settings* appears.

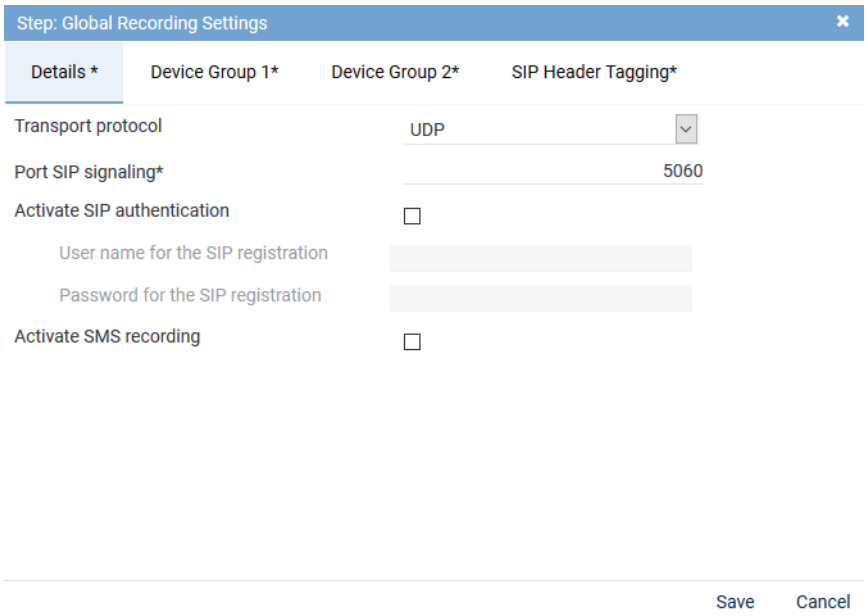


Fig. 405: Configuration step - Global Recording Settings - Multi-Server Parallel Recording

2. Set the following parameters in the tab *Details*:

Parameter	Value/Description
Transport protocol	Select the transport protocol *UDP* for the SIP signaling between the recording server and the PBX.
Port SIP signaling	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is *5060.* Default value with TLS encryption is *5061.*
Activate SIP authentication	Deactivate this option for this recording solution.
Activate SMS recording	This function is not supported in this recording solution.

Tab. 89: Global recording settings

NOTICE! In parallel recording architectures, the PBX connection is activated in the tabs *Device Group 1* and *Device Group 2*

3. To save the entries, click on the button *Save*.
   To discard entries, click on the button *Cancel*.

Tab Device Groups

In parallel recording, you can configure connections to different PBXs.

1. Select the tab Device Group 1 to configure the connection to PBX 1.

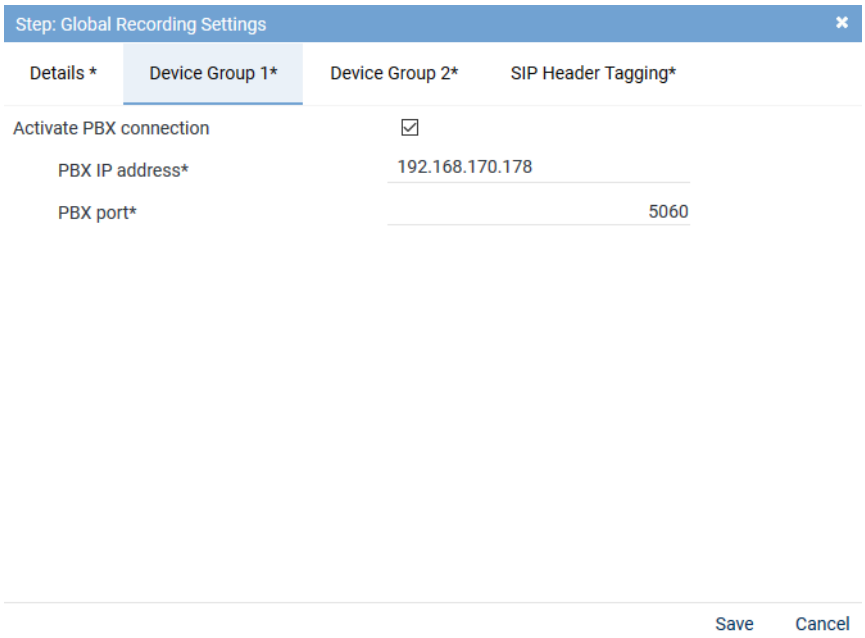


Fig. 406: Configure device group 1

Parameter	Description
Activate PBX connection	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
PBX IP address	Enter the IP address of the PBX for the first device group.
PBX port	Enter the port of the PBX which is used to communicate with the PBX.

2. Select the tab *Device Group 2* to configure the connection to PBX 2.

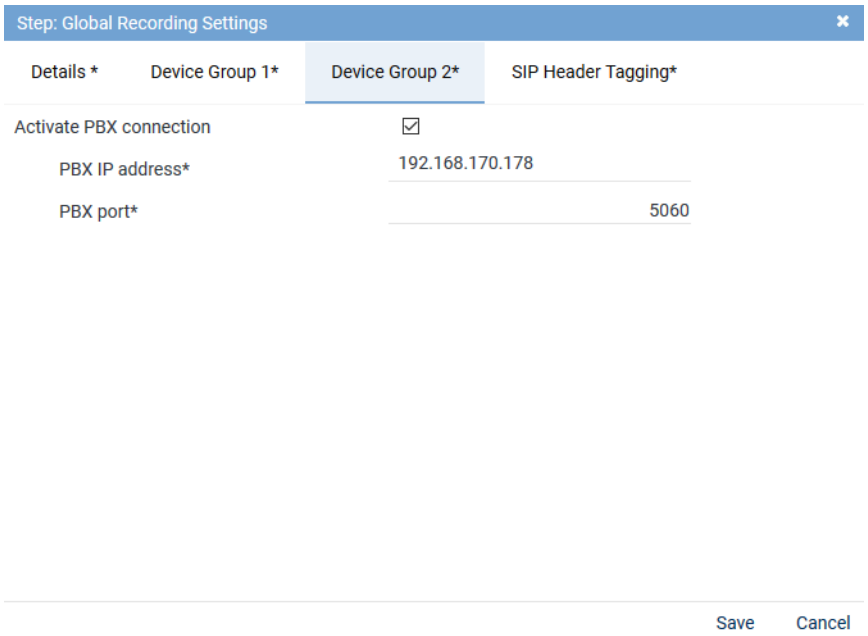


Fig. 407: Configure device group 2

Parameter	Description
Activate PBX connection	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
PBX IP address	Enter the IP address of the PBX for the second device group.
PBX port	Enter the port of the PBX which is used to communicate with the PBX.

3. To save the entries, click on the button *Save* in the detail view.
   To reset the entries, click on the button *Reset* in the detail view.

Tab SIP Header Tagging

In this recording solution, no additional data is extracted from the *SIP header*. The SIPREC meta data is provided by means of an XML document. To have ASC configure the mapping file, contact your distribution partner. The individual additional data which can then be read out from the file can be configured in the Additional Data module and subsequently mapped in the tab SIP Header Tagging.

1. If you would like to configure the SIP header tagging, select the tab *SIP Header Tagging*.

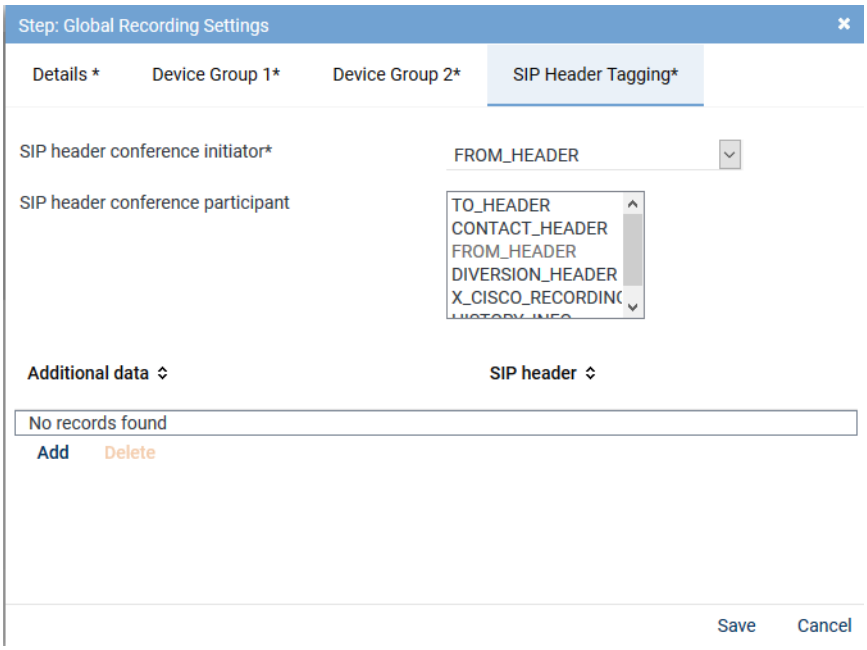


Fig. 408: Tab SIP Header Tagging Configure sources

2. If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.

   ⇨ The window *SIP Additional Data* appears.

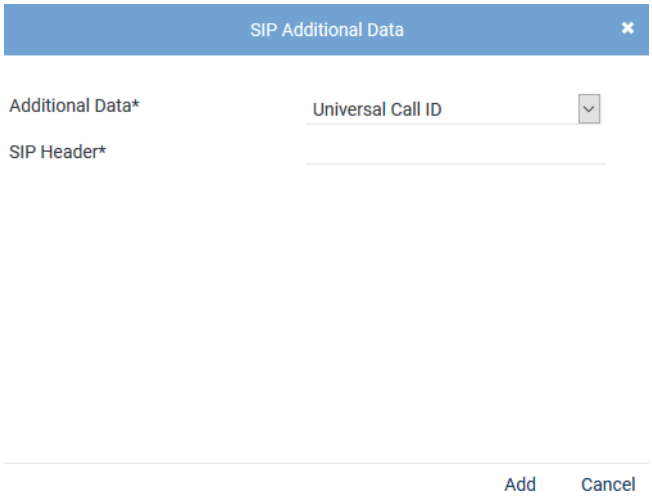


Fig. 409: SIP Additional Data

ⓘ Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

3. Enter the following parameters:

Parameter	Value/Description
Additional Data	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
SIP Header	If you would like to use additional data, the mapping of the tag name must have been configured in the file *siprecmapping.xml*. Then you can enter the tag name from where the information is to be extracted.

Parameter	Value/Description
	To have ASC configure the mapping file, contact your distribution partner.

Tab. 90: Configure SIP conversation parameters

4. Click on the button *Save* to close the window.
5. Click on the button *Save* to finish the configuration in this step.

Configure recording server for Multi-Server Parallel Recording

When using several recording servers, you must configure the port range for each recording server separately. The range may be the same for all recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

1. In the main view in the line *Configure recording servers* click on the button *(Edit configuration step)*.
   ⇨ The window *Step: Configure Recording Servers* appears.

