

EVOIPneo passive for SIP



Administration manual for system providers

3/29/2022

Product line neo, version 7.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (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>.

Copyright © 2022 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Contents

1	General information	5
2	Introduction	6
3	System requirements.....	8
3.1	Hardware components	8
3.1.1	Recorder	8
3.1.2	Additional requirements	8
3.2	Software components	8
3.3	Supported end devices	8
3.4	Additional restrictions	9
3.5	Genesys system components (optional)	9
3.5.1	Genesys Framework	9
4	Installation requirements	10
4.1	Licenses	10
4.2	Information	10
5	Overview install and configure product.....	11
6	Installation	12
6.1	Install OpenScope Contact Center Campaign Director (optional).....	12
6.1.1	Add database entry	13
6.1.2	Define recording profile as default	14
7	Configuration.....	15
7.1	System Configuration.....	15
7.1.1	Start application	15
7.1.2	Configure recording solution	16
7.1.2.1	Configure recording solution All-in-one Basic	16
7.1.2.2	Configure recording solution All-in-one Failover	67
7.1.2.3	Configure recording solution All-in-one Parallel Recording.....	120
7.1.2.4	Configure recording solution Multi-Server Recording	173
7.1.2.5	Configure recording solution Multi-Server Failover	226
7.1.2.6	Configure recording solution Multi-Server Parallel Recording	280
7.1.3	Adjust neo configuration file	333
7.1.3.1	Adjust Recording module	333
7.1.4	Configure Recording Content Validation	336
7.1.5	Configure CTIconnect add-on	338
7.1.5.1	Configure Genesys T-Server (optional)	338
8	Troubleshooting.....	343
	List of figures	344
	List of tables	354



Glossary 357

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.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization 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} passive for SIP provides the functionality which is necessary for the recording of unencrypted conversations in a SIP environment.

In this passive recording solution, the recording server is no active communication participant.

The data packages are duplicated at the network switch and sent to a dedicated separate network card of the recording device via the monitor/mirror/SPAN port.

The conversation data is extracted from the RTP packages. Additional data such as phone number, call direction, and duration of the conversations are extracted from the SIP signaling and processed.

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.

EVOIP_{neo} passive for SIP

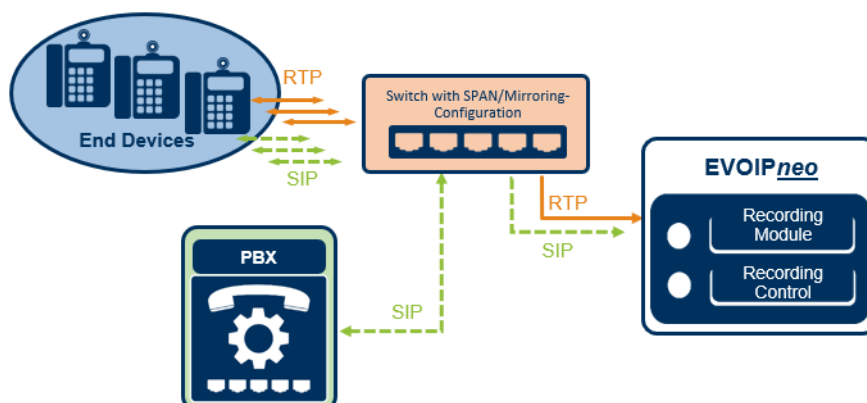


Fig. 1: Overview of the recording solution



For more information about the switch configuration refer to the administration manual *Configuration switch for passive VoIP recording* and in the installation manual *Configuration virtualization*.

EVOIPneo passive for SIP - SIP trunk recording

Conversation data and additional data are recorded by capturing the network packages at the SIP trunk at the gateway or an SBC.

EVOIP_{neo} passive for SIP – SIP trunk recording

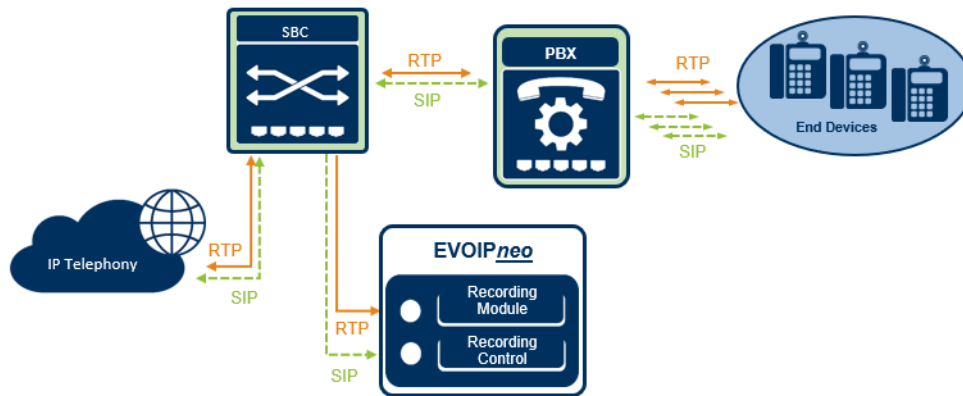


Fig. 2: SIP trunk recording with gateway or SBC

The data packages or Ethernet frames are duplicated at the network switch and sent to a dedicated network port of the recording server via the monitor/mirror/**SPAN** port. The audio data is extracted from the **RTP** packages and the additional data from the Ethernet frames and de-coded.

The following additional data is available:

- *Date and time*
- *Call duration*
- *Dialed and called phone number*
- *Call direction*

Restrictions

- Internal calls are not recorded
- Encrypted trunks cannot be recorded.
- In trunk-side recording, mapping the agents to the recordings is not possible. For one thing, the internal phone number is hardly ever called directly via the trunk (collective phone numbers instead of direct extension) and for outgoing calls, the internal phone number is rarely signaled on the trunk. For another, it cannot be determined either whether a call has been forwarded, accepted by a representative or included in a conference.

Therefore, it is not possible to

- control recordings via **CLIENT_{command}** or **WEB_{command}**,
- record with **SCREEN_{rec}** scan,
- carry out quality management,
- track the actual call history with all participants.
- **PHONE_{app}** universal is not supported.



These restrictions do not apply when using **CTI_{connect}** for Genesys T-Server in connection with SIP passive. In this case, the conversation history can be tracked and participants mapped via Genesys T-Server. However, internal conversations are not recorded either.

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.

3.1.2 Additional requirements

A network switch is required which provides one or several SPAN ports.



For further information about the switch configuration refer to the administration manual *Switch configuration for passive VoIP recording*.

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 Supported end devices

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

The following RFC standards are supported:

- RFC 3261 (SIP)
- RFC 3550 (RTP)
- RFC 3665 (SIP Basic Call Flow Examples)
- RFC 4566 (SDP Session Description Protocol)
- RFC 4733 (DTMF) optional

- RFC 6068 ([DTMF](#) via SIP INFO) optional

For the recording to work, the phone numbers must be transferred in the [SIP](#) communication. The information must be contained in the To and From headers in the [SIP](#) invite.

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

3.4 Additional restrictions



The recording of encrypted calls is not supported in this solution. Encryption must be deactivated for the end devices to be recorded.

3.5 Genesys system components (optional)

3.5.1 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 - passive	1 license per recording server
EVOIP _{neo} passive for SIP	1 license per concurrent recording

Tab. 1: Licenses of ASC

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. 2: Licenses for Genesys

Sparkassen FI ISP (optional)

License name	Number
CTI _{connect} for Sparkassen FI ISP	1 per recording system

Tab. 3: Licenses for Sparkassen FI ISP optional

OpenScape Contact Center Campaign Director (optional)

License name	Number
CTI _{connect} for Unify OpenScape Contact Center Campaign Director	1 per recording system
Search & Replay Access software license	1 per concurrent user
Search & Replay Access system license	1 per recording system

Tab. 4: Licenses for OpenScape Contact Center Campaign Director optional



Depending on the deployed PBX additional vendor-specific licenses can be required.

4.2 Information

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

- Name of the network connection in Windows which is supposed to be used for recording. The name is selected from the drop-down list during the configuration.
- IP address of the recording server
- IP addresses or MAC addresses of known network components which are no phones, e. g. PBX, media server, gateways, etc.

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
Link the integration to the previously created recording architecture.
 - Configure recording servers
Configuration of the parameters of the recording server, e. g. sniffer card
 - Configure add-on
The add-on is disabled by default.
Optionally, you can configure the following add-ons for this recording solution:
Genesys T-Server
MiContact Center Business
OpenScape Contact Center
Sparkassen FI ISP
 - 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 Microsoft Windows Server 2016*, *Configuration Microsoft Windows Server 2019* or *Configuration Microsoft Windows Server 2022*.



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 OpenScape Contact Center Campaign Director (optional)

If you would like to use the software CTIconnect for Unify OpenScape Contact Center Campaign Director, you have to proceed as follows.

1. Copy the file CTIConnect UCD-41.3.0.zip from the recording server from the directory:
\\Program Files (x86)\\ASC\\ASC Product Suite\\modules

to the server of the Unify Campaign Director into the directory:

\\Program Files\\Siemens\\OpenScape Contact Center Campaign Director\\RDS\\Implementations

6.1.1

Add database entry

1. Add the following entry to the database table *SriImplementation*:

Name	Description	Configuration
ASC Recording	ASC neo recording solution	<pre><?xml version="1.0" encoding="utf-8"?> <configuration> <option name="local_ip" datatype="string" display="local ip to bind the PIF connection" type="required" value="192.168.170.41"/><option name="port" datatype="numeric" display="port for the PIF connection" type="required" value="9020" minvalue="9020" maxvalue="10000"/> </configuration></pre>

ImplAssembly	ImplClassMain	ImplClassAgent	ImplClassCall	GuiS- napIn- Class	UserBuiltIn
CTIconnectUCD.dll	CTIconnectUCD.CTI- connectUCD	CTIconnectUCD.ASCAgentSession	CTIconnectUCD.DefaultRecordingSession	NULL	0

NOTICE! The IP address 192.168.170.41 is exemplary; please insert the IP address of your Campaign Director! Port 9020 is the default port which may be adapted to your requirements.

6.1.2 Define recording profile as default

1. Open the Configuration Manager of the Campaign Director and define the Recording Interface Profile as default.

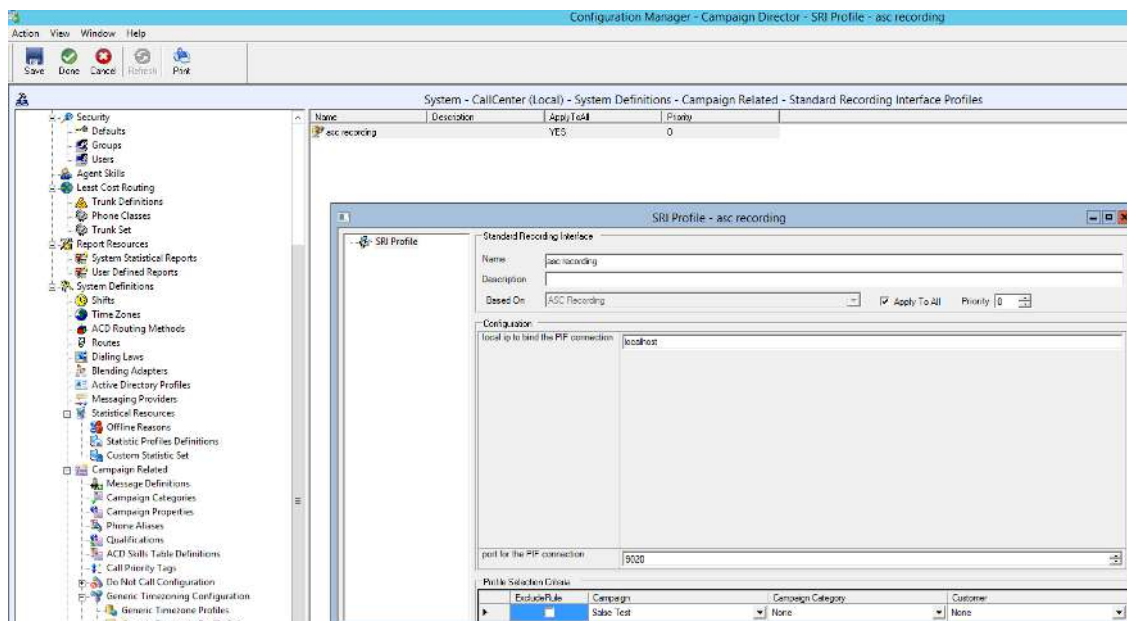


Fig. 3: Configuration Manager - Select recording profile as default

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>.