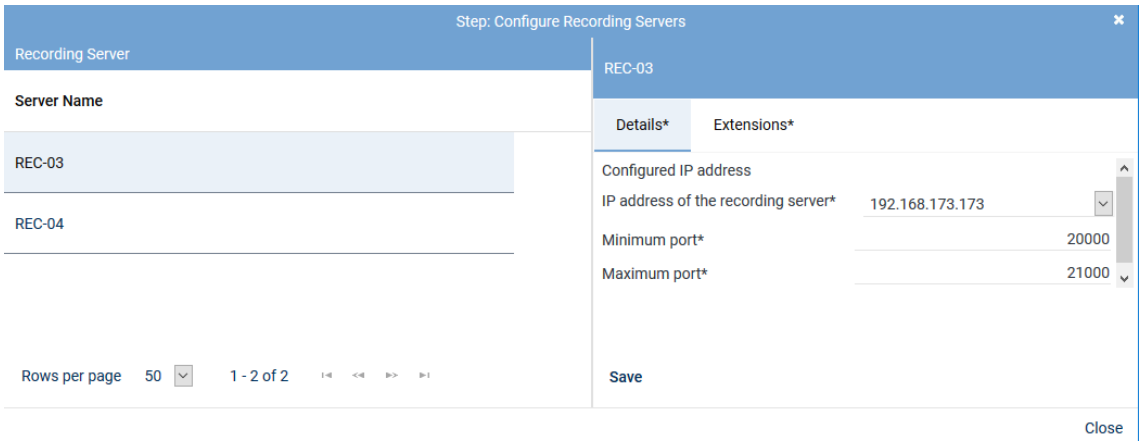


Fig. 410: Configuration step - Configure recording servers

2. Enter the following parameters in the tab *Details*:

Parameter	Value/Description
Configured IP address	Here, the IP address is displayed which has been configured for this recording server and via which the data to be recorded is received.
IP address of the recording server	From the drop-down list, select one of the available IP addresses of the recording server for the recording data.
Minimum port	Enter the lowest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *20000*.
Maximum port	Enter the highest port of the port range configured for the PBX via which the RTP data is supposed to be received, e. g. *21000*.

Tab. 91: Configure recording servers

ⓘ For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.
In addition, stereo recording requires more storage space.

If you use several active integrations in one recording architecture, you must configure different port ranges for each integration in the configuration step *Configure recording servers*.

Tab Extensions

1. Click on the tab *Extensions*.

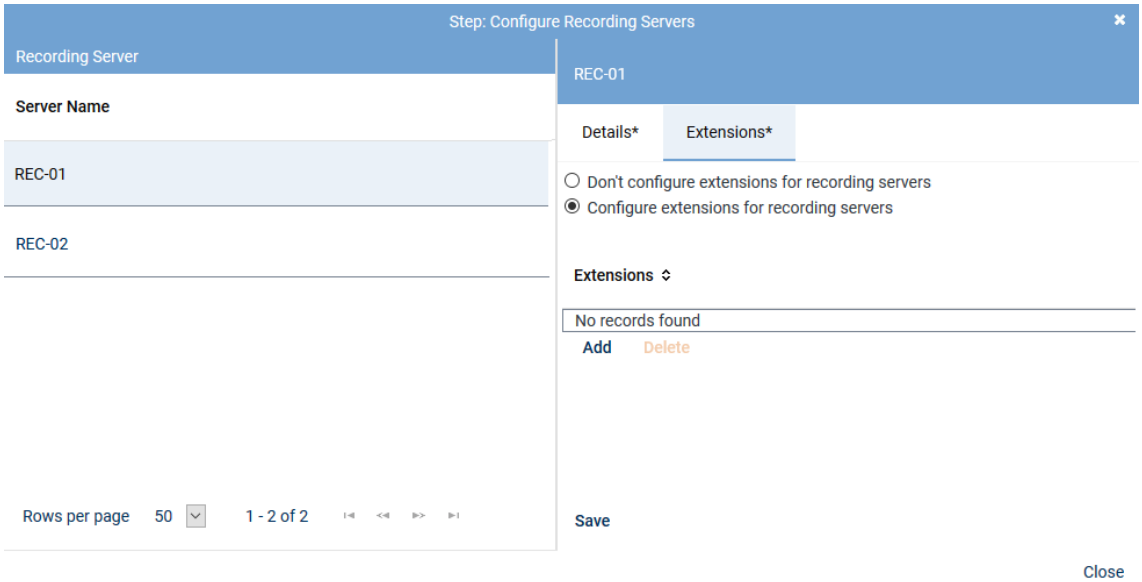


Fig. 411: Tab Extensions

The following options are available:

Configure no extensions for recording servers	Activate this option if you have not configured the extensions for the recording server in the PBX.
Configure extensions of the recording server	Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

2. To add extensions, click on the button *Add* in the table *Extensions*.
   ⇨ The window *Add Extensions* appears.

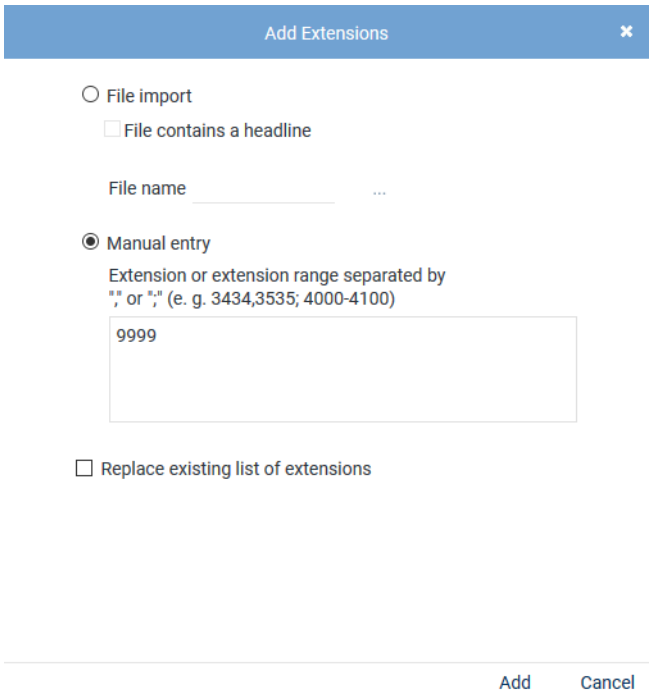


Fig. 412: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

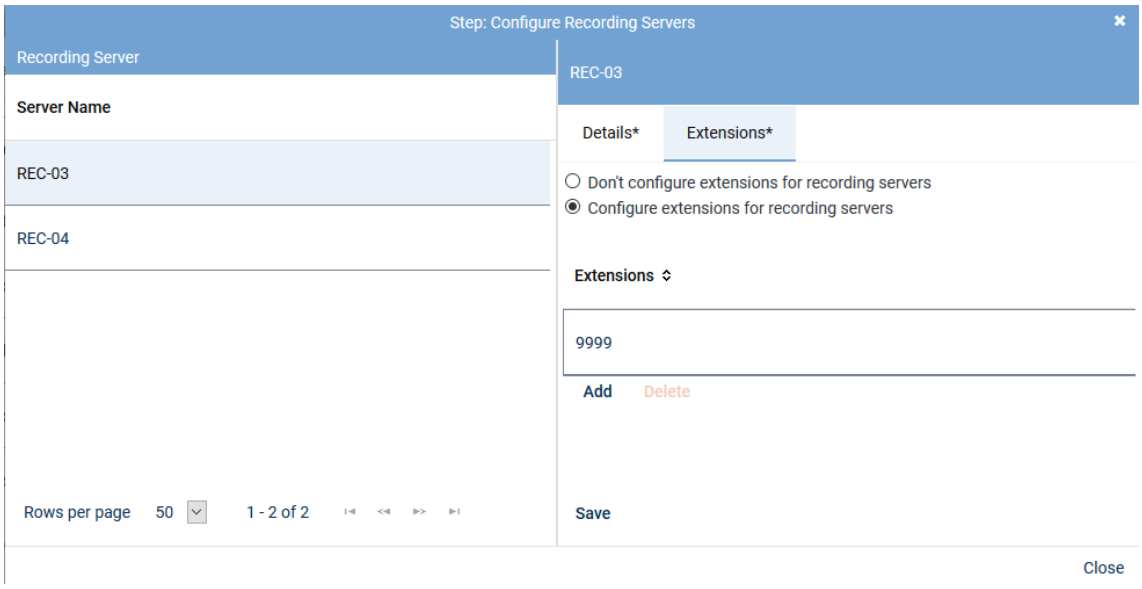


Fig. 413: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.
8. Click on the button *Save*.

9. Click on the button *Close* to finish this configuration step.

Configure add-on

The use of the add-on in the integration is optional. The status of this configuration step has been set to *No selection* by default and is considered to be completely configured that way. You can activate and use the integration without an add-on, too.

If you use an application with add-on, you can select the required grammar in the corresponding version in this configuration step. Additionally, you can configure the connection data and the additional data.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

Only those add-ons are displayed for which a license has been installed in the system.

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of CTI*connect* for Sparkassen FI ISP in the DACH region and only has to be configured if the add-on is used.

The add-on cannot be used in a failover architecture. The application Sparkassen FI ISP cannot connect to more than one IP address.

The integration runs in combination with a PBX and the recording server. The service CTI*connect* for Sparkassen FI ISP receives the additional data from the PBX and sends them to the recording server. In addition, the recording decision which is initiated by the user on the end device is processed via CTI*connect* for Sparkassen FI ISP and sent to the recording server.

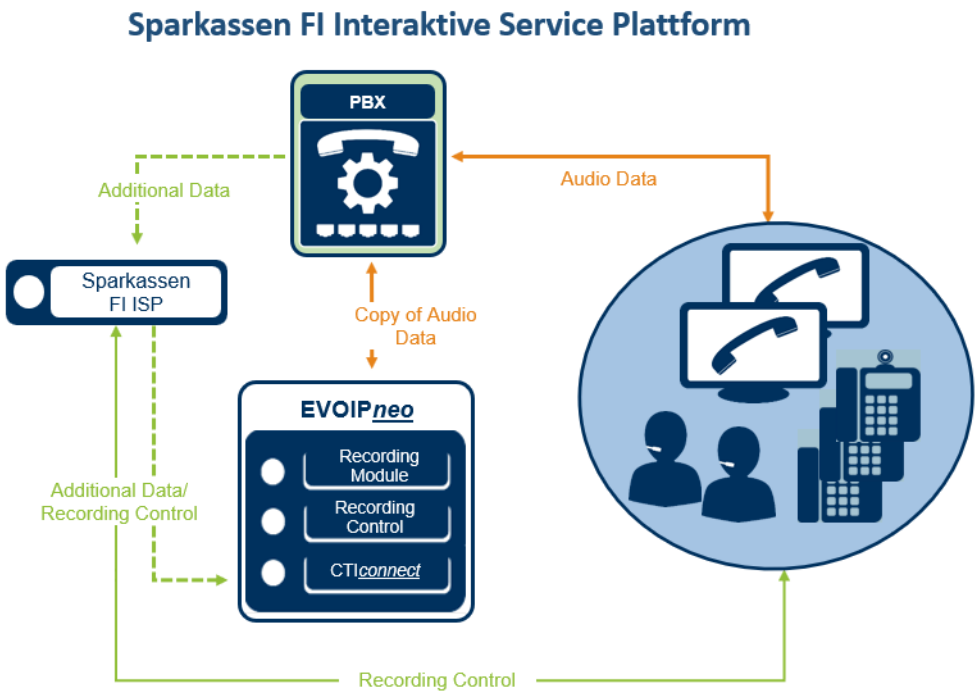


Fig. 414: Overview of Sparkassen FI ISP

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. Select the add-on *Sparkassen FI ISP* in the detail view.