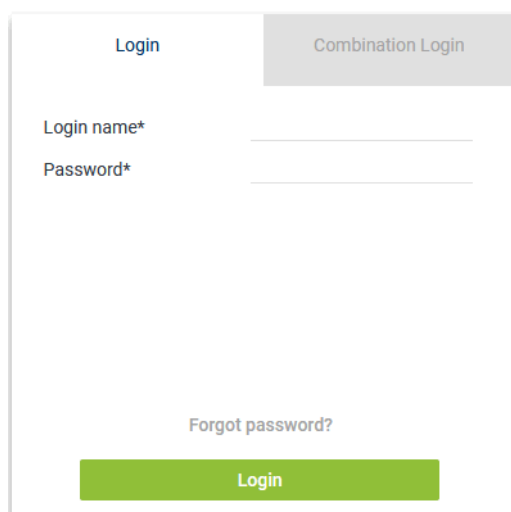


Fig. 4: System Configuration - web interface

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:	<i>system-admin</i>
Neo version < 6.3	
Default password:	<i>1</i>
	If the default password <i>1</i> 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:	<i>A\$c123</i>

Tab. 5: Login data - system provider

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

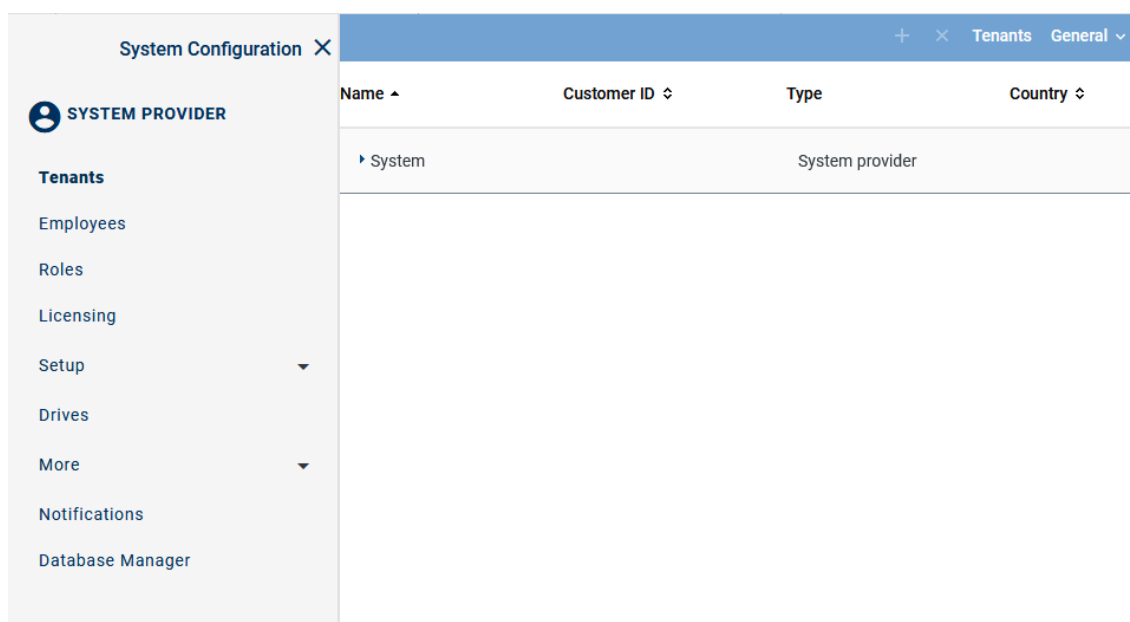


Fig. 5: System Configuration - main view:

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

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:

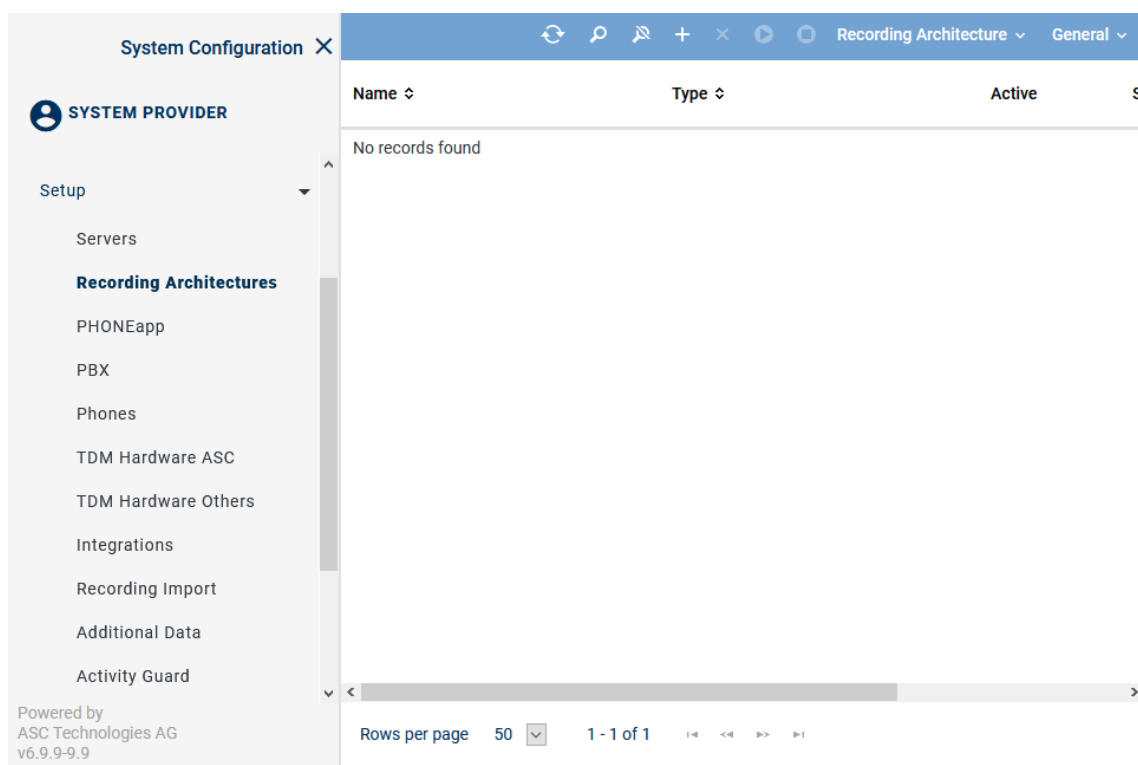




Fig. 6: Recording architectures - main view

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. 7: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

Create a recording architecture of the type *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.

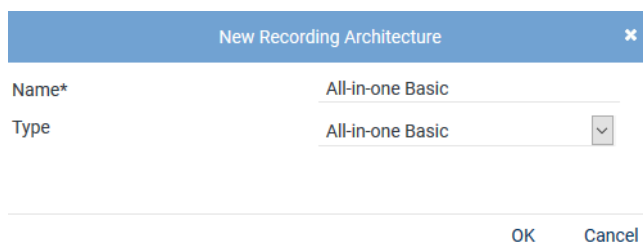
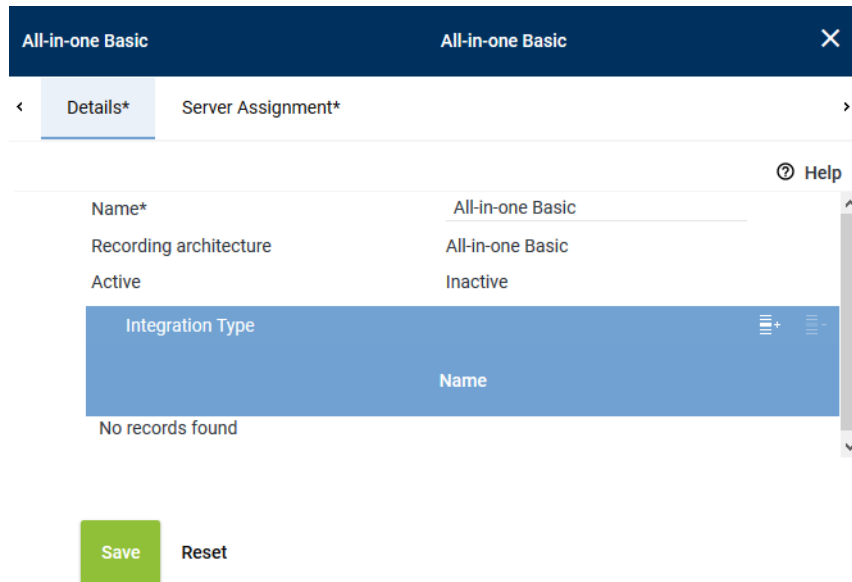


Fig. 8: Create recording architecture - All-in-one Basic Recording

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.



All-in-one Basic All-in-one Basic ✕

< **Details*** Server Assignment* >

ⓘ Help

Name* All-in-one Basic

Recording architecture All-in-one Basic

Active Inactive

Integration Type ⓘ ⓘ

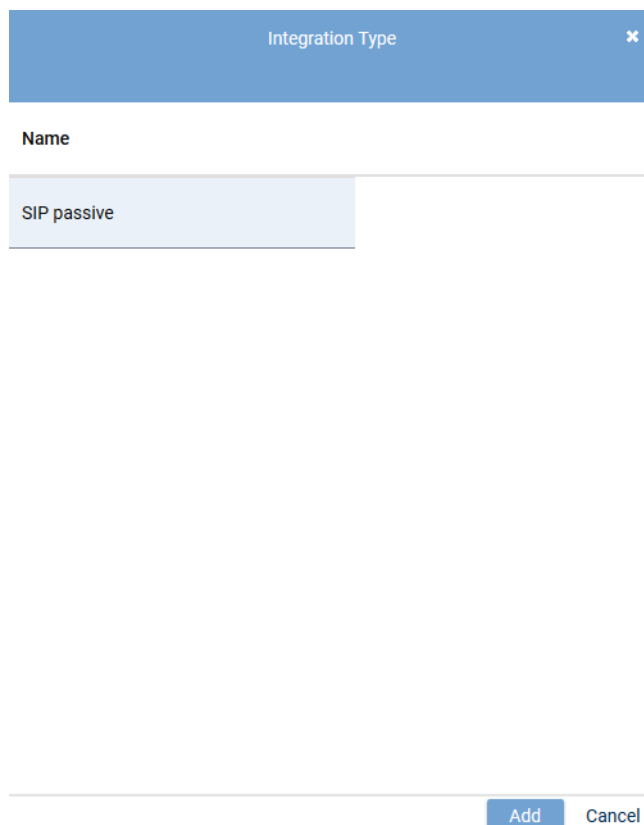
Name
No records found

Save Reset

Fig. 9: 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.



Integration Type ✕

Name

SIP passive

Add Cancel

Fig. 10: Select integration type



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



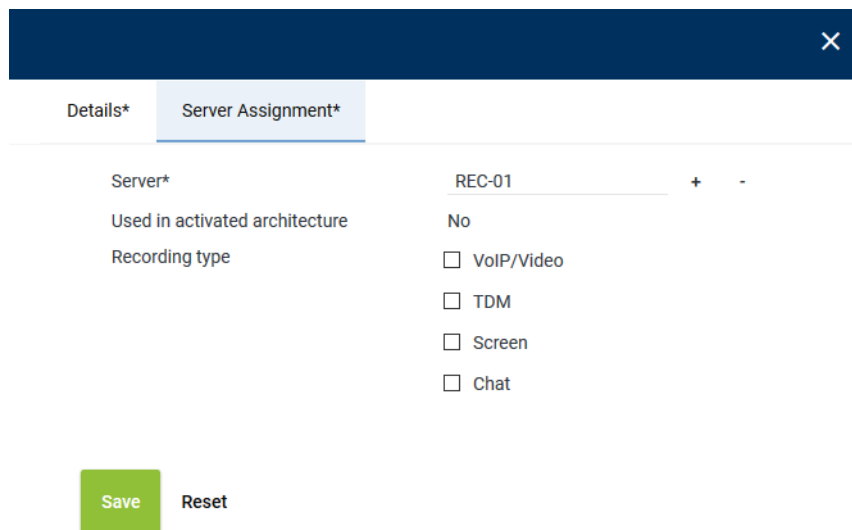
Any number of integration types can be assigned to a recording architecture.

2. Select *SIP passive* 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 view.

Assign server for All-in-one Basic

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



Details* Server Assignment*

Server* REC-01 + -

Used in activated architecture No

Recording type

☐ VoIP/Video

☐ TDM

☐ Screen

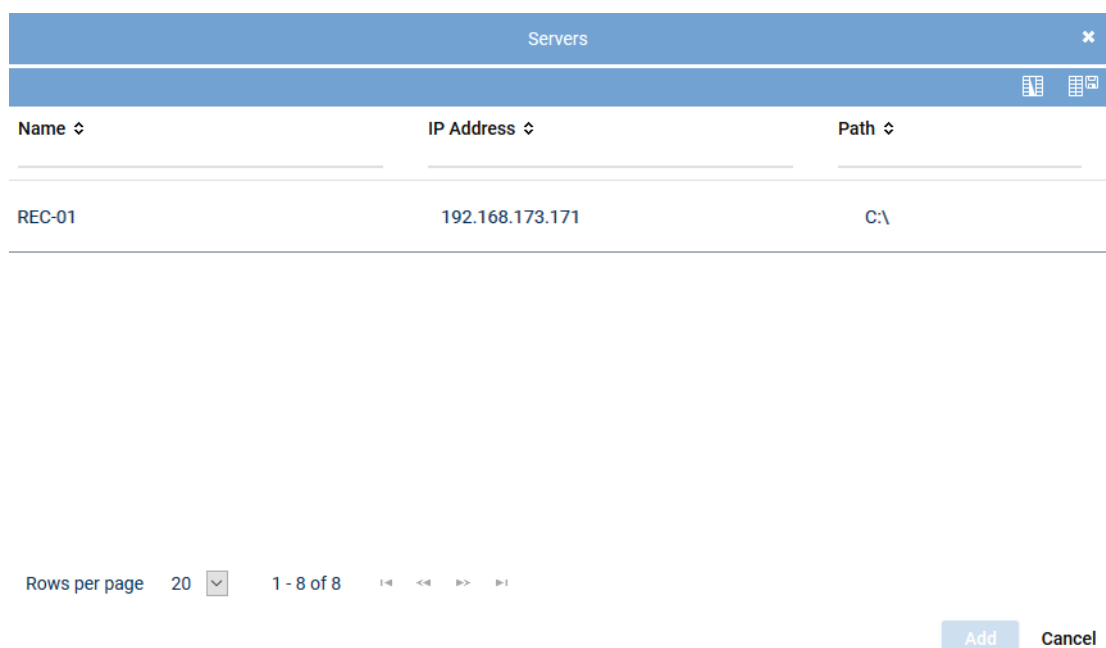
☐ Chat

Save Reset

Fig. 11: Recording architecture - tab Server Assignment

2. Click on the button *+* next to the entry field *Server*.

⇒ The window *Servers* appears.