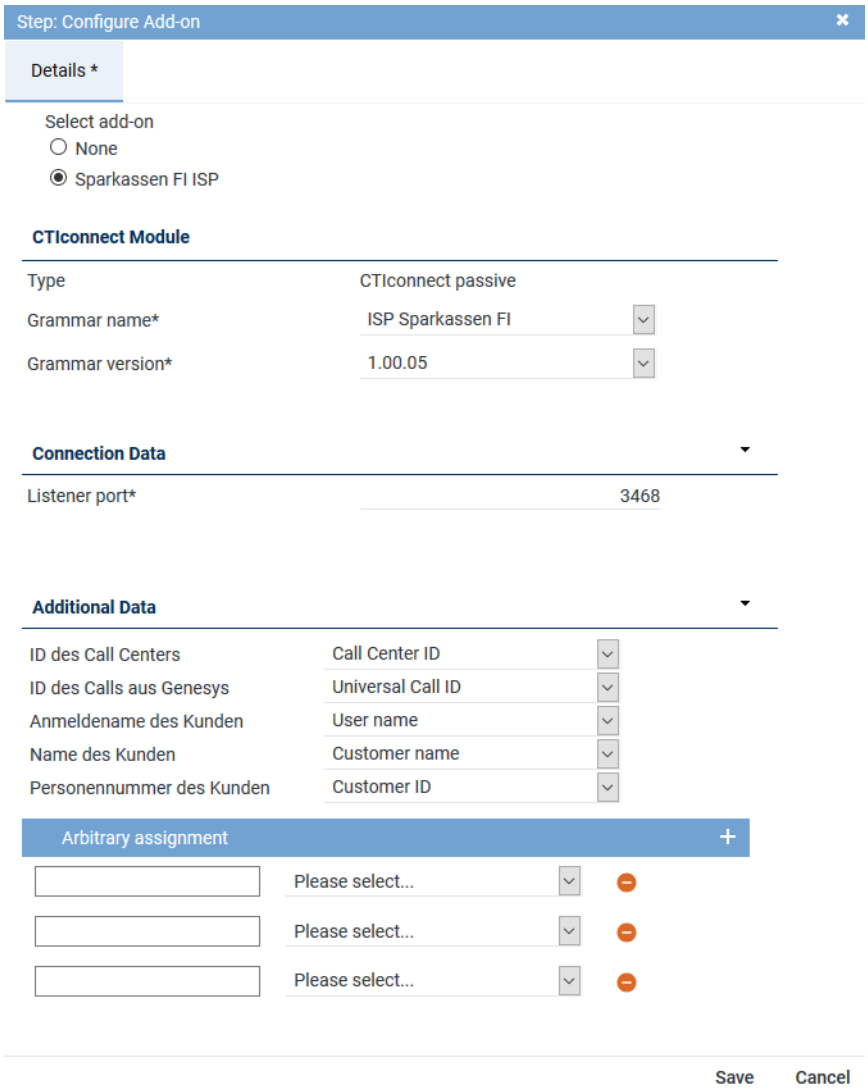


Fig. 415: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 92: Configure CTIconnect module

For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See chapter "Import grammar", p. 342.

Group field Connection Data

Set the following parameter in the group field *Connection Data*; the IP address for the PBX does not have to be entered, since the PBX connects to our recording server:

Parameter	Value/Description
Listener port	Enter the port that the add-on connects to, e. g. *3468*.

Tab. 93: Configure connection data

Group field Additional Data

This add-on is used exclusively in the DACH region; for this reason the additional data is only available in German, too. The names of the fields refer to the assignment of the strings which are delivered by the interface.

When using CTI*connect* for Sparkassen FI ISP, the following additional data is delivered with the protocol:

- *ID of the call center*
- *ID of the call from Genesys*
- *Login name of the customer*
- *Name of the customer*
- *Employee number of the customer*

In addition, the following additional data is provided which is always displayed in the drop-down list without having to configure it separately in the Additional Data module:

- *Transaction ID*
- *Customer ID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

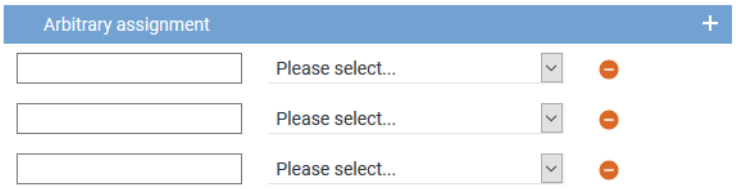


Fig. 416: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.

   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI*connect* Service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

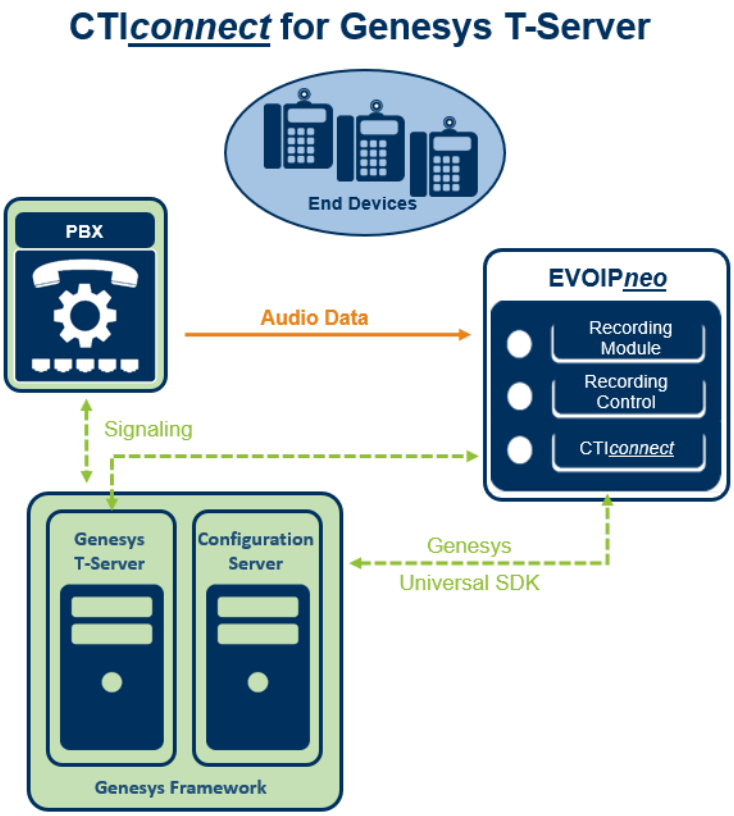


Fig. 417: Overview of the add on of Genesys T-Server

For further information about the configuration of Genesys T-Servers, see chapter "Configure Genesys T-Server (optional)", p. 377.

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.

The additional data delivered by an add-on supplements the additional data which is delivered by the CTI*connect* module of the integration.

When using a CTI*connect* for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path *C:\ASC Product Suite\data\CTIConnectForGenesysT*.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button *(Edit configuration step)* in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

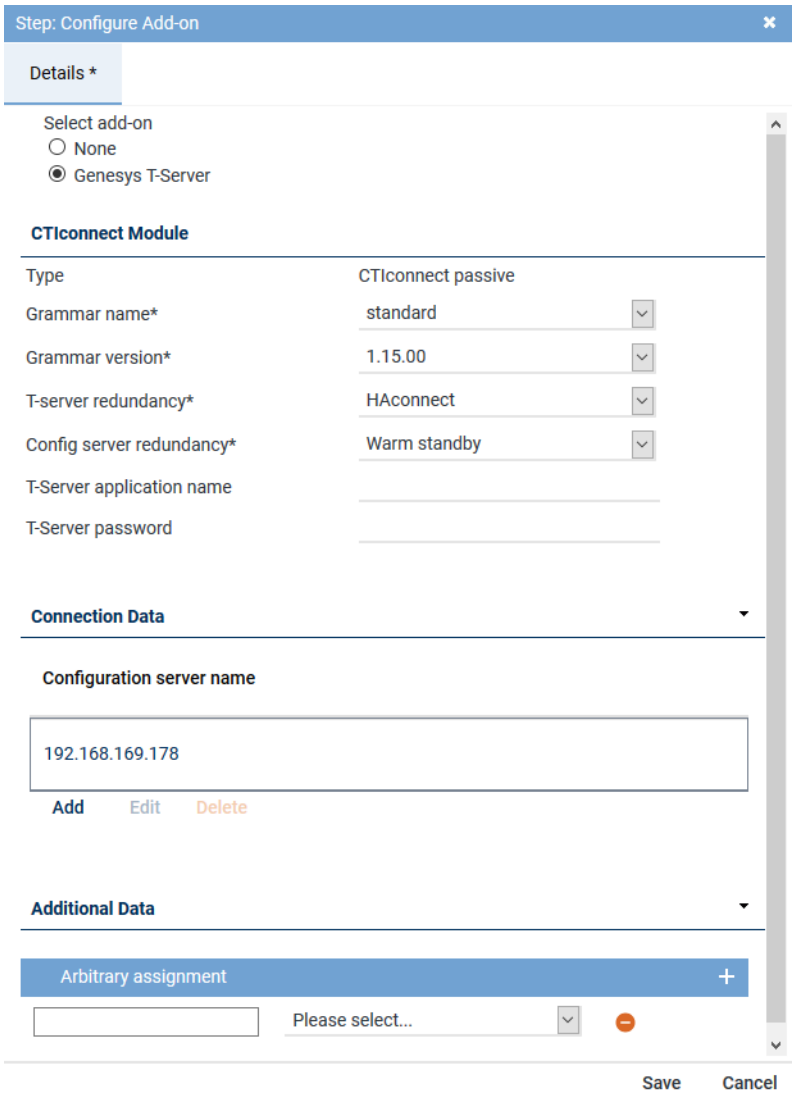


Fig. 418: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
Type	Here, the type of the CTI*connect* module is displayed.
Grammar name	Select the respective grammar.
Grammar version	Select the respective grammar version.
T-server redundancy	Select the redundancy which is used from the drop-down list. • *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
Config server redundancy	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	• *No redundancy* • *HAconnect* - for High Availability Connection • *Warm Standby* - for a connectable redundancy
T-Server application name	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.
T-Server password	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI*connect* module is supposed to use to log in to the Genesys T-Server. If you use several Genesys T-Servers, the login data must be identical for all servers.

Tab. 94: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

1. In the group field *Connection Data* in the table, click on the button *Add*.
   ⇨ The following window appears:

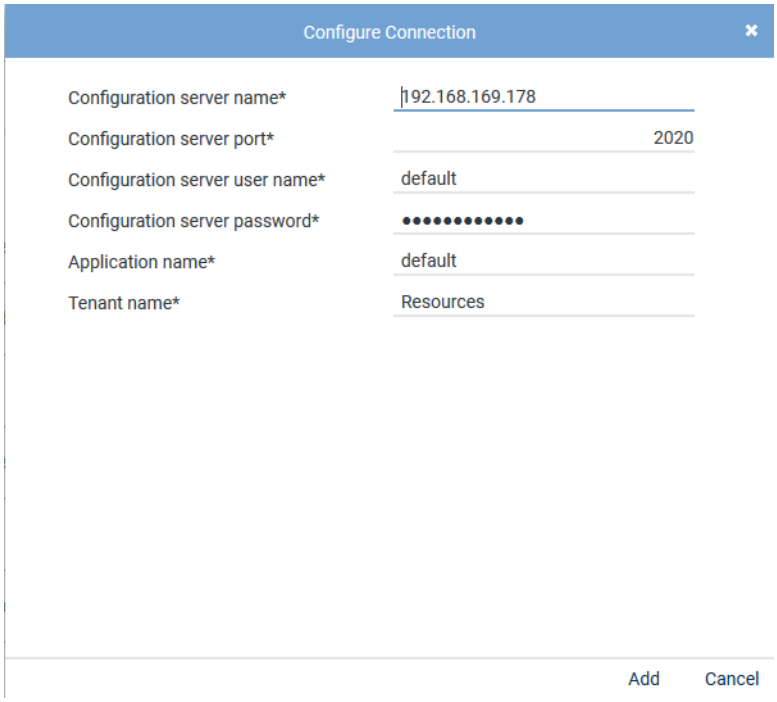


Fig. 419: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
Configuration Server: Name	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
Configuration Server: Port	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
Configuration Server: User name	Enter the user name to log in to the Genesys Configuration Server.
Configuration Server: Password	Enter the password to log in to the Genesys Configuration Server.
Application name	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is *default*.
Tenant name	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is *Resources*. Several tenants can be added separated by commas.

Tab. 95: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*

Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.

The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ▸ to expand the group field and to assign the additional data to the data fields of the search and replay applications.

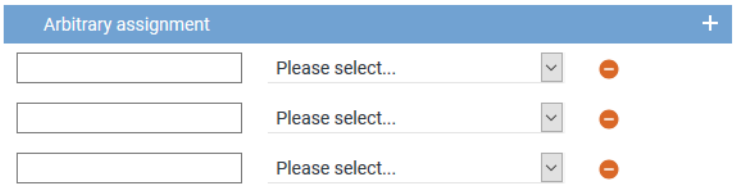


Fig. 420: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*
- *Duration*
- *Calling party phone number*
- *Called party phone number*
- *Conversation direction*

2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
4. To add a new assignment, click on the icon + *(Create)* in the toolbar of the table.
   ⇨ An additional row appears to assign another additional data type.
5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.