Servers

Name ↕	IP Address ↕	Path ↕
REC-01	192.168.173.171	C:\

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 12: 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.

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen




☐ Chat

Fig. 13: 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 tool-bar becomes active.
3. To activate the recording architecture, click on the icon  (*Activate*).
⇒ In the column *Active*, the icon  (*Active*) appears.





Recording Architecture			
Name ▾	Type ▾	Active	Standby active ▾
All-in-one Basic	All-in-one Basic		

Fig. 14: 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:

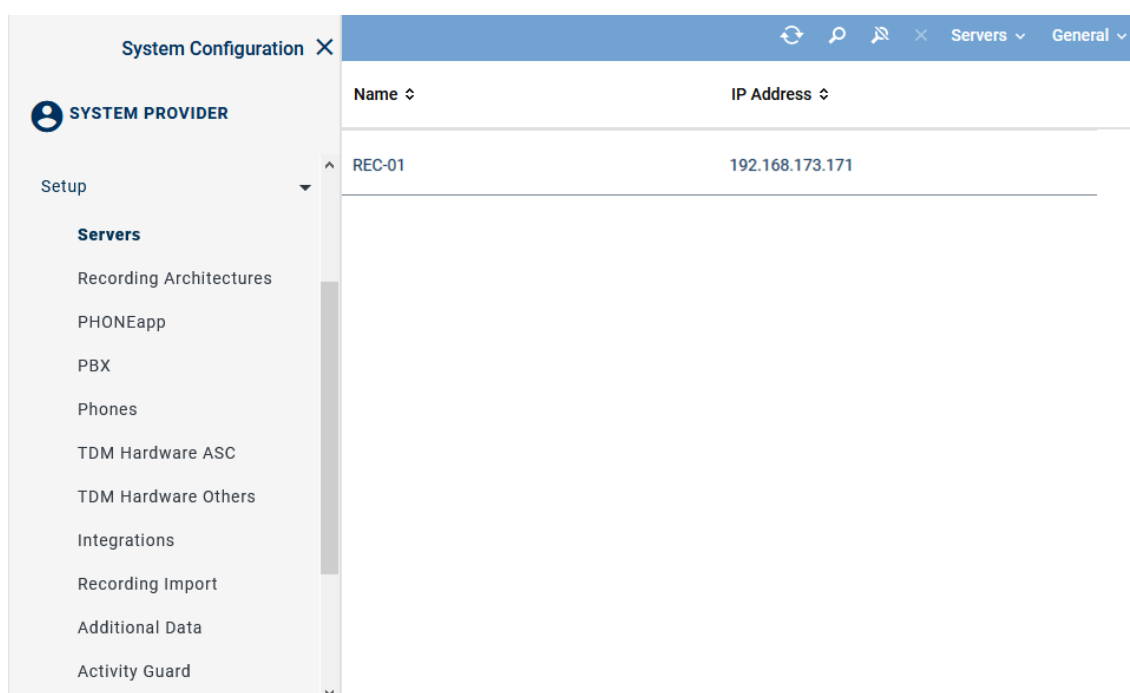


Fig. 15: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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.

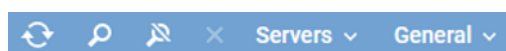







Fig. 16: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	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

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

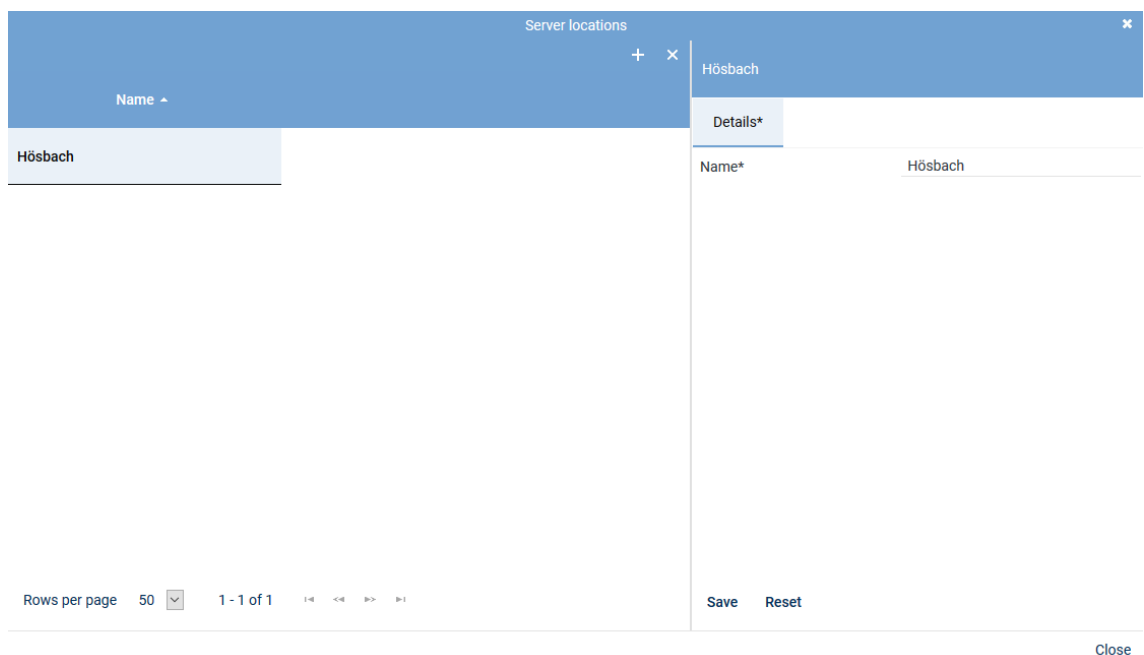



Fig. 17: Add server locations

- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.

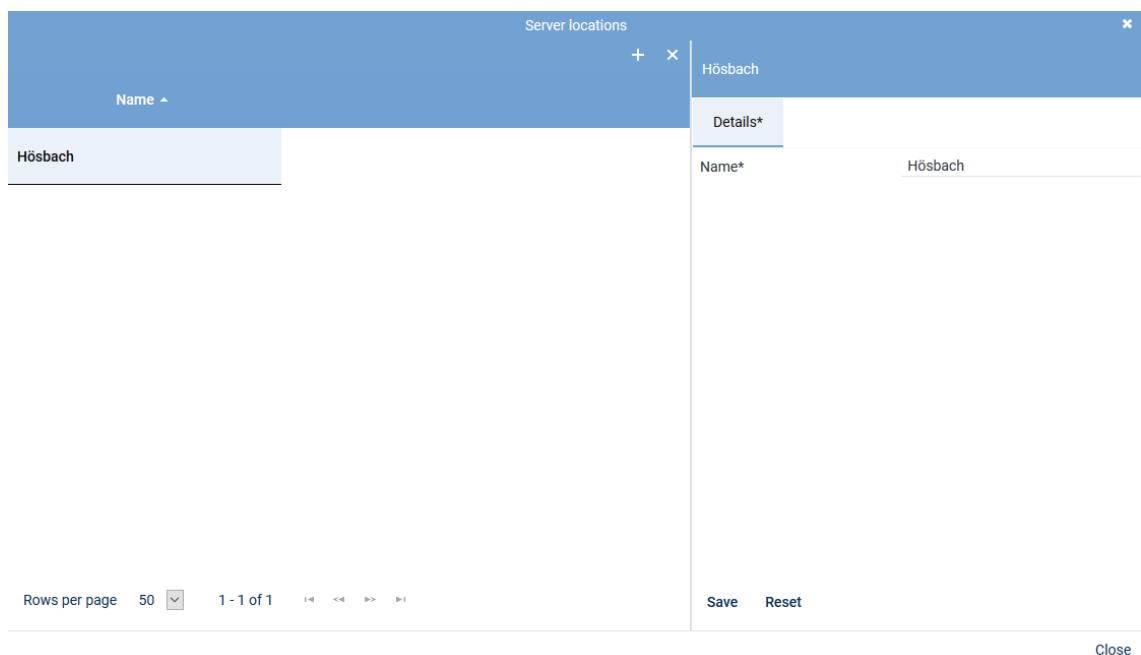
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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.



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a table with a header "Name" and a dropdown arrow. The table contains one row with the value "Hösbach". To the right of the table is a "Details*" tab. Below the table, there is a "Rows per page" dropdown set to "50" and a "1 - 1 of 1" indicator. At the bottom right of the window, there are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the entire screenshot area.

Fig. 18: 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.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
Key Ma >

? Help

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171 <input type="button" value="v"/>
Server location	Hörsbach <input type="button" value="v"/>

Fig. 19: Servers - tab Details

- From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
- Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.
- Click on the button **Save** if the entries are correct.

Tab Usage

- 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.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

API Server	▶
Audio Analysis	▶
Recording Control/Key Management	▶
Data Processing	▶
Replay	▶
Virtualization	▶

Fig. 20: Servers - tab usage

Group field API Server

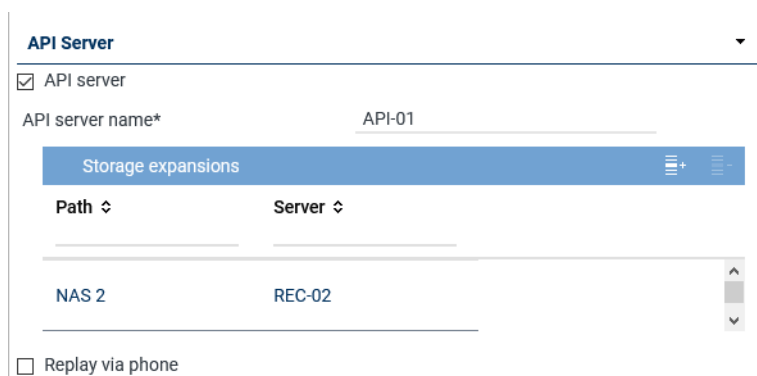




Fig. 21: Group field API Server

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
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 36.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 27. By clicking on the icon  (<i>Remove</i>), 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.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWER<u>play</u> Pro • Application POWER<u>play</u> Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 34. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.

Storage Expansion for Replay				
Device Type ↕	Name ↕	Path ↕	Free Disk Space ↕	Server ↕
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page: 20  1 - 1 of 1



 

Fig. 22: Select storage expansion

- 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

Audio Analysis

☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 23: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> 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

Emotion Detection ×

📋

Name ↕

REC-01

Rows per page 20 ▼ 1 - 8 of 8 1< << >> 8>

Add Cancel

Fig. 24: Select server for emotion detection

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

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☐ Recording control/Live Streaming

Recording architecture Please choose... ▼

☐ neo key management

Fig. 25: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 7: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 26: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list</p>

Parameter	Value/Description
	<p><i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 31. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 31. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Replay server</i> 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. <p>NOTICE! For the export from Neo to Neo, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> • <i>Recording architecture</i> 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. <p>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.</p>

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.

Target Server	
Name	IP Address
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173

Fig. 27: Select server



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

- 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

Replay

☒ Replay

Replay server*

replay1

WebSocket port*

12345


(max. 5 characters)


API server*

Name

Connection Status

Fig. 28: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. 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.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 33.

Parameter	Value/Description
	<ul style="list-style-type: none"> 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.
- To assign an [API](#) server, click on the icon  (Add) in the toolbar of the list *API Server*.
 - Select the server from the list on which the [API](#) service is running.



Fig. 29: 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](#).

- 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

Virtualization

☐ VM without Trusted License

Fig. 30: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <i>licensing.asc.de</i> If you enter this domain, there is no key management. • <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 10: Configure virtualization



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*.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

PBX +

PBX	PBX	▼
Extension* (max. 18 characters)	123456	
Media streamer IP address*	192.168.169.192	▼
Minimum port	24000	
Maximum port	24099	
Transport protocol	UDP	▼
SIP signaling port	5062	
User name		
Password		
PBX IP address		
PBX port	5060	
Registration required	<input checked="" type="checkbox"/>	
SIP registration expiration	3600	Second(s)

Save
Reset

Fig. 31: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>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. 40.</p>
Extension	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>

<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
>

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 32: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

< Usage* Media Streamer* Replay Server Address Mapping **Key Management** >

Key creation interval

☒ All
365 Day(s)

☐ Create key manually

Delay usage

until 0 Day(s) 0 Hour(s)

☐ Key expiration date

after 0 Day(s)

☒ In case of an error switch to simple key management automatically

Save Reset

Fig. 33: Servers module - tab Key Management

<i>Key creation interval</i>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> • <i>All</i> 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 • <i>Create key manually</i> Select that a key is supposed to be generated manually. <p>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.</p>
<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p>

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.

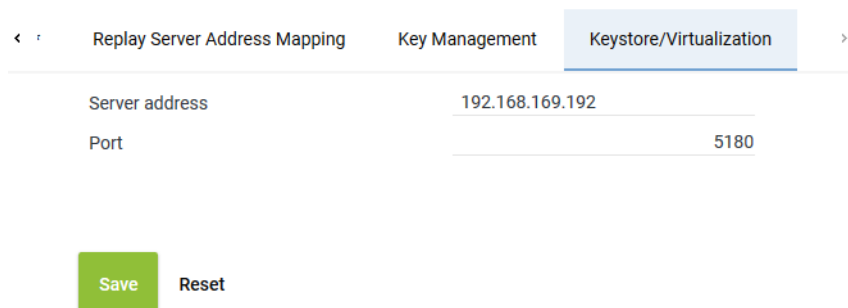


Fig. 34: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management: IP address of the server where the service <i>DongleMan</i> has been installed.
Port	<p>Enter the port for the connection.</p> <p>5180 = Dongle Manager</p> <p>8181 = ASC License Management System</p>



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:

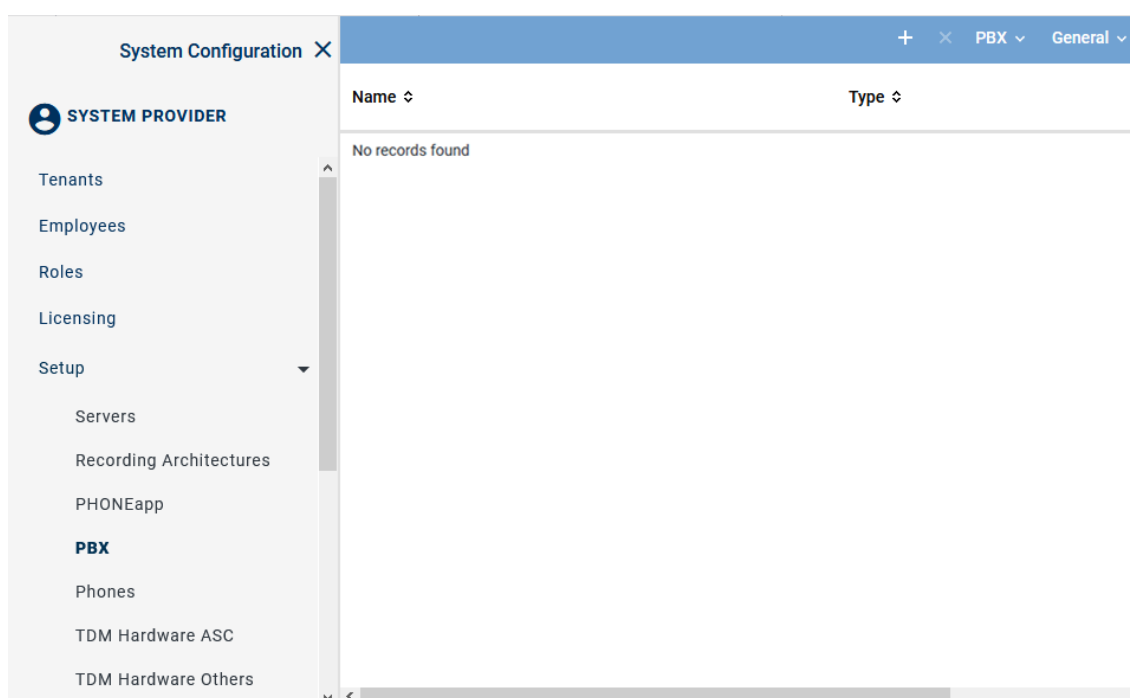




Fig. 35: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 36: Toolbar PBX module

	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

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

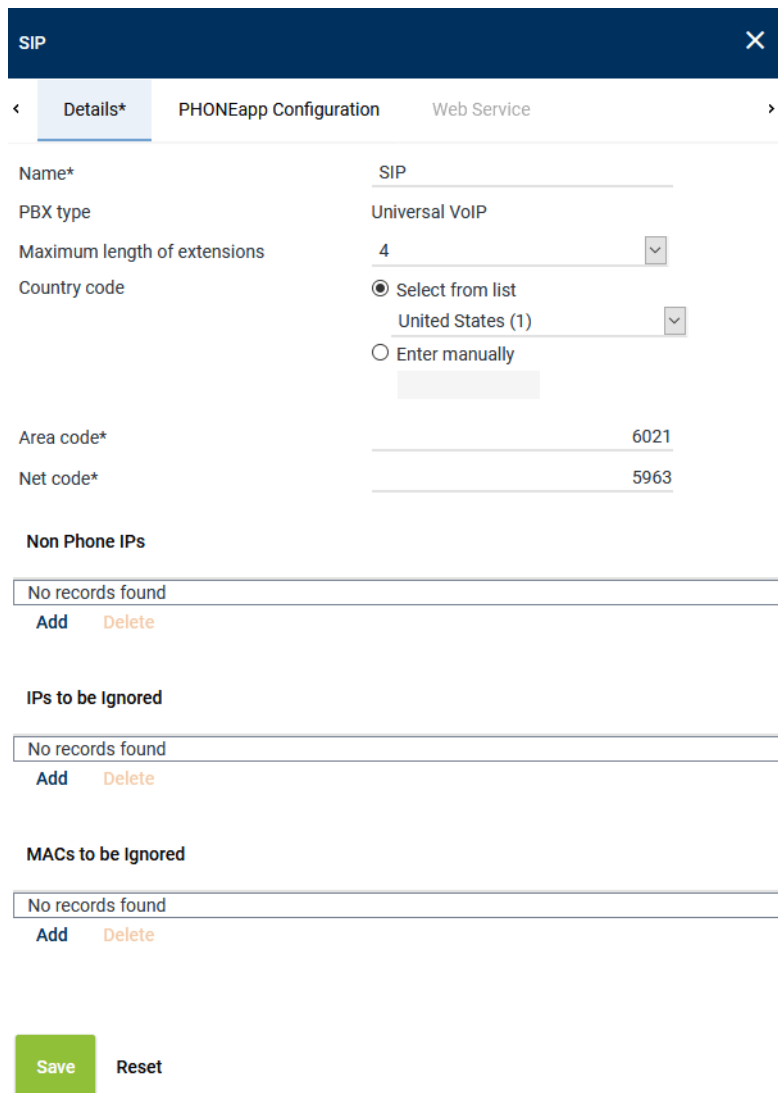


Fig. 37: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.

Parameter	Value/Description
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 11: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

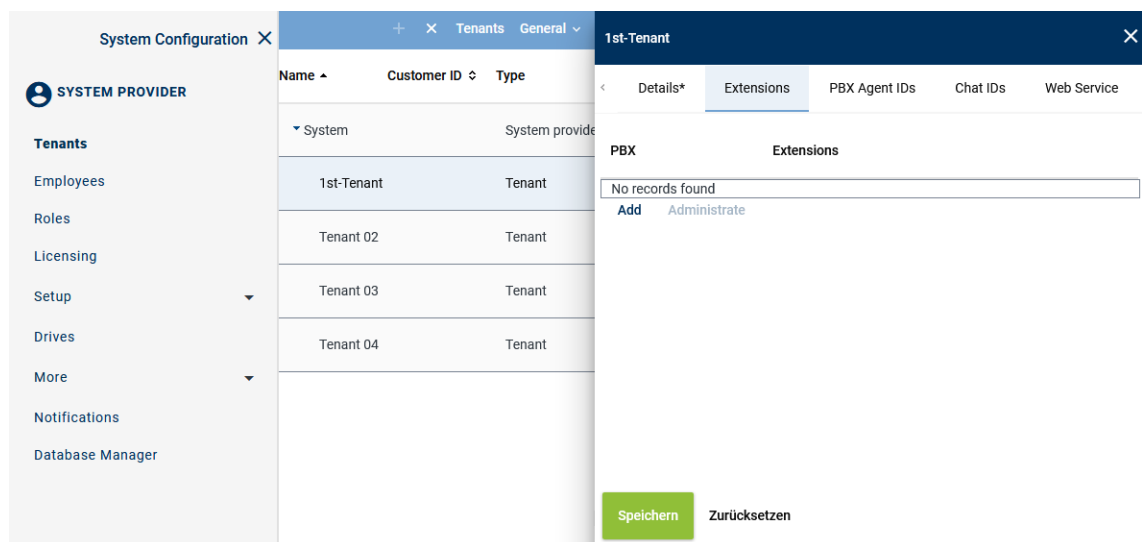


Fig. 38: Tenants - main view - tab Extensions

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:

Add Extensions ✕

PBX

PBX ▼

☐ File import

☐ File contains a headline

File name

...

☒ Manual entry

Extension or extension range separated by
 ", or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 39: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> ZIP TXT CSV <p>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.</p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP_{neo} passive for SIP - neo 7.x Rev. 1

45 / 358

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.

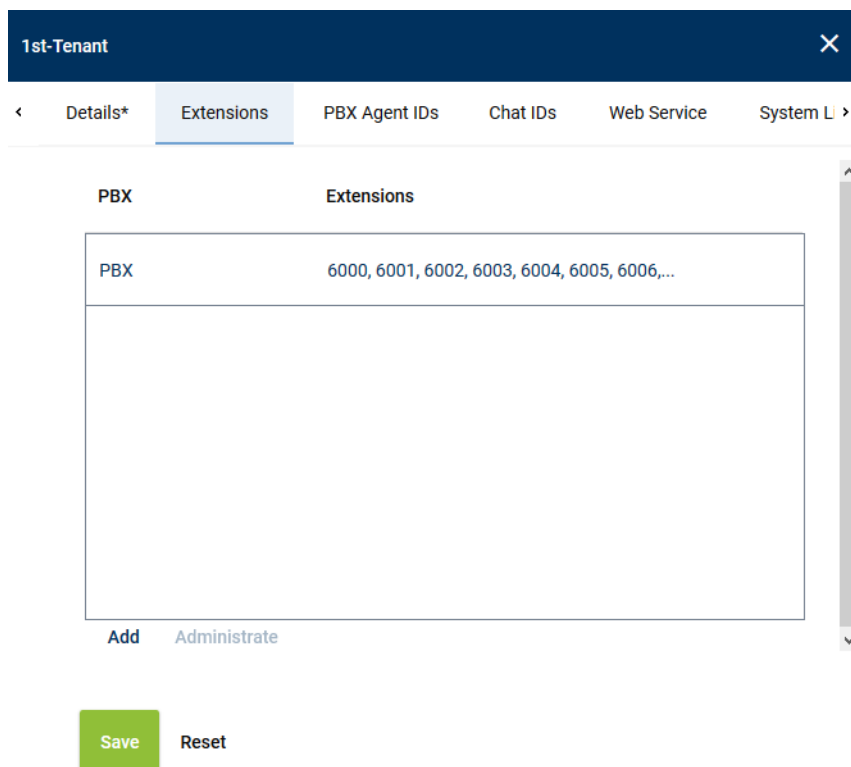
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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 detected, 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.



1st-Tenant

Details* Extensions PBX Agent IDs Chat IDs Web Service System L

PBX	Extensions
PBX	6000, 6001, 6002, 6003, 6004, 6005, 6006,...

Add Administrate

Save Reset

Fig. 40: Remove extensions

2. Click the button *Administrate*.

- 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.

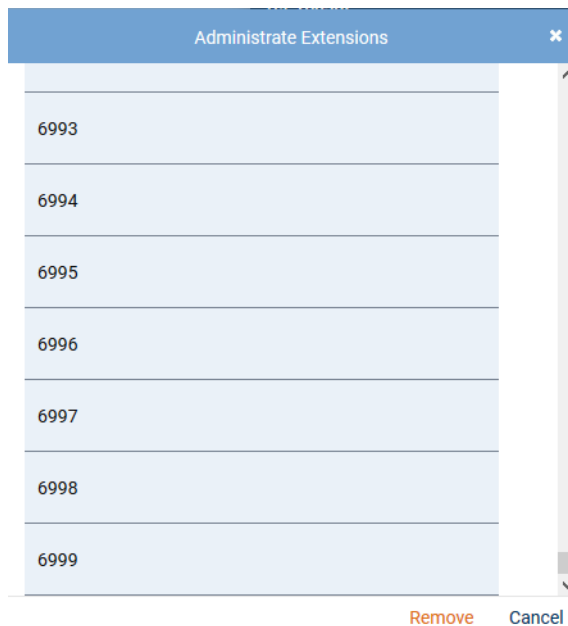


Fig. 41: Select extensions

- To remove the selected extensions, 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.