To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.

For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button *(Edit configuration step)* in the line *Configure recording servers* in the main view.
   ⇨ The window *Step: Miscellaneous Settings* appears.

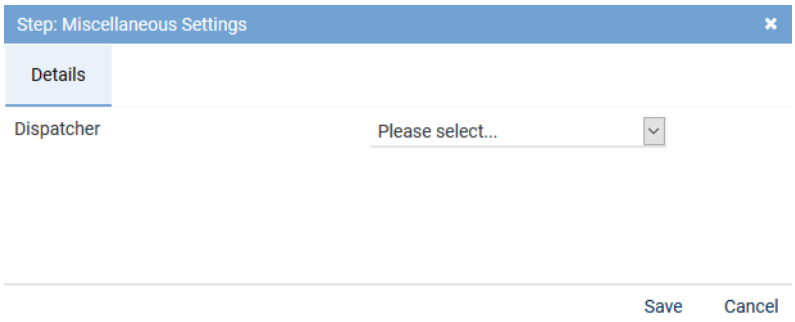


Fig. 421: Configure miscellaneous settings

2. Enter the following parameter:

Parameters	Description
Dispatcher	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.

Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon *(Incomplete)* will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon ✓ *(Complete)* will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon *(OK)* will appear in the main view, in the line of the created integration, in the column *Status*.

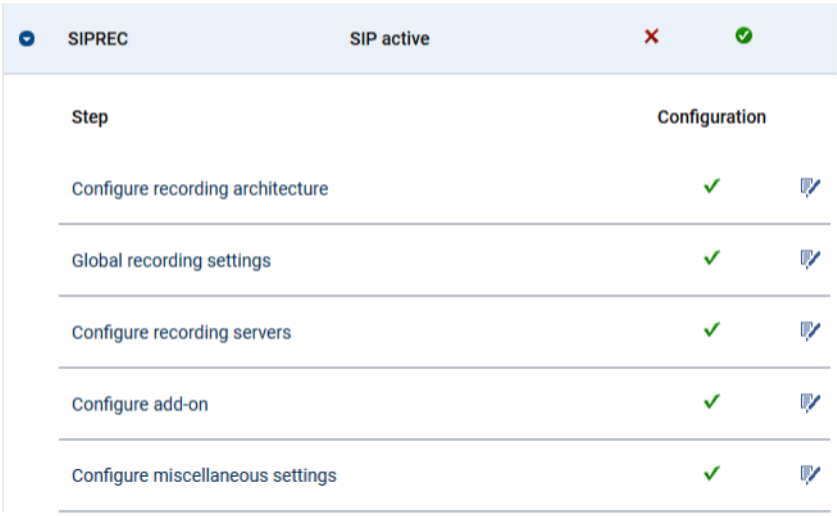


Fig. 422: Activate integration

1. Mark the integration in the main view, so that the icon *(Activate)* becomes active in the toolbar.
2. To activate the integration, click on the icon *(Activate)*.
   ⇨ In the column *Active*, the icon ✓ *(Active)* appears.

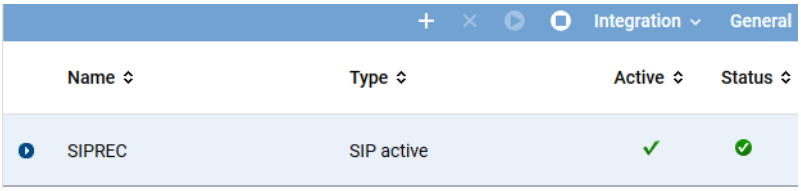


Fig. 423: Activated integration

If you use several PBXs, you can create and activate several integrations with the same recording architecture.

If you take advantage of the grace period and there is no valid license file in the system after its expiration, all integrations are deactivated. After uploading a valid license file, you have to activate the integrations again.

Upon activating the standard configuration, a bulk recording will start.

To restrict the recording to particular end devices, the tenant can configure the Recording Planner in the System Configuration accordingly.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

1. To deactivate the integration, click on the icon *(Deactivate)* in the toolbar.
   ⇨ In the column *Active*, the icon ✕ *(Inactive)* appears.
   ⇨ The icon *(Delete)* becomes active in the toolbar.

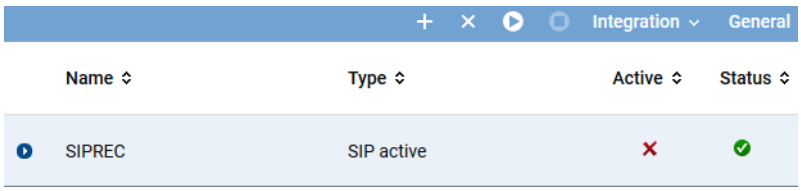


Fig. 424: Deactivate integration

2. Click on the icon *(Delete)* and confirm the security prompt to delete the integration.

7.1.3 Configure Recording Content Validation

Recording Content Validation is an easy and quick possibility to check the functionality of the recording system whenever required. The information is displayed in the Notifications module. Reports can be used to visualize the results.

Preconditions for validation:

- *The license Recording Content Validation must have been installed.*
- *Emotion detection must have been activated in the Servers module.*
- *The server for emotion detection must have been selected.*

Configuration in the Servers module

1. Go to the *Servers module*.
2. In the main view, select the server that you would like to configure.
3. Select the tab *Usage*.
4. Open the group field *Audio Analysis*.

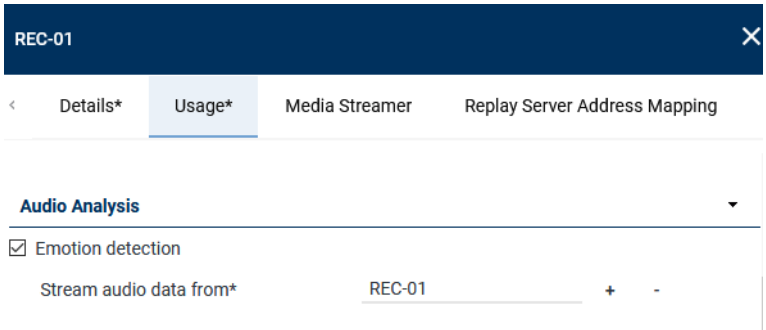


Fig. 425: Servers module - Activate emotion detection

5. Activate the function *Emotion detection*.

6. By clicking on the icon + , select the server that emotion detection runs on.
   ⇨ This server will then appear in the list in the Integrations module in the tab *Recording Content Validation* to configure silence detection.

Configuration in the Integrations module

1. In the main view, select the integration for which you would like to check the validity of recording.
2. Select the tab *Recording Content Validation*.

The following criteria are available to check proper recording:

- *Packet loss detection*
- *Decryption error detection*
- *Silence detection*

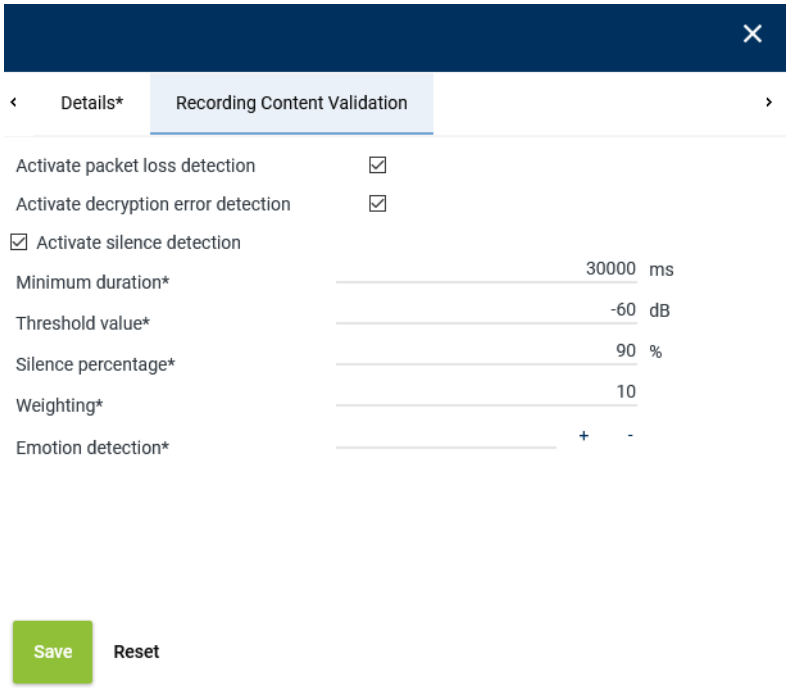


Fig. 426: Create integration - tab Recording Content Validation

Activate packet loss detection	☑ Activate the check box to check whether packets of a recording have been lost. **NOTICE!** Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	☑ Activate the check box to check whether errors occurred during decryption. **NOTICE!** Decryption errors result in noise which may corrupt the audio file.
Activate silence detection	☑ Activate the check box to check whether the recording contain sections of silence and under which conditions sections are recognized as silence. **NOTICE!** Detection is useful in case the PBX sends RTP packages which contain silence instead of an audio signal.

Minimum duration	Enter the minimum duration of silence after which a notification is supposed to be issued. Default value is 30000 ms *(30 seconds)*.
Threshold value	Enter a threshold value of the audio level in dB under which the section is supposed to be considered a silence section. Default value is -60 dB.
Silence percentage	Enter the percentage of silence in a recording which is supposed to trigger a notification. Default value is 90 %.
Weighting	Enter the smoothing factor defining to which extent the audio curves (samples) are supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 0-10000 can be recommended.
Emotion detection server	By clicking on the icon +, select the server that emotion detection runs on. The speech analysis software recognizes whether there are silence sections in the recording.

NOTICE! The list only displays servers which have been configured for audio analysis and have been assigned in the Servers module.

3. Select the respective server from the list of available servers.

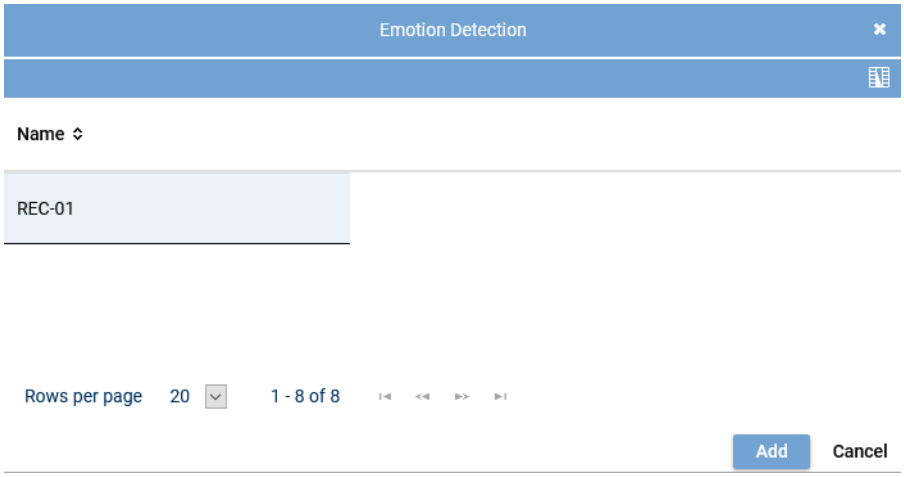


Fig. 427: Select server for emotion detection

4. Click on the button *Add* to apply the selected server.
5. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

Configuration in the Notifications module

To issue notifications in case of an error, the corresponding notifications must be configured in the Notifications module.

For basic information about the Notifications module refer to the administration manual for tenants *Notifications module*.

Configuration in the application INSIGHT*neo*

To issue a report visualizing the errors occurred, a report must be created in the application INSIGHT*neo*.

For information about using the Report Templates module and the Report Instances module refer to the respective INSIGHT*neo* user manuals.