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

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

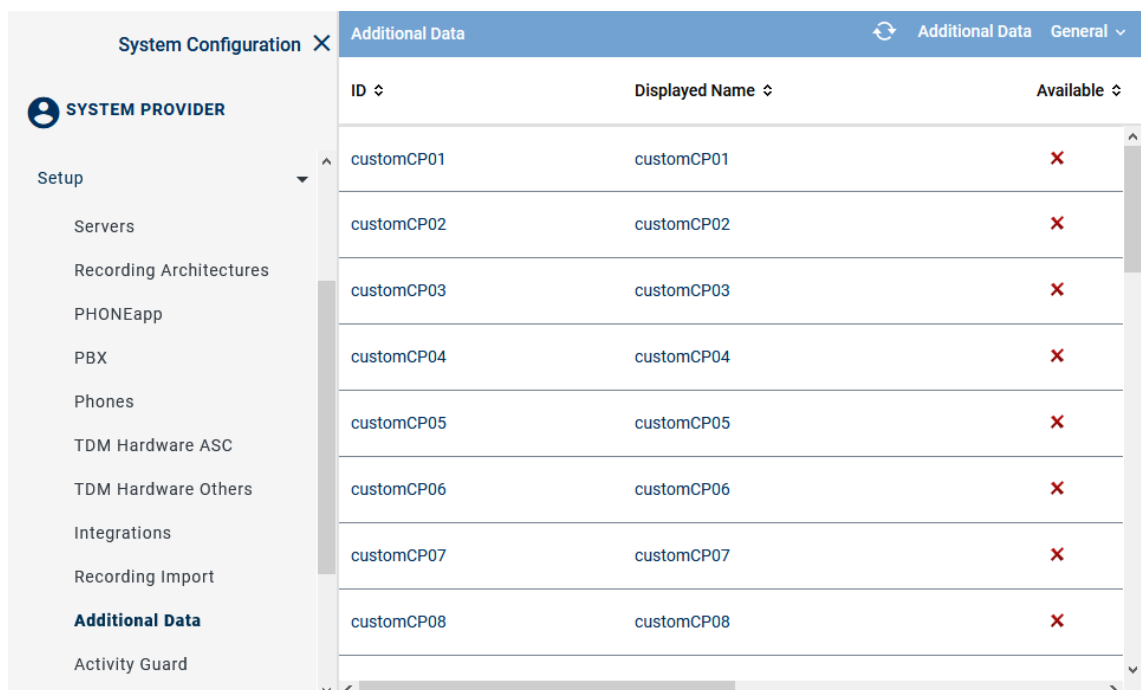


Fig. 42: Additional Data module main view

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

Change display name






Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	

Fig. 43: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 44: 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:

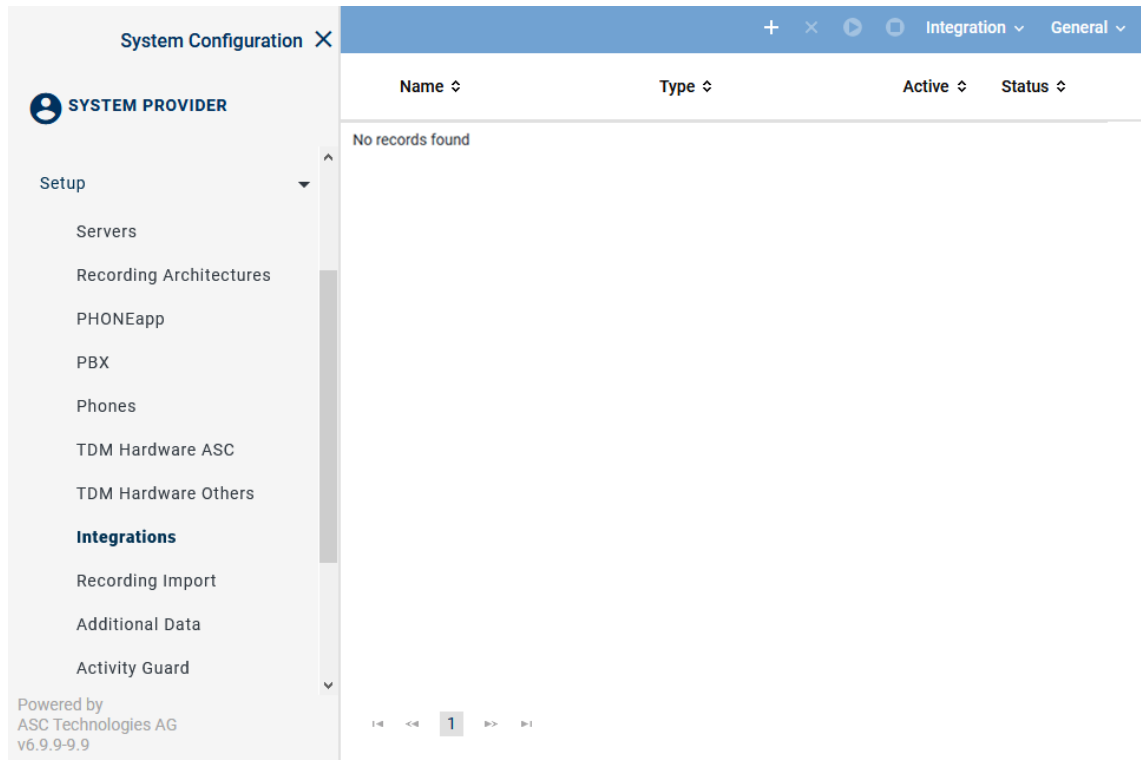




Fig. 45: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module

The toolbar offers the following functions.

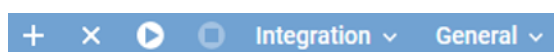







Fig. 46: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

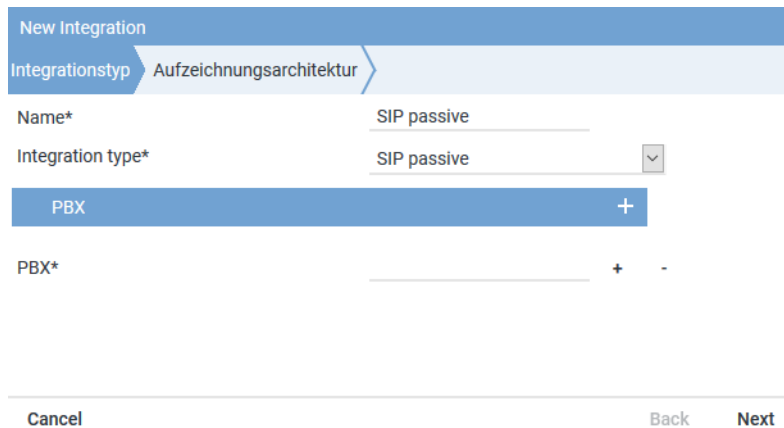



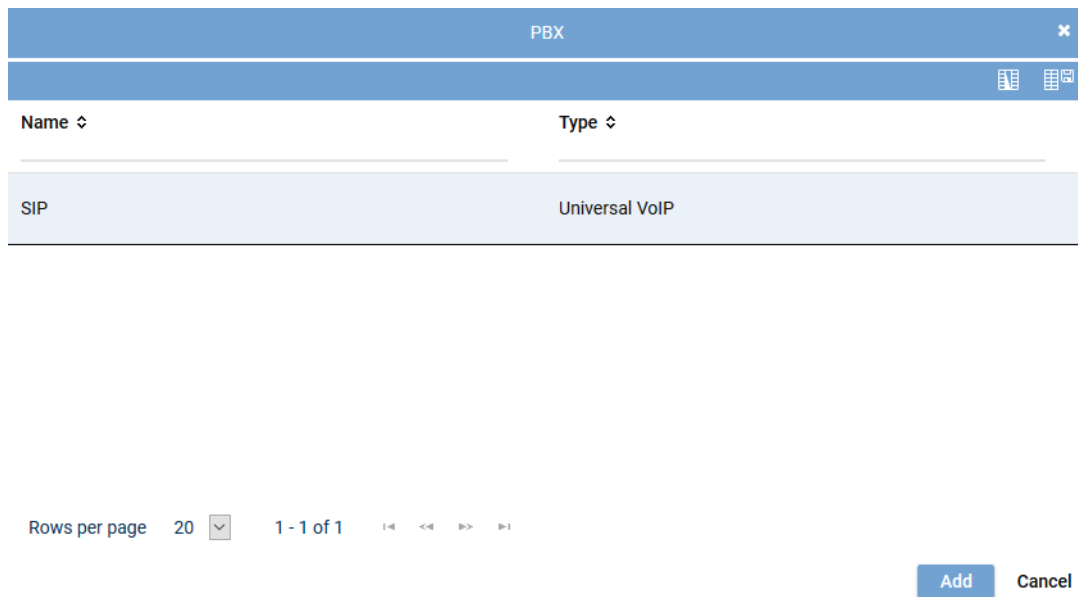
Fig. 47: Create integration type

- Enter the following parameters:

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

Tab. 12: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 48: Integrations - 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.



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Basic

Save Cancel Back Next

Fig. 49: 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:






<div> <div>SIP passive</div> <div>SIP passive</div> <div>✗</div> <div>⚙️</div> </div>	
Step	Configuration
Configure recording architecture	✓ 
Configure recording servers	✗ 
Configure add-on	✓ 
Configure miscellaneous settings	✓ 

Fig. 50: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture

Details *

Recording architecture*

All-in-one Basic

▼


Save

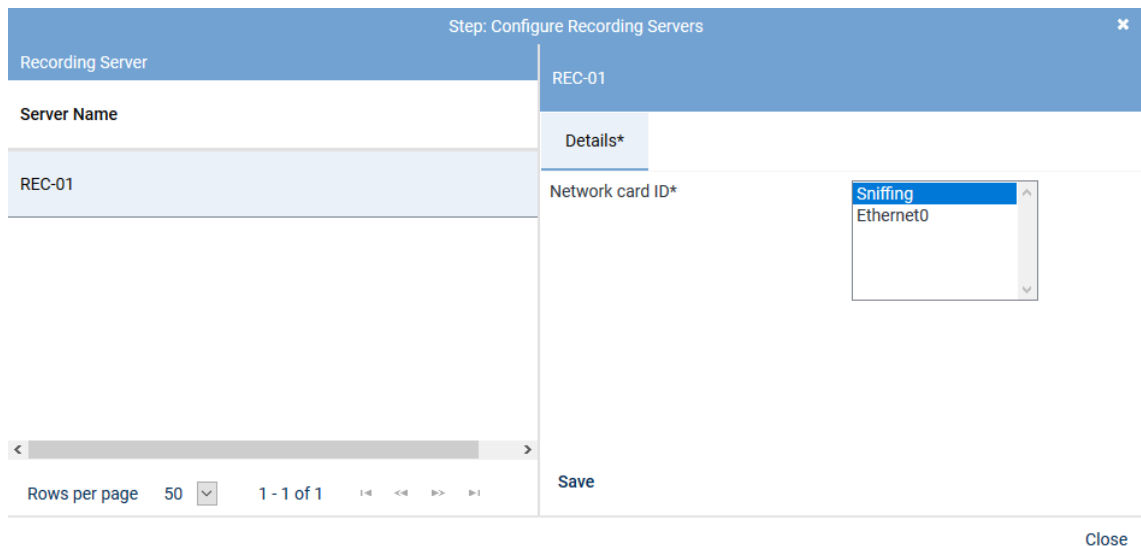
Cancel

Fig. 51: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.



Step: Configure Recording Servers

Recording Server	REC-01
Server Name	REC-01

Details*

Network card ID*

Sniffing
Ethernet0

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 52: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
Network card ID	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 13: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 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 CTIconnect 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.

CTIconnect for Genesys T-Server

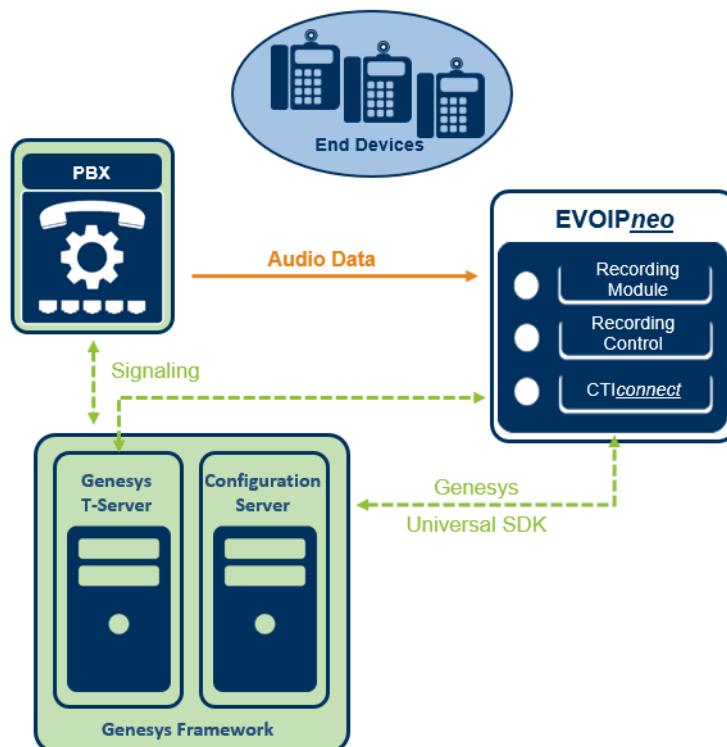


Fig. 53: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

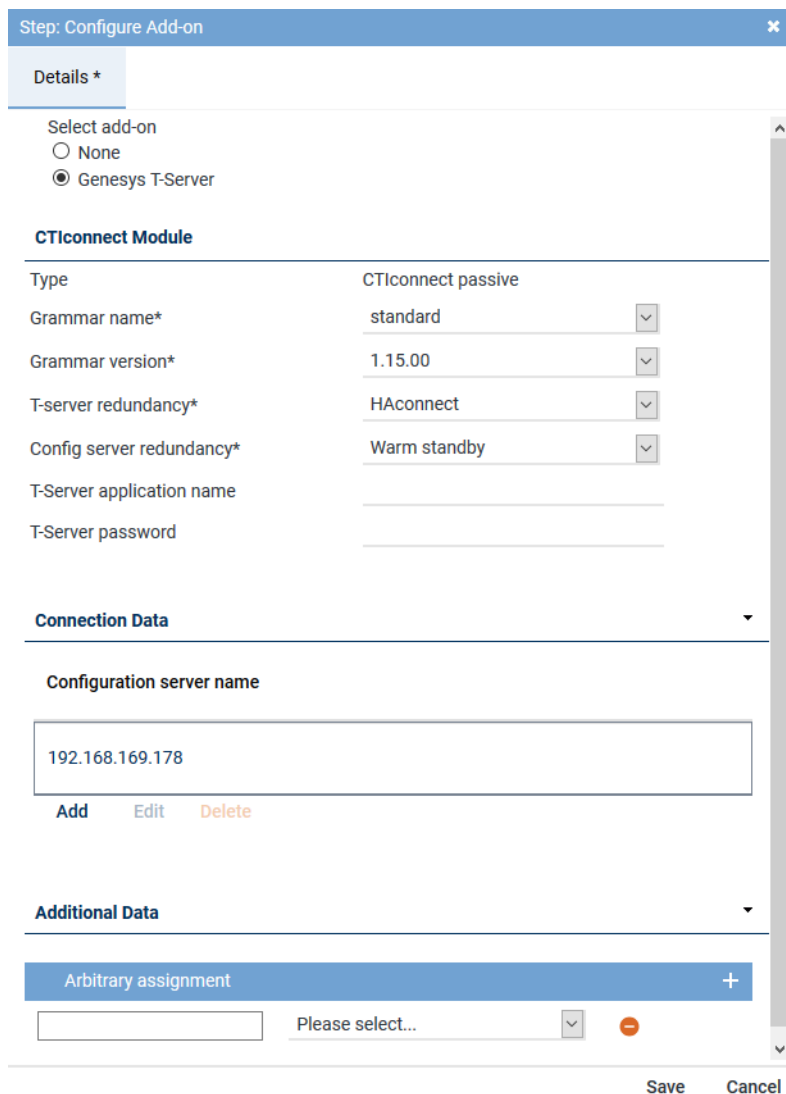
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name
192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment +

Please select...

Save Cancel

Fig. 54: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	<p>Select the redundancy which is used from the drop-down list.</p> <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	<p>From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.</p> <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 14: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 55: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 15: 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.

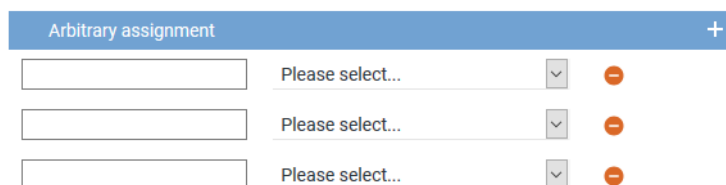



Fig. 56: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

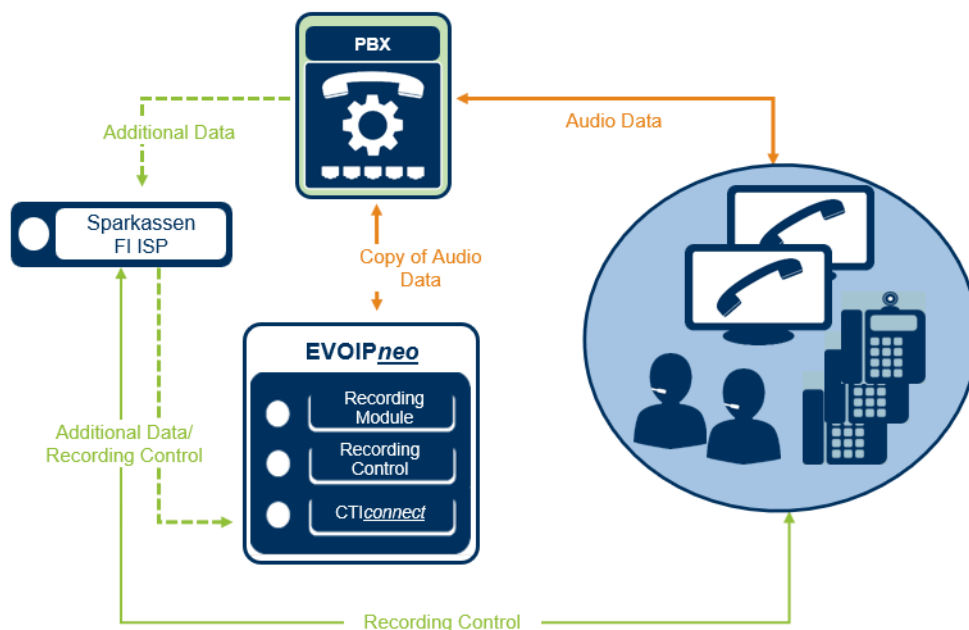



Fig. 57: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

	Please select...	▼	⊖
	Please select...	▼	⊖
	Please select...	▼	⊖

Save Cancel

Fig. 58: 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. 16: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 17: 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 CTIconnect 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.

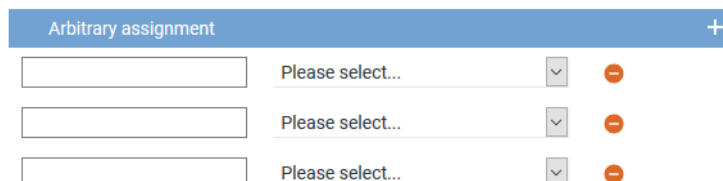



Fig. 59: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

Add Edit Delete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

Save Cancel

Fig. 60: Configure add-on for OSCC

Group field CTIconnect Module

- 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. 18: Configure CTIconnect module

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

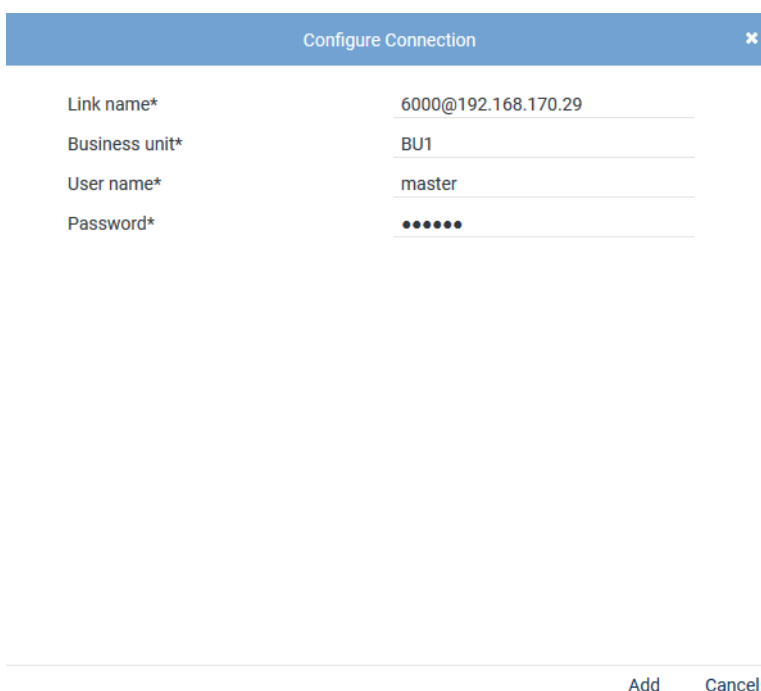


Fig. 61: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 19: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

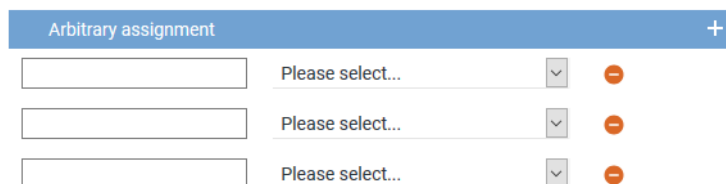





Fig. 62: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 63: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.











	SIP passive	SIP passive		
Step		Configuration		
Configure recording architecture				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 64: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✓	✓

Fig. 65: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✗	✓

Fig. 66: Deactivate integration

- 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.

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

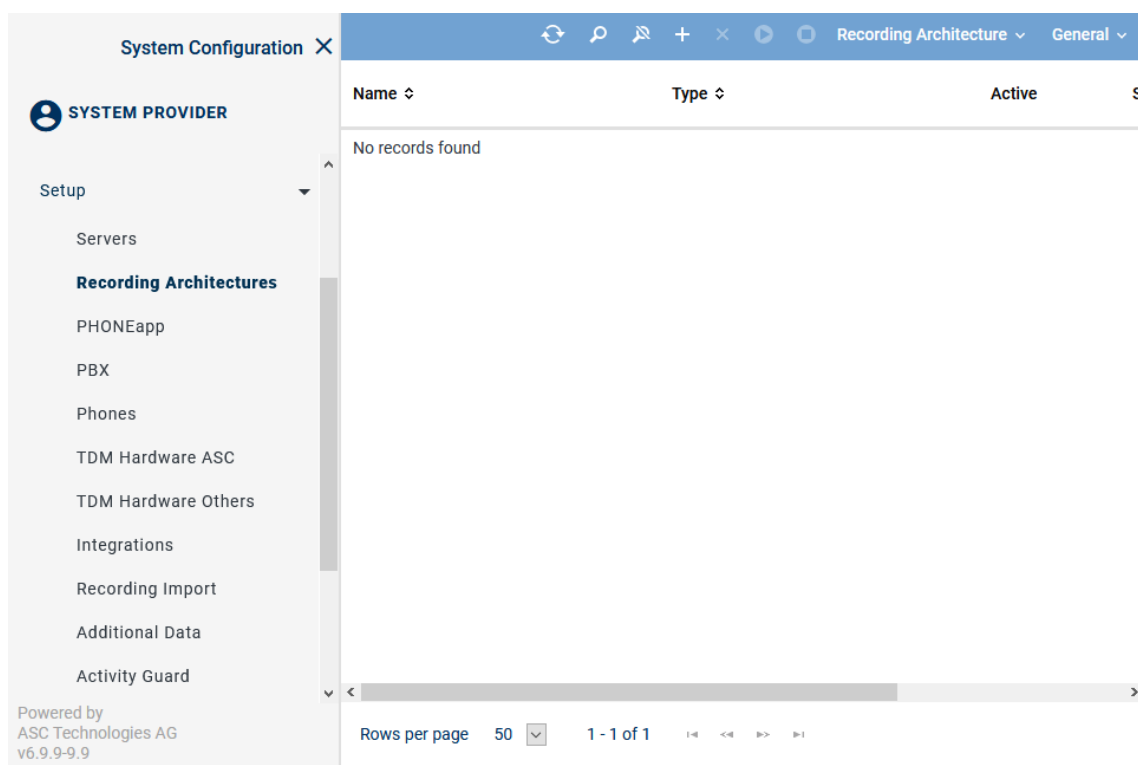




Fig. 67: Recording architectures - main view

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. <div> ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div>
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. <div> ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined. </div>
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. 68: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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*.

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

⇒ The window *New Recording Architecture* appears.

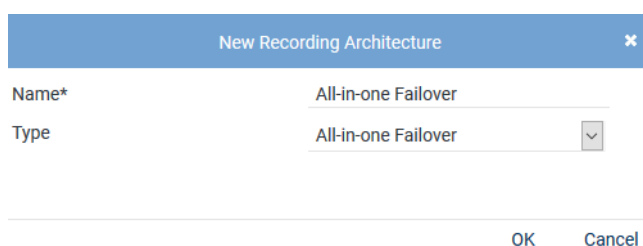



Fig. 69: Create recording architecture - All-in-one Failover

- 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.

All-in-one Failover
All-in-one Failover X

Details* Server Assignment*

 Help

Name*	All-in-one Failover
Failover timeout*	15 Sec
Recording architecture	All-in-one Failover
Standby Failover aktivieren	<input type="checkbox"/>
Active	Inactive

Integration Type
⌵ ⌶

Name
No records found

Save


Reset

Fig. 70: 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 Standby management for failover architectures.

<i>Failover timeout</i>	<p>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 <i>OK</i> within this time, then the failover process is not triggered.</p> <p>NOTICE! Check these parameters after an update and set the timeout to 15 seconds, if required.</p>
<i>Activate standby failover</i>	<p>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.</p> <p>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.</p> <p>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.</p>
<i>Active</i>	Shows the status of the recording architecture.