7.1.4 Synchronization options

The are 2 different types of synchronization:

- Synchronization of the Recording Control Service for recording control
- Synchronization of the system storage to compare recording data

7.1.4.1 Synchronization of recording control

Recording Control Services

For parallel recording servers installed in the same system architecture, you can configure synchronization of recording control.

ATTENTION!

Before the configuration, contact your ASC support to ensure that this function is suitable for your recording solution and to avoid a possible loss of recordings!

For information about which recording solutions support this function refer to the file *neo* Integration Overview.

If recording is supposed to be controlled manually by means of applications such as CLIENT*command*, PHONE*app*, SCREEN*rec* scan Editor, or by external control, synchronization of the Recording Control Services of the parallel recording servers must be created.

Initially, the 1st Recording Control Service is responsible for recording control. The Recording Control Service ensures that the conversations of both recording servers are recorded.

If the 1st Recording Control Service fails, the 2nd Recording Control Service takes over recording control for both recording servers each of which then records the conversations.

Synchronization of recording control is configured in the Recording Architectures module. In parallel recording architectures, the check box *Synchronize recording control* appears in the tab *Details*.

1. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers.

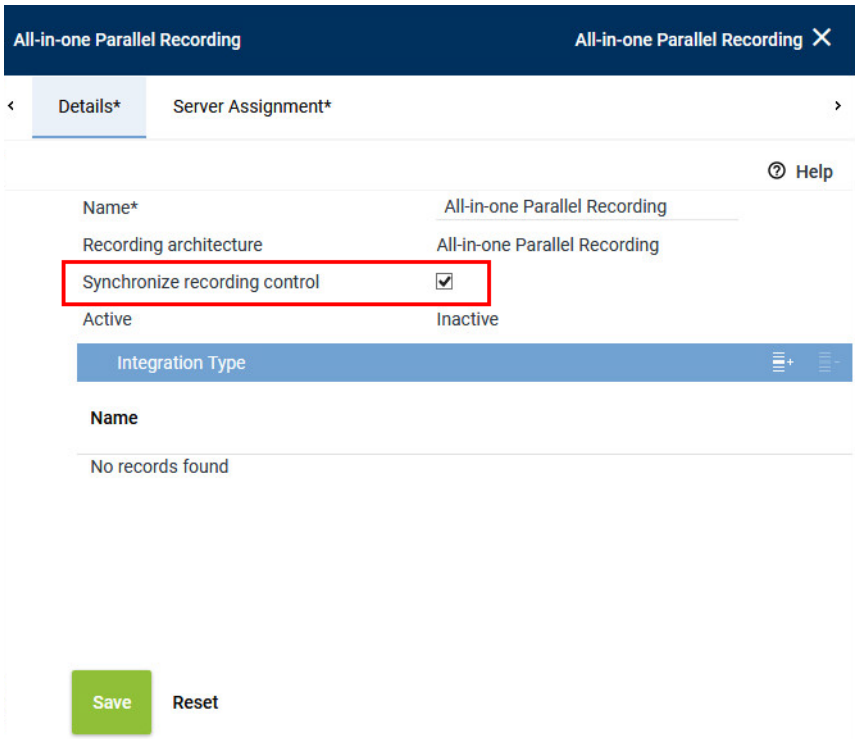


Fig. 428: Synchronize recording control

2. To save the settings, click on the button *Save*.
   To discard the settings, click on the button *Reset*.

ⓘ Synchronization of recording control brings stricter timeouts between the components. Observe the increased hardware and network requirements. Latency must be < 100 ms.

If you activate or deactivate this synchronization option subsequently, you must repeat the following configuration steps for the changes to take effect:

1. Select the required state of recording control:
   ☑ = *Recording control is synchronized*
   ☐ = *Recording control is not synchronized*
2. Deactivate the integration.
3. Deactivate the recording architecture.
4. Ensure that the following services have been stopped:
   - *ASC RecordingControl*
   - *ASC RecordingModule*
   - *ASC CTIconnect(integration name)*
5. Activate the recording architecture.

WARNING! In this status, all services have received the updated configuration but states may be conflicting.

Therefore, repeat the following steps:

6. Deactivate the recording architecture again.
7. Ensure that the services have been stopped.
8. Activate the recording architecture again.
9. Activate the integration.

⇨ The changes are now active.

7.1.4.2 Synchronization of system storage

In recording architectures with 2 system storages, you can configure synchronization to compare recordings.

A synchronization configuration is always created for 2 system storages. All recordings which are saved on one system storage are also copied to the other one and vice versa. That way, all recordings always exist on both system storages.

> In a multi-core architecture, the system storage must not be synchronized between the Enterprise Cores.

Synchronization of the system storages is configured in the Servers module.

1. To create a synchronization configuration, click on the menu item *Servers* > *Manage Synchronization Configuration* in the toolbar of the main view.

Fig. 429: Menu item Manage Synchronization Configurations

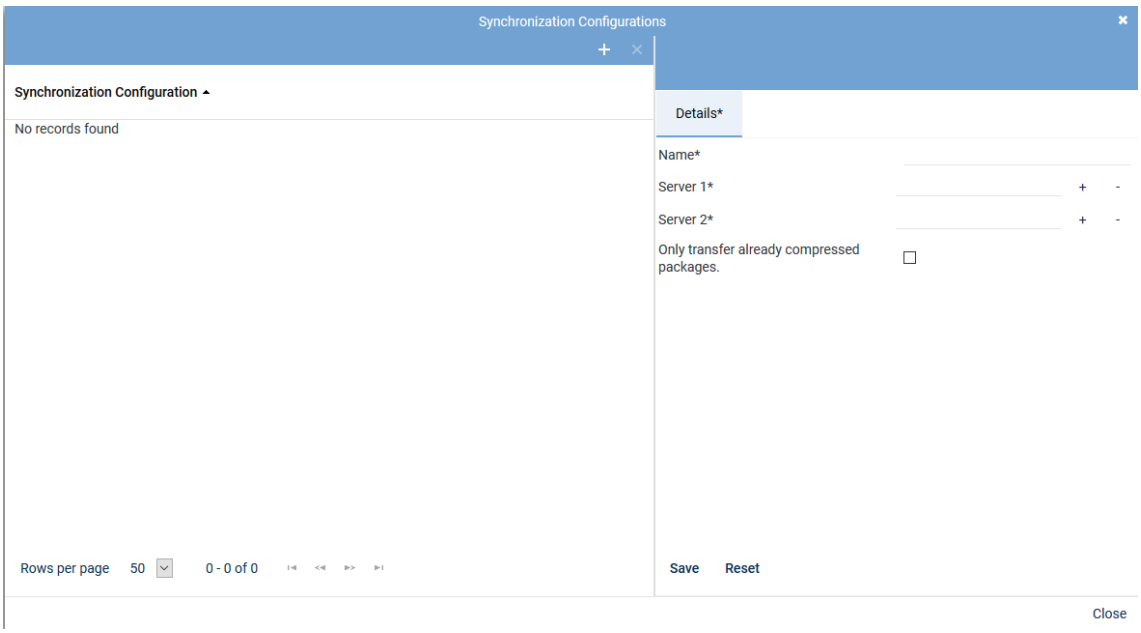


Fig. 430: Configure synchronization configurations

The following options are available:

+	*Create*	Creates a new synchronization configuration, see chapter "Create synchronization configuration", p. 368.
×	*Delete*	Deletes the selected synchronization configuration, see chapter "Delete synchronization configuration", p. 368.

A synchronization configuration becomes active upon saving it and remains active until deleted. During this time, both system storages are regularly checked for new content and synchronized.

> A server which is already used in a synchronization configuration cannot be used in another synchronization configuration.

7.1.4.2.1 Create synchronization configuration

1. In the window *Administrate Synchronization Configuration*, click on the icon + *(Create)*.
   ⇨ The tab *Details* becomes active.

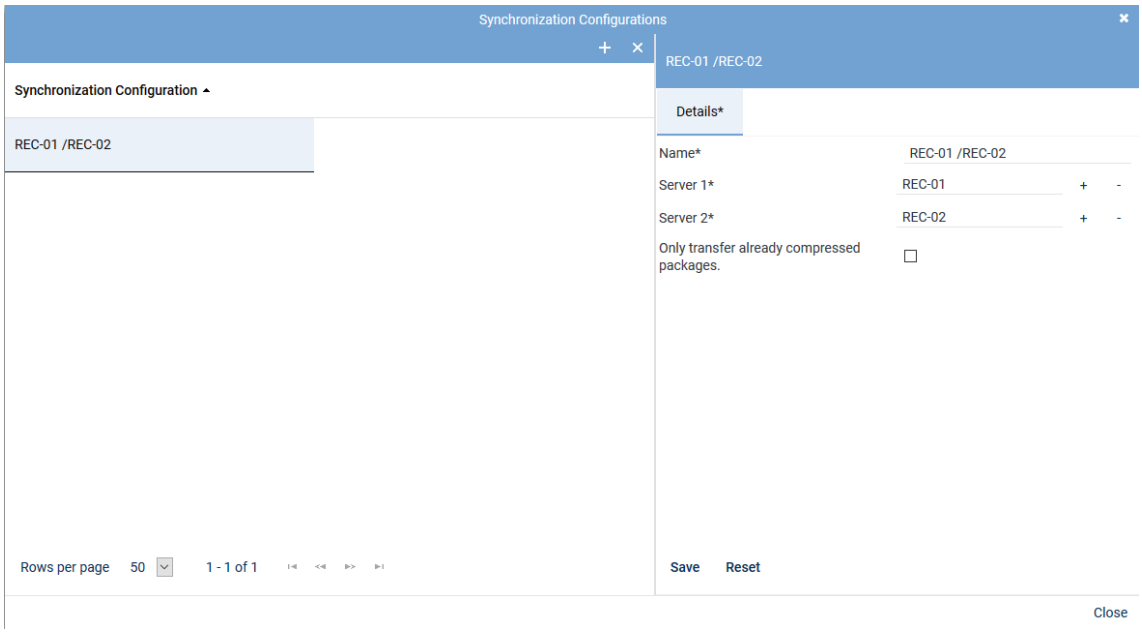


Fig. 431: Create synchronization configuration

2. Complete all fields for the new synchronization configuration:

Name	Enter a name for the synchronization configuration.
Server 1 / *Server 2*	Click on the button + next to the entry field to select the respective server for the synchronization of the system storage from the list of available servers. If you would like to delete an entry in one of the entry fields, click on the button - next to the respective entry field.
Only transfer already compressed packages	Select whether data which has not yet been compressed is supposed to be transferred, too. ☑ = Uncompressed data is transferred, too. ☐ = Only compressed data is transferred. **NOTICE!** This option is not available until you have entered and saved the two servers.

3. Click on the button *Save* to apply the configuration.
4. Click on the button *Close* to finish this configuration step and close the window.

7.1.4.2.2 Delete synchronization configuration

1. In the window *Administrate synchronization configurations*, select the synchronization configuration you would like to delete.
2. Click on the icon × *(Delete)* in the toolbar of the window.

⇨ The synchronization of the two entered system storages is finished.

⇨ The selected synchronization configuration is deleted.

7.1.5 Duplicates in parallel recording architectures

In parallel recording architectures in which recording control is synchronized, no duplicates are created which could be deleted. Both recordings are merged in one package and thus cannot be deleted separately. Keep in mind that more storage space must thus be available for the recordings.

A parallel recording without synchronization results in redundant recording data in the system. To avoid that conversations are displayed twice in the replay applications (e. g. POWER*play* Web) because the database contains them twice, you can delete duplicates so that only one of the double recordings remains.

Conversations with the following characteristics are considered identical:

- Identical start and end times

  You can define an allowed difference for the start and end times so that the conversations are still considered duplicates despite a differing start or end time, see chapter "Configure duplicate detection", p. 369.

  The start and end times of complete conversations as well as the start and end times of the individual recordings belonging to a conversation are checked.
- Identical call participants
- Identical additional data

Duplicate detection is configured in the Integrations module. There, you can configure for each integration individually under which circumstances conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings, see chapter "Configure duplicate detection", p. 369.