Add integration type

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

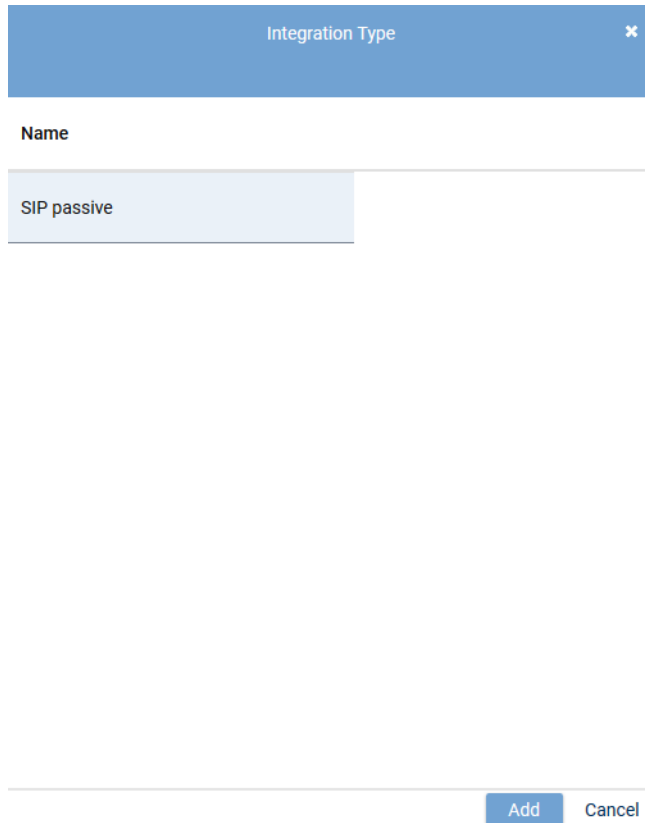


Fig. 71: Select integration type



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.

- Select *SIP passive* 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 view.

Assign server for All-in-one Failover Recording

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

All-in-one Failover
All-in-one Failover
×

Details*

Server Assignment*

Primary server*	REC-01	+	-	
Used in activated architecture	No			
Standby server*	REC-02	+	-	
Used in activated architecture	No			
Recording type	<input type="checkbox"/> VoIP/Video <input type="checkbox"/> TDM <input type="checkbox"/> Screen <input type="checkbox"/> Chat			

Save

Reset

Fig. 72: Recording Architecture - tab Server Assignment

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

Servers

Name	IP Address	Path
REC-01	192.168.173.171	C:\
REC-02	192.168.173.172	C:\

Rows per page20

1 - 8 of 8

Add

Cancel


Fig. 73: 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.

Recording type

☒ VoIP/Video

☒ TDM

☒ Screen

☒ Chat



 




Fig. 74: 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.










     Recording Architecture ▾ General ▾			
Name ▾	Type ▾	Active ▾	Standby active ▾
All-in-one Failover	All-in-one Failover		

Fig. 75: 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 Standby Management.



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:

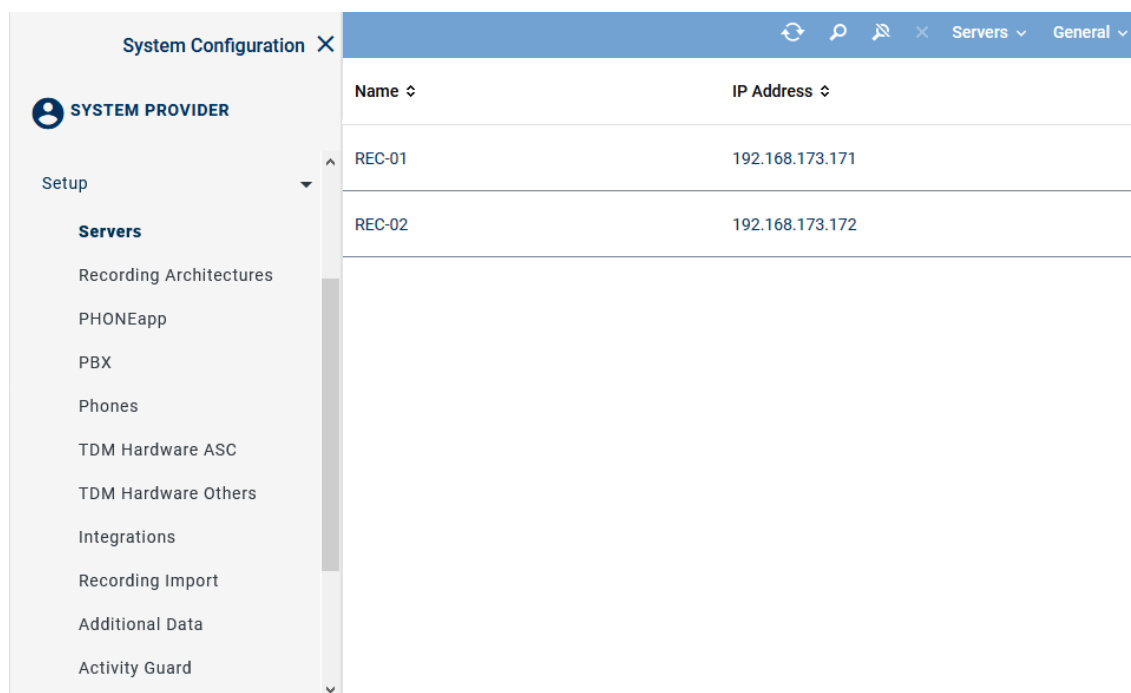


Fig. 76: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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.

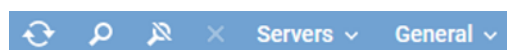








Fig. 77: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.

	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 75 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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.

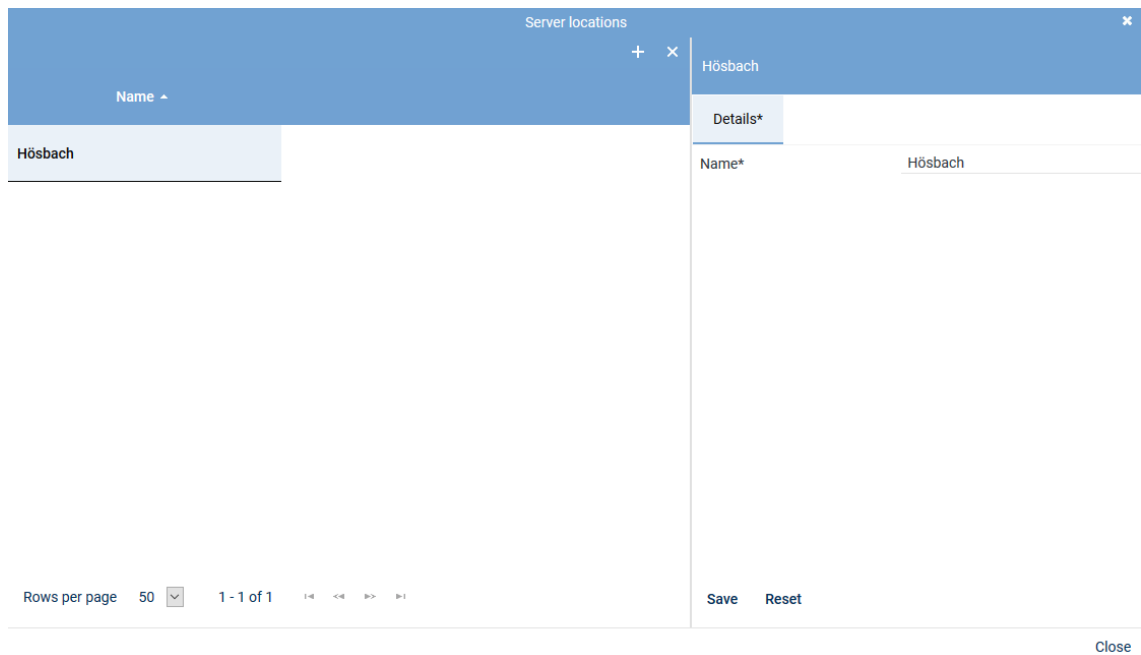



Fig. 78: Add server locations

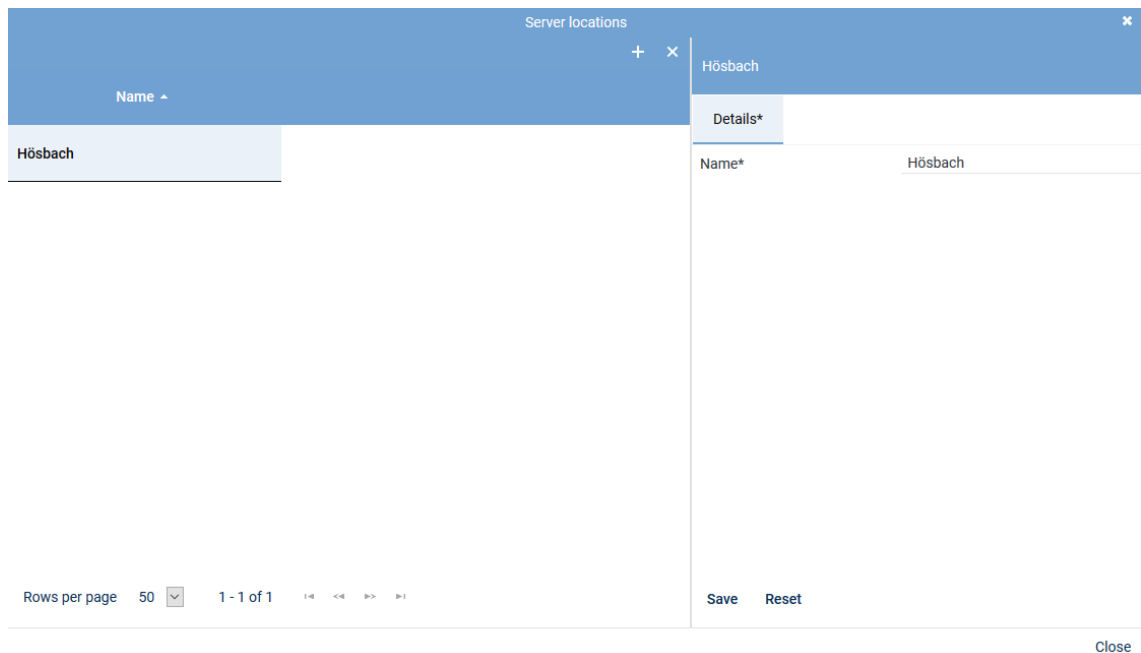
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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



Server locations

Name
Hörsbach

Details*


Name* Hörsbach

Rows per page 50 1 - 1 of 1

Save Reset

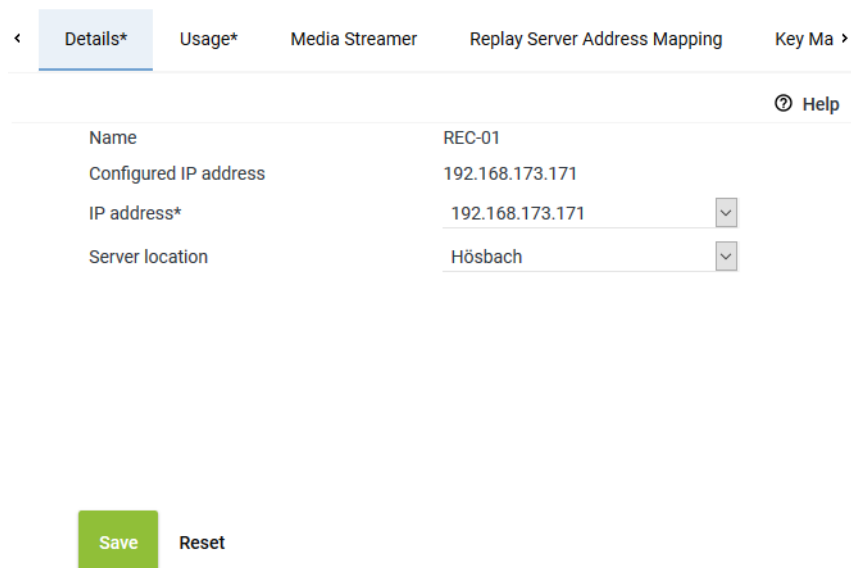
Close

Fig. 79: Delete server location

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

Tab Details

- 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.



Details* Usage* Media Streamer Replay Server Address Mapping Key Ma >

Help

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171
Server location	Hörsbach

Save Reset

Fig. 80: Servers - tab Details

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

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

Tab Usage

- 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.

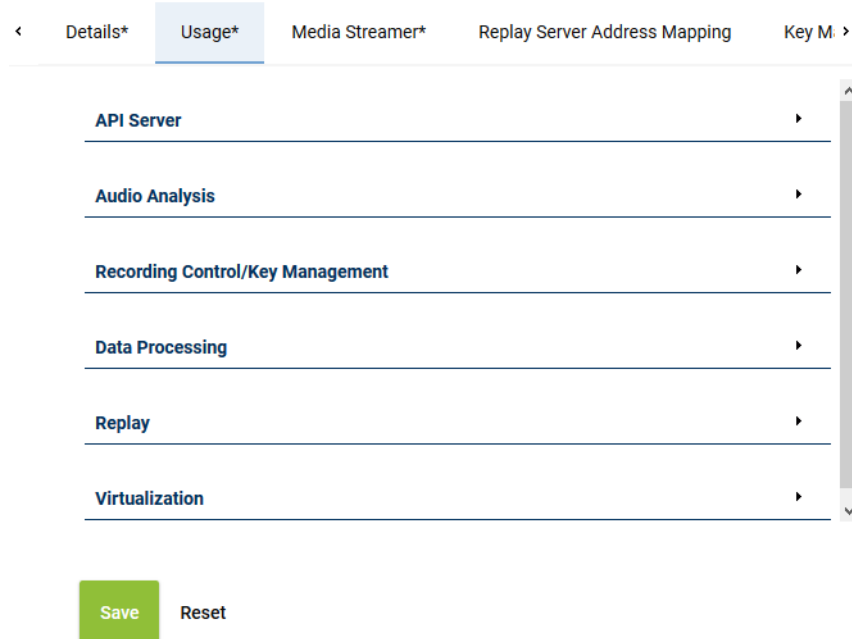


Fig. 81: Servers - tab usage

Group field API Server

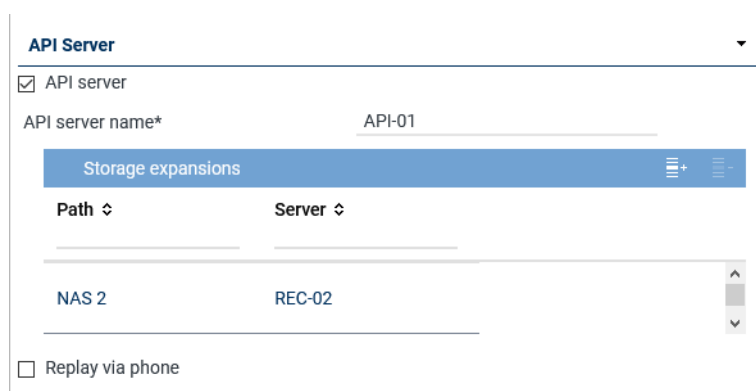




Fig. 82: Group field API Server

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
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 88.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 80. • By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list. <p>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.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 87. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.