The shorter one of the two identical recordings is deleted. To calculate the total recording length, the recording lengths of all sections of a conversation are added. The additional data as well as the audio data of the duplicate are deleted. On which of the two recording servers a duplicate is deleted thus depends on the location where the shorter recording has been saved. If the recording length is the same, the recording which has been checked second is considered a duplicate and deleted.

Duplicate detection is executed regularly for all new recordings from the moment on it has been activated but not for past recordings. This means Recordings which already exist when duplicate detection is activated are not checked for duplicates.

For information about the status of a job refer to the Jobs module in the application System Monitoring, see user manual *Usage System Monitoring*.

If you would like to delete duplicates but nevertheless want that all conversations exist on both recording servers, you can create a synchronization configuration in the Servers module which synchronizes the system storages of the two recording servers.

7.1.5.1 Configure duplicate detection

In the Integrations module, you can configure for each integration separately under which circumstances 2 conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings.

1. In the main view of the Integrations module, select the integration for which you would like to configure duplicate detection.
2. Select the tab *Parallel Recording* in the detail view and adjust the following settings:

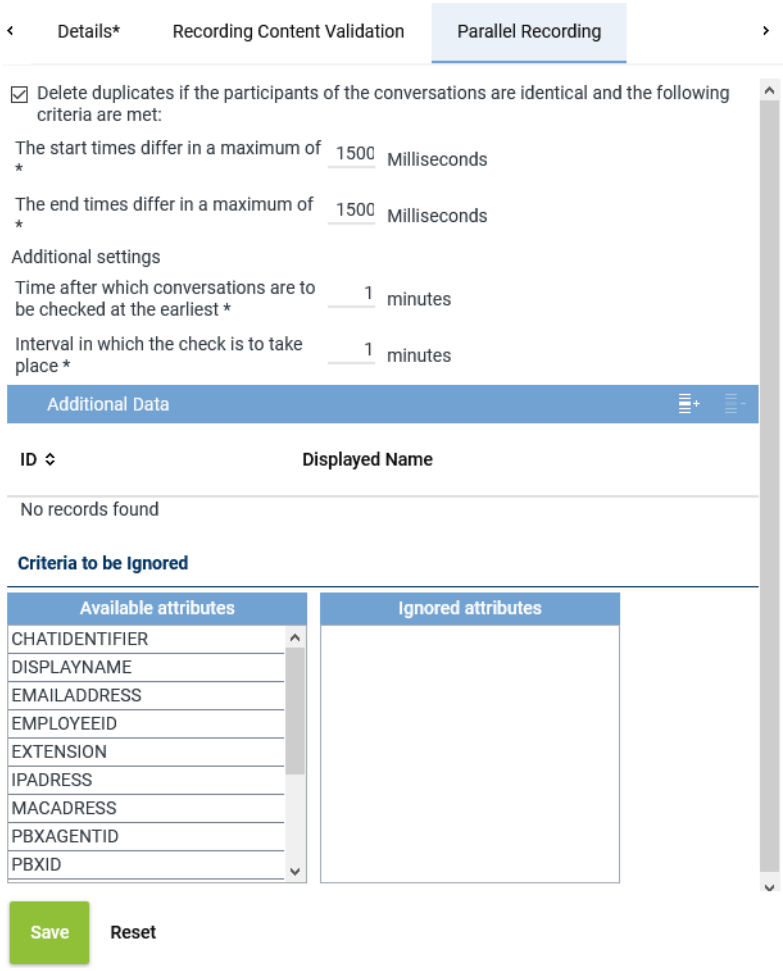


Fig. 432: Tab Parallel Recording (integration)

Delete duplicates,....	When activating this option, you can define by means of the displayed criteria when 2 recordings are supposed to be identified as identical. ☑ = Duplicate detection has been activated. Duplicates are deleted according to the defined criteria. ☐ = Duplicate detection has been deactivated.
The start times differ in a maximum of	Enter the maximum difference with regards to the start time. The start times of complete conversations as well as the start times of the individual recordings belonging to a conversation are checked. Example: *1000 milliseconds* If one conversation started at 2:20:15 PM and a second conversation started at 2:20:16 PM, and if the start times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their start time.
The end times differ in a maximum of	Enter the maximum difference with regards to the end time. The end times of complete conversations as well as the end times of the individual recording sections belonging to a conversation are checked. Example: *1000 milliseconds* If one conversation ended at 2:20:15 PM and a second conversation ended at 2:20:16 PM, and if the end times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their end time.

Time after which conversations are to be checked at the earliest	Enter the time interval which is supposed to pass before a recording is checked for duplicates. Example: *3 minutes* If one conversation ended at 2:20 PM, i. e. the recording has been saved at 2:20 PM, then the recording is not check for duplicates before 2:23 PM.
Interval in which the check is to take place	Select the intervals in which the job for duplicate detection is supposed to be executed. Example: *2 minutes* The job for duplicate detection is started over again every 2 minutes to search for new recordings and possible duplicates and to delete duplicates.
List *Additional Data*	Add all additional data to the list which are supposed to be used as criteria. When searching for duplicates, only those recordings are considered which contain an additional data type from the list. If an additional data type is empty in both conversations, this is considered identical, too, and one of the conversations is deleted. = Add additional data to the list, see chapter "Map additional data", p. 371. = Remove additional data from the list, see chapter "Delete additional data assignment", p. 372.

3. To save the settings, click on the button *Save*.

⇨ Upon activating the option *Delete duplicates...* the recordings are checked for duplicates and the detected duplicates are deleted.

7.1.5.2 Additional data

7.1.5.2.1 Map additional data

In addition to the start time and the end time, you can configure more additional data which is supposed to be used for checking for duplicates.

1. In the list *Additional data*, click on the icon *(Add)* to configure more additional data.

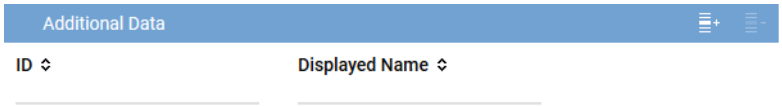


Fig. 433: Map additional data

2. Select the respective additional data from the list which are supposed to be used additionally to check for duplicates.
   To select several entries or revoke a selection, click on the respective line while holding the [Ctrl] key down.

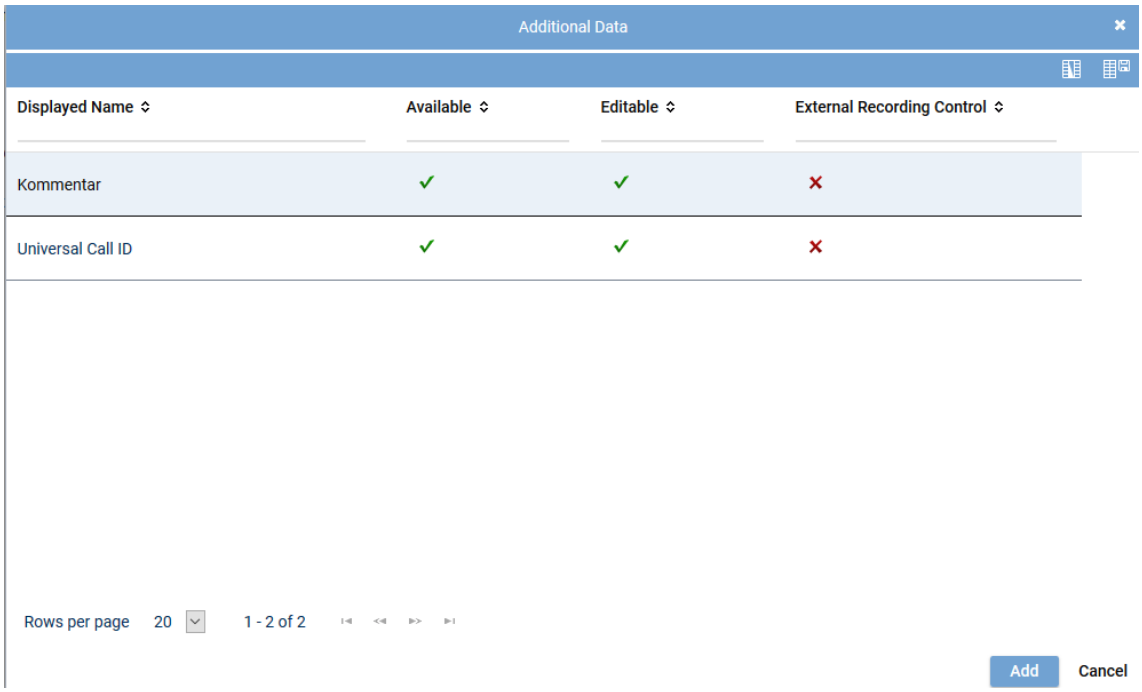


Fig. 434: Select additional data

NOTICE! The list contains only additional data which have been configured in the Additional Data module previously.

For information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

3. To apply the selection, click on the button *Add*.
   To discard the selection and close the window, click on the button *Cancel*.

7.1.5.2.2 Delete additional data assignment

1. Select the tab *Parallel Recording*.
2. Select the additional date that you would like to remove in the list *Additional Data*.
3. Click on the icon *(Delete)*.

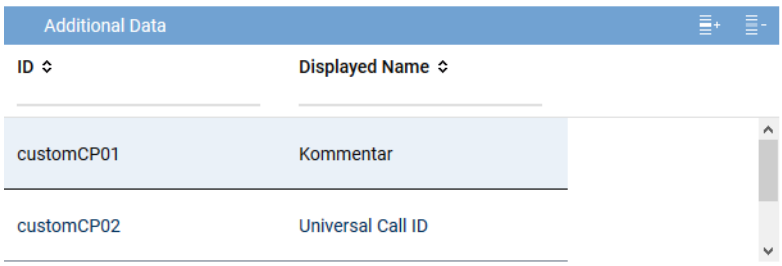


Fig. 435: Delete additional data assignment

7.1.5.3 Criteria to be ignored

In this group field, you can exclude certain criteria for duplicate detection which may prevent conversations to be detected as duplicates.

If conversations differ in just one attribute, they are not considered as duplicates. This holds true for conversations with different PBX IDs, for example.

To exclude this criterion during duplicate detection, add the respective attribute to the list of attributes which are supposed to be ignored.

In the list of available attributes, you can select which attributes are supposed to be excluded during duplicate detection. Click on the respective attributes and drag and drop them in the list of attributes to be ignored.

7.1.6 Standby management for failover architectures

For architectures with failover concepts, you can go to the standby management to manually select which server with which components is supposed to be active.
For architectures of the type *Parallel Recording*, you can also use the standby management if you have provided for the respective resources.
Using the standby management makes sense in the following cases:

- You would like to switch back to the primary server, e. g. when the standby server has automatically taken over and the primary server is now available again.
- You would like to switch to the standby server manually, e. g. during maintenance of the primary server.

ⓘ You can only edit the standby management if the corresponding architecture has been activated.

7.1.6.1 Standby management for All-in-one Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
   ⇨ If the selected recording architecture has been activated, the menu item *Standby Management* is active.

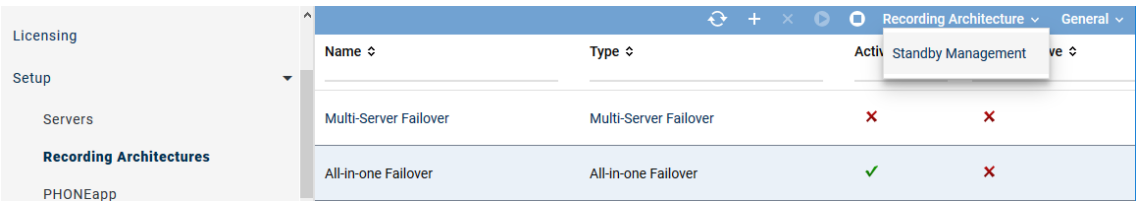


Fig. 436: Configure standby management

3. Click on the menu item *Standby Management*.
   ⇨ The window *Standby Management* appears.

Fig. 437: Switch server

Here, you see the assignment of the deployed components.
In the column *Status*, you can see which component is currently active.

4. To activate a standby server, select the respective server in the list.
5. Click on the icon *(Activate)* in the toolbar.

⇨ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server

ⓘ This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

1. To activate shutdown mode for a server, select the respective server in the list.
2. Click on the icon *(Activate shutdown mode)* in the toolbar.
   ⇨ The status of the server changes from *Active* to *Shutdown Mode*.
3. To deactivate shutdown mode again, click on the icon in the toolbar again.
   ⇨ The status of the server changes from *Shutdown Mode* to *Active*.

ⓘ In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

1. To activate a standby server, select the respective server in the list.

2. Click on the icon *(Activate)* in the toolbar.

⇨ The status of the standby server changes from *In Standby* to *Active*.
Only now can this server record new conversations.

7.1.6.2 Standby management for Multi-Server Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
   ⇨ If the selected recording architecture has been activated, the menu item *Standby Management* is active.

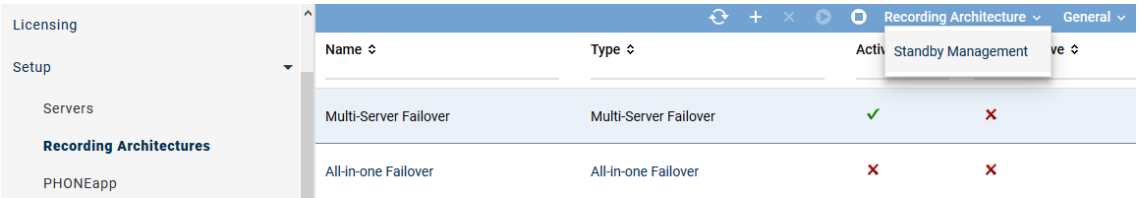


Fig. 438: Menu of the standby management

3. Click on the menu item *Standby Management*.
   ⇨ The window *Standby Management* appears.

Fig. 439: Switch server

If you have installed the required redundancy options on different servers, you can use standby management for the following components:

- **RC** *(Recording Control Standby Management)* to secure recording control

- **RM** *(Recorder Standby Management)* to secure recording
- **RIA** *(CTIconnect Standby Management* to secure the additional data of the recordings

Here, you see the assignment of the deployed components.
In the column *Status*, you can see which component is currently active.

4. To activate a standby server, select the respective server in the list.
5. Click on the icon *(Activate)* in the toolbar.

⇨ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server

ⓘ This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

1. To activate shutdown mode for a server, select the respective server in the list.
2. Click on the icon *(Activate shutdown mode)* in the toolbar.
   ⇨ The status of the server changes from *Active* to *Shutdown Mode*.
3. To deactivate shutdown mode again, click on the icon in the toolbar again.
   ⇨ The status of the server changes from *Shutdown Mode* to *Active*.

ⓘ In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

1. To activate a standby server, select the respective server in the list.
2. Click on the icon *(Activate)* in the toolbar.

⇨ The status of the standby server changes from *In Standby* to *Active*.
Only now can this server record new conversations.

7.1.7 Adjust neo configuration files

Some parameters cannot be configured via the graphic interface but have to be adjusted in the configuration files.

7.1.7.1 Adjust recording control

1. Open the Windows Explorer.
2. Change to the installation directory of the recording software *\Program Files (x86)\ASC\ASC Product Suite\data\RecordingControl*.
3. Open the configuration file *ASC.RecordingControl.ini* with the Editor.

Configure merging

4. Set the following parameter to *0* so that the conversations are not merged via the URI or the phone number.

   Section [SimSettings]

   - `simRMMergeViaParticipants=0`

5. Save the changes in the configuration file.
6. Restart the service *ASC RecordingControl* so that the changes are applied.

For further information about how to adjust the configuration files contact your local ASC support or call ASC support at +49 700 27278776.

7.2 Configure CTIconnect add-on

7.2.1 Configure OpenScape Contact Center (optional)

7.2.1.1 Create user for CTIconnect

Create a user in OSCC server administration.

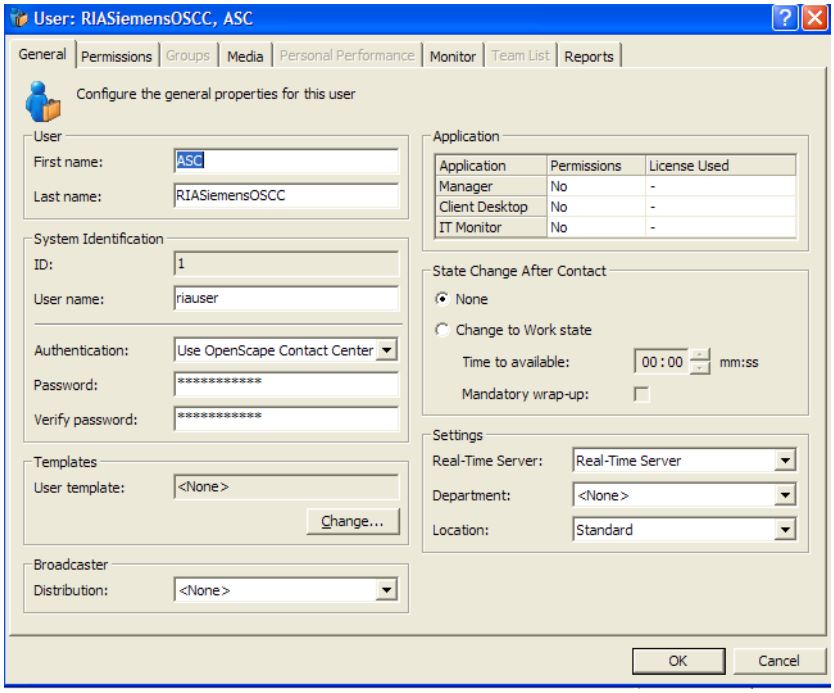


Fig. 440: Create a user for CTIconnect service

This user does not need other special authorizations. All other settings can remain on default values.

7.2.2 Configure Genesys T-Server (optional)

7.2.2.1 Configure IP address and port of the Genesys T-Server

1. Log in to the Genesys Administrator.
2. Click on the menu item *Environment* > *Applications* in the navigation bar.

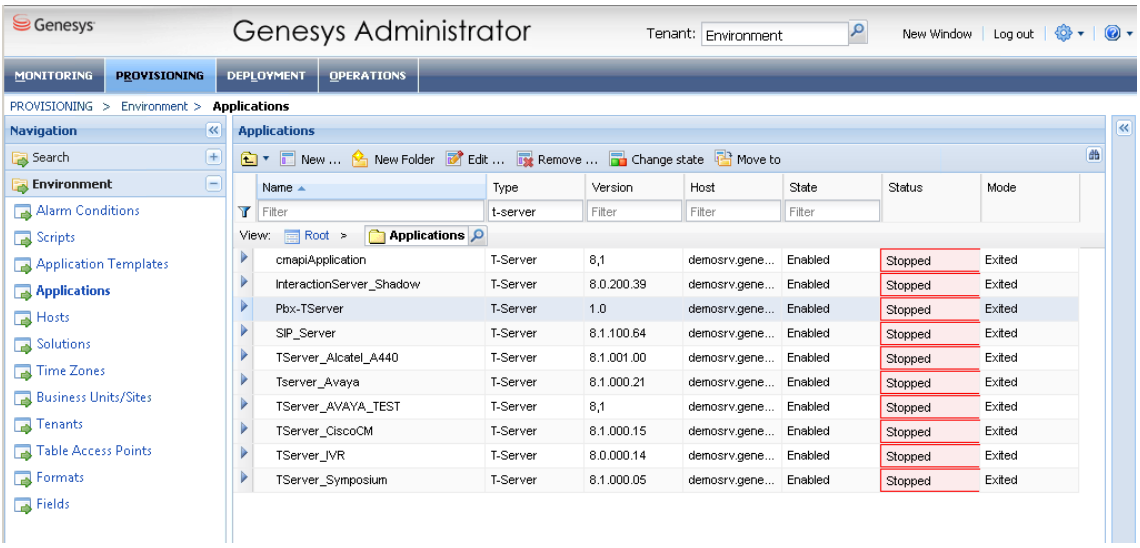


Fig. 441: Genesys Administrator - select T-Server

3. Double-click on the entry T-Server which has been connected to the switch instance to be monitored.

   ⇨ The window *Configuration* appears.

4. Expand the area *Server Info*.

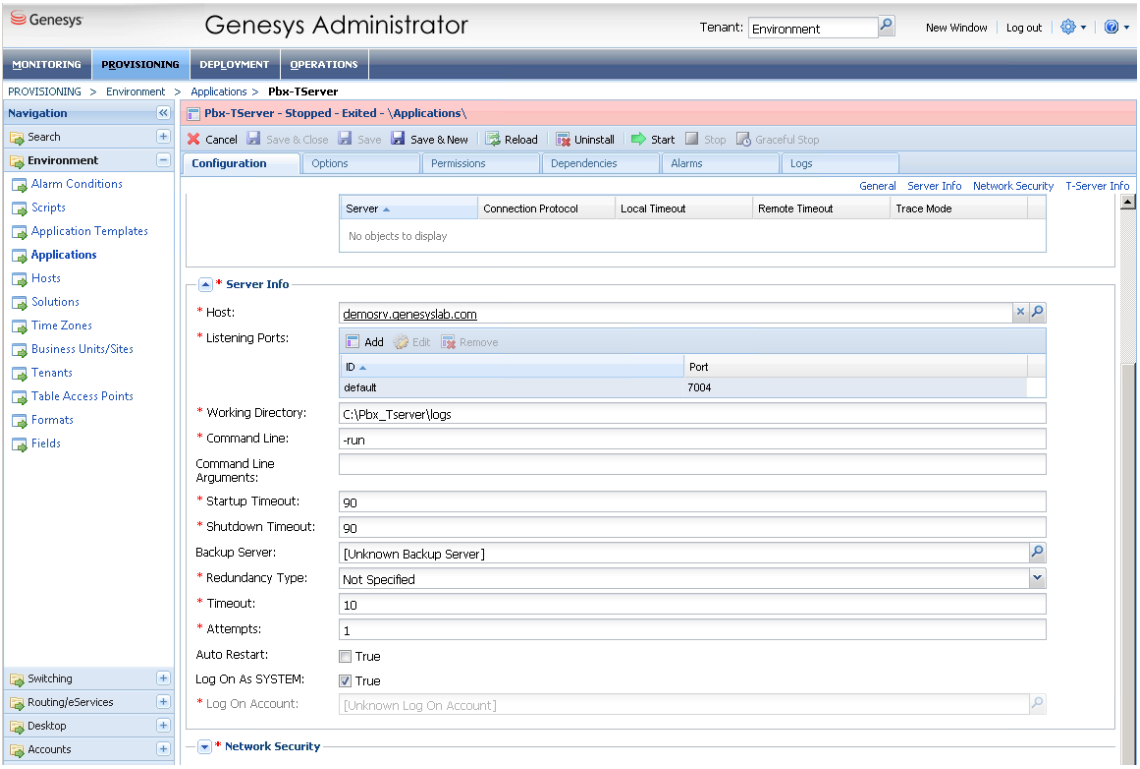


Fig. 442: Genesys Administrator - configure T-Server

5. In the field *Host*, enter the IP address or the computer name of the T-Server, e. g. *demosrv8.genesyslab.com*.
6. In the field *Listening Port*, enter the port of the T-Server, e. g.

7.2.2.2 Configure IP address and port of the Genesys Configuration Server

1. Click on the menu item *Environment* > *Applications* in the navigation bar.

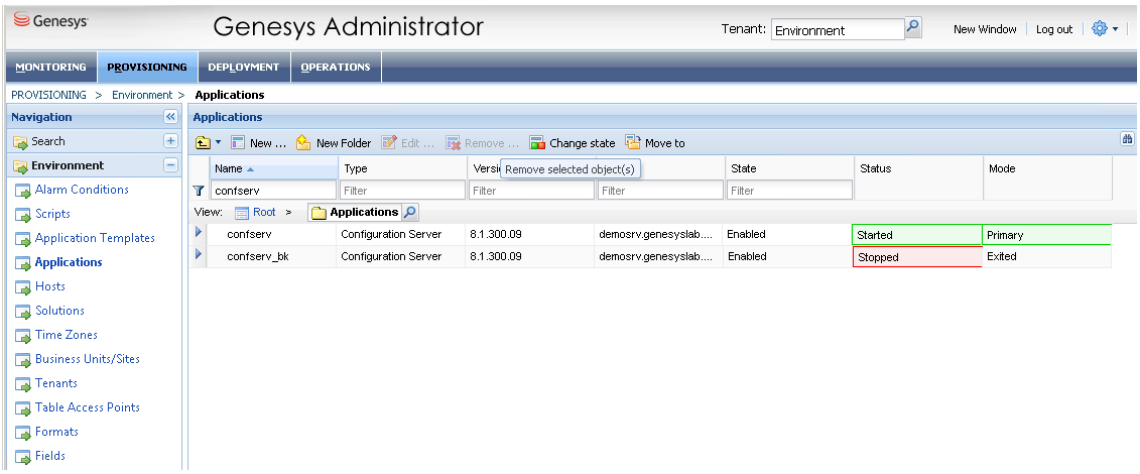


Fig. 443: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.

   ⇨ The window *Configuration* appears.

3. Expand the area *Server Info*.

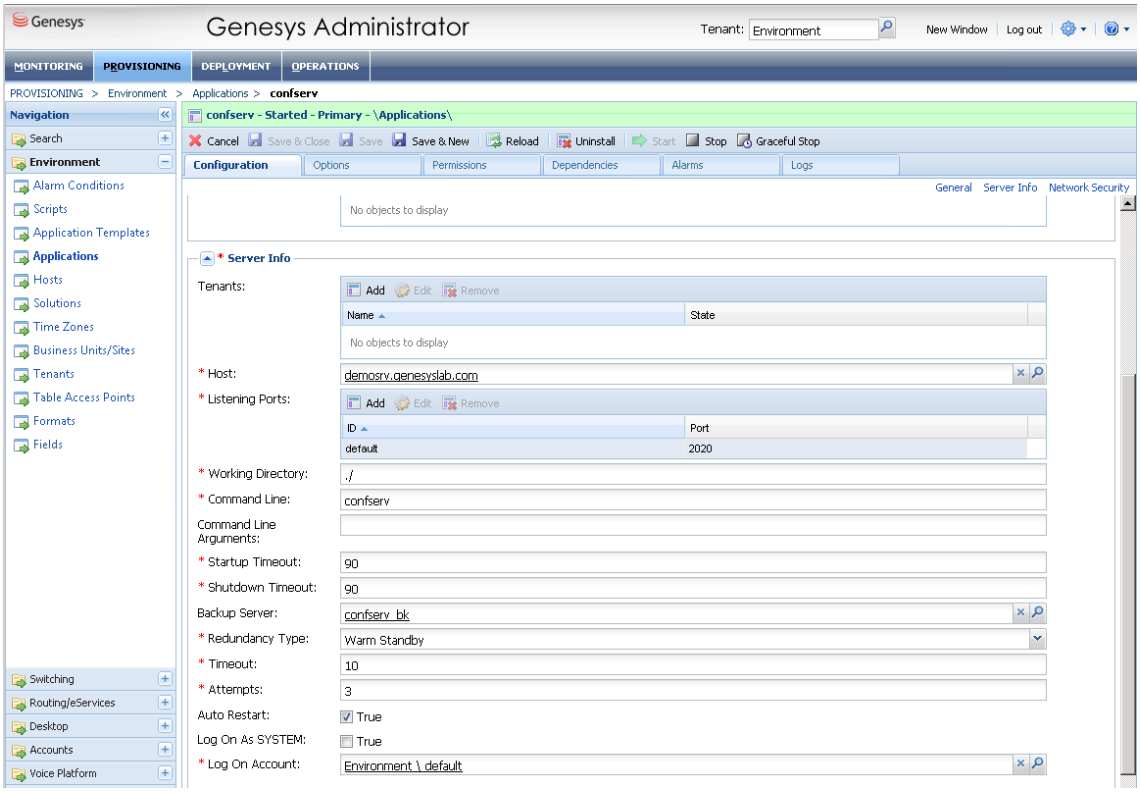


Fig. 444: Genesys Administrator - configure configuration server

4. In the field *Host*, enter the IP address or the computer name of the configuration server, e. g. *demosrv8.genesyslab.com*.
5. In the field *Listening Port*, enter the port of the configuration server, e. g. *2020*.

7.2.2.3 Configure switch instance in the Genesys Configuration Server

1. Click on the menu item *Switching* > *Switches* in the navigation bar.

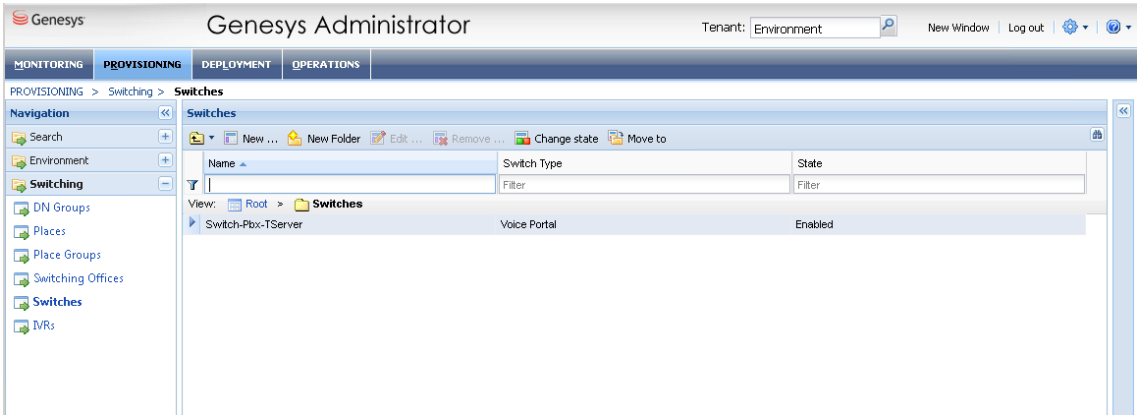


Fig. 445: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.

   ⇨ The window *Configuration* > *General* appears.

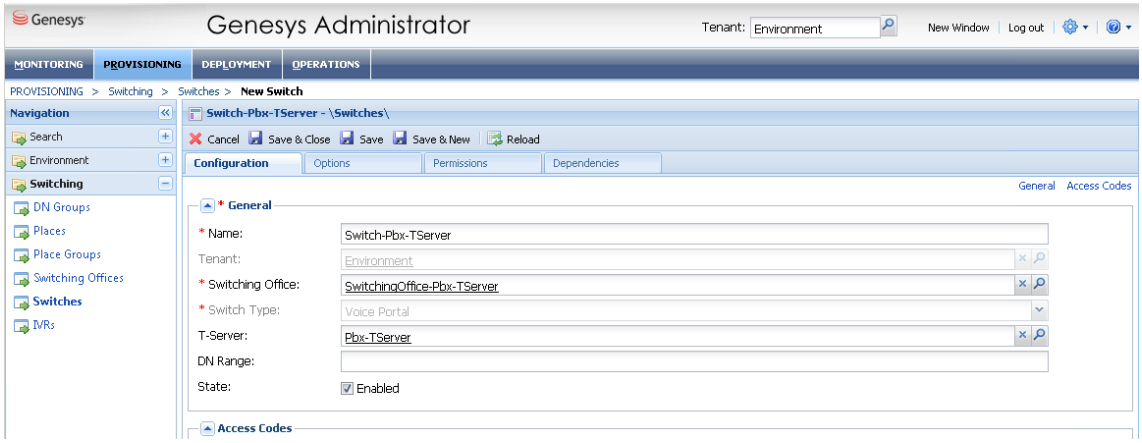


Fig. 446: Genesys Administrator - configure switch instance

3. Enter the same name in the configuration as in the Genesys T-Server.
4. Check whether the T-Server is identical to the T-Server configured in the Genesys T-Server.
5. Click on the button *Save* to save the entries.

7.2.2.4 Create users for the Genesys Configuration Server

To access the Genesys Configuration Server, you have to create a user.

1. Click on the menu item *Account* > *Users* in the navigation bar.
2. Click on the button *New*.

   ⇨ The window *Configuration* > *General* appears.

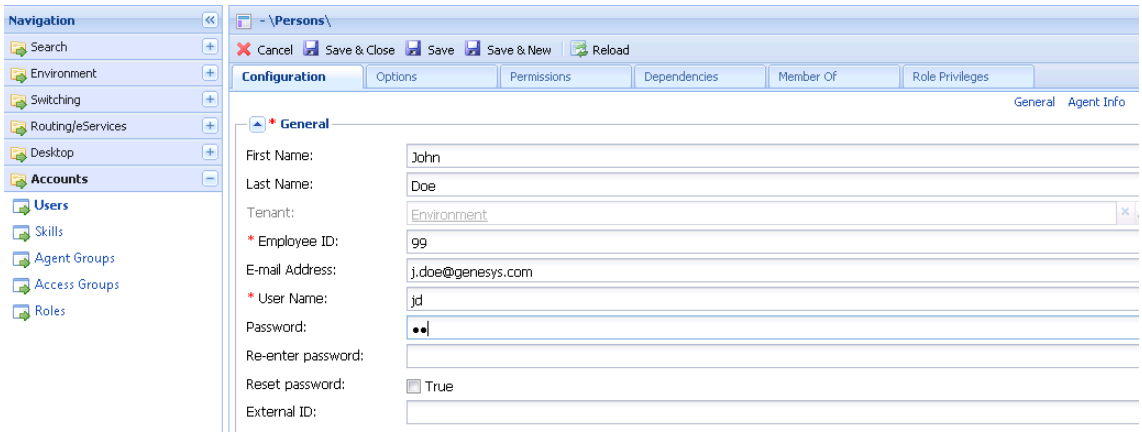


Fig. 447: Genesys administrator - create user

3. Complete the mandatory fields *Employee ID*, *User Name*, and *Password*.
4. Assign the user the rights to the created switch instance.
5. Click on the button *Save* to save the entries.

List of figures

List of tables

Glossary

API

Application Programming Interface

API server

Server on which the API service runs. (API=Application Programming Interface)

CSV

Comma-separated values is a file format which stores tabular data in plain text form.

DNS

Domain Name System is a worldwide directory service which administrates the name domain of the Internet. It main task is to answer the queries regarding name resolutions. (Source: Wikipedia 5th April 2017)

DTMF

Dialed Dual Tone Multi Frequency keys represent dialing signals on the analog connecting cable of the telephone. This is a method to transmit the phone number to the telephone network or to a PBX.

IP

Internet Protocol, basic protocol for Internet communication

LCR

Last Conversation Repeat

OSCC

OpenScape Contact Center

PBX

Private Branch Exchange

RTP

Real-time Transport Protocol is a protocol to continuously transmit audio and video files via the IP protocol within the network.

SDK

Software Development Kit

SIP

Session Initiation Protocol

SIPREC

Session Initiation Protocol Recording

SSL

Secure Socket Layer

TCP

Transmission Control Protocol, controlled connection establishment, secure data transmission, controlled connection termination

TDM

Time Division Multiplexing is an umbrella term for time-slot-oriented interfaces, ITU G.703 defined. The term is used ASC-wide representative for conventional telephony.

TLS

Transport Layer Security, former name Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

UDP

User Datagram Protocol UDP is a minimal, connectionless network protocol which belongs to the core members of the Internet protocol suite. Its purpose is to make sure that data transmitted via the Internet reach the designated application. There is no destination check.

URL

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)

VM

Virtual machine

VoIP

Voice over IP

XML

Extensible Markup Language is a human-readable and machine-readable language which defines a set of rules for encoding documents.