Storage Expansion for Replay				
Device Type ↕	Name ↕	Path ↕	Free Disk Space ↕	Server ↕
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 83: 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

Audio Analysis

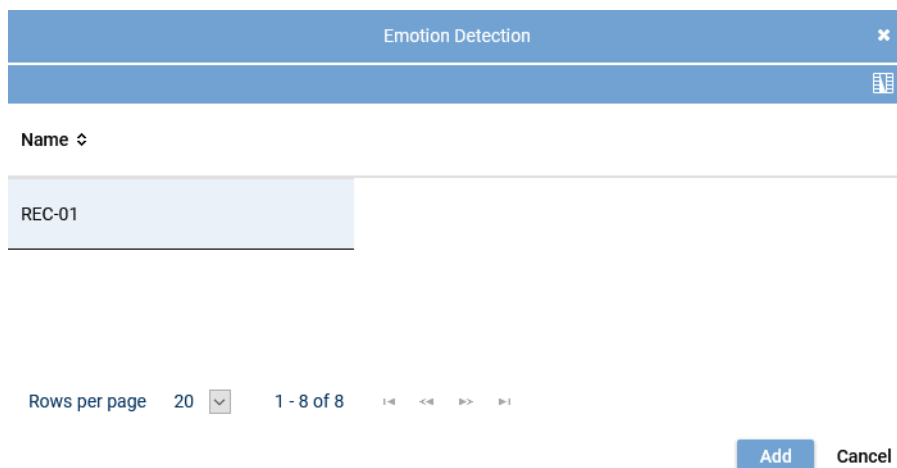
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 84: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis. <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function. <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> 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. 20: Configure audio analysis



Emotion Detection

Name ↕

REC-01

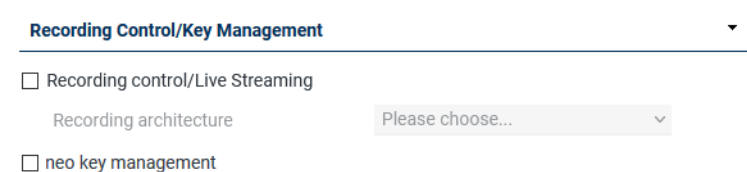
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 85: Select server for emotion detection

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

Group field Recording Control/Key Management



Recording Control/Key Management

☐ Recording control/Live Streaming

Recording architecture Please choose...

☐ neo key management

Fig. 86: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 21: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server

☒ Import

Recording architecture

Fig. 87: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 84. By clicking on the icon  (Remove), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 84. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <i>Replay server</i> 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. <p>NOTICE! For the export from Neo to Neo, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <i>Recording architecture</i> 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. 22: 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.



Name	IP Address
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173

Rows per page: 20 | 1 - 6 of 6 | Add | Cancel

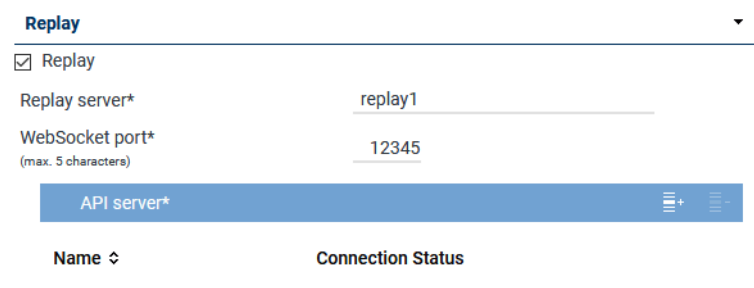
Fig. 88: Select server



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





Replay

☒ Replay

Replay server*



WebSocket port*
(max. 5 characters)

API server*  

Name	Connection Status
------	-------------------

Fig. 89: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . 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
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 85. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 23: 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. 90: Select server



Only those servers are available on which the **API** service has been installed and activated.
See [chapter "Group field API Server", p. 78](#).

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. 91: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <i>licensing.asc.de</i> If you enter this domain, there is no key management.

Parameter	Value/Description
	<ul style="list-style-type: none"> <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 24: Configure virtualization



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.

- 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

- 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*.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

PBX +

PBX	PBX <input type="text"/>
Extension* <small>(max. 18 characters)</small>	123456
Media streamer IP address*	192.168.169.192 <input type="text"/>
Minimum port	24000
Maximum port	24099
Transport protocol	UDP <input type="text"/>
SIP signaling port	5062
User name	<input type="text"/>
Password	<input type="text"/>
PBX IP address	<input type="text"/>
PBX port	5060
Registration required	<input checked="" type="checkbox"/>
SIP registration expiration	3600 Second(s)

Save

Reset

Fig. 92: Servers module - tab Media Streamer

- 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.
------------	--

	<p>If no PBX has been created in the system yet, you can create a PBX via the blue bar <i>PBX</i>, see chapter "Create PBX", p. 93.</p>
<i>Extension</i>	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

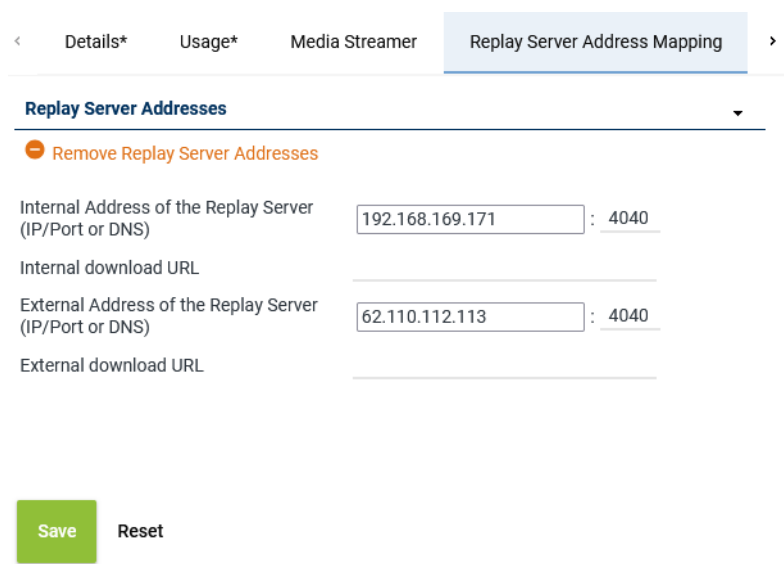



Fig. 93: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

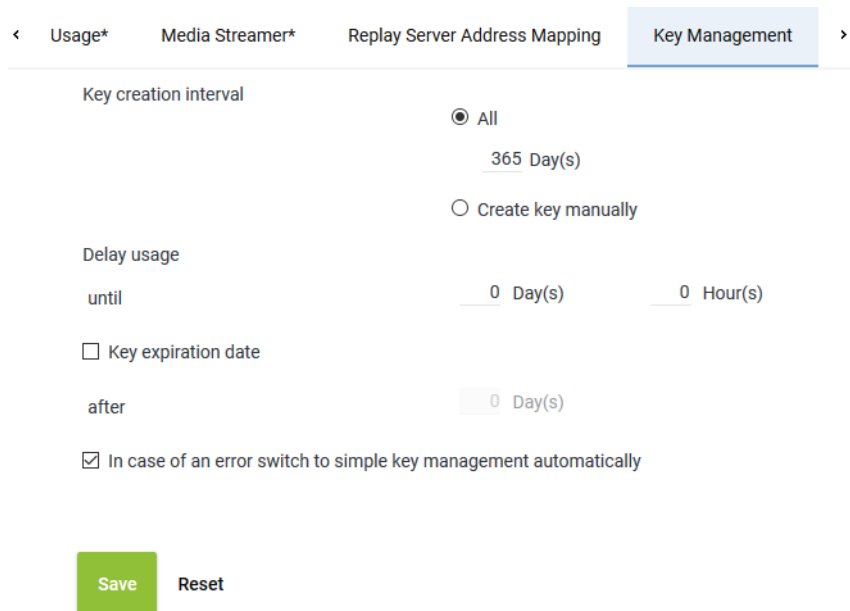


Fig. 94: Servers module - tab Key Management

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.

<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p> <p>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo key management does not work (e. g. if the service <i>DongleMan</i> 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.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = 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 <i>Usage</i>.</p>



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*

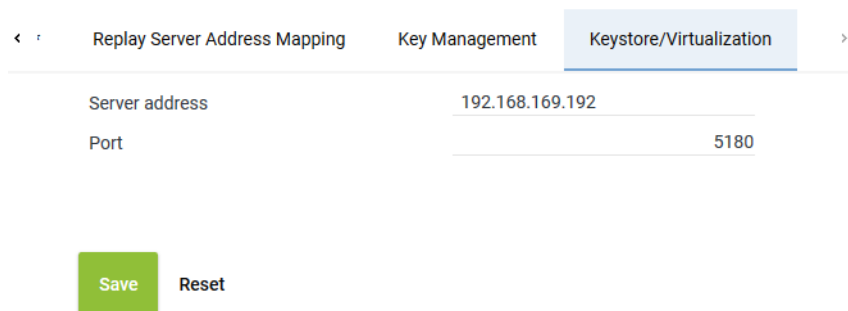
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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.



The screenshot shows a web interface for configuring the Servers module, specifically the 'Keystore/Virtualization' tab. The interface has a top navigation bar with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is selected and highlighted. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom of the form, there are two buttons: a green 'Save' button and a grey 'Reset' button.

Fig. 95: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management:
-----------------------	--

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	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*.

- 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.

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

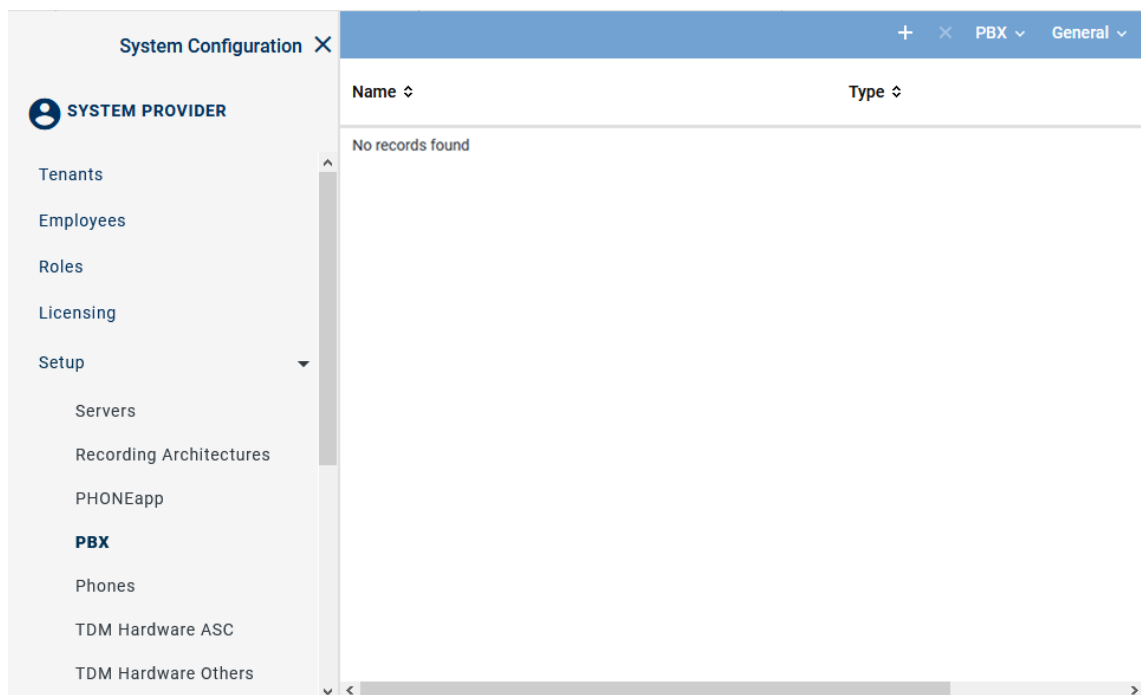


Fig. 96: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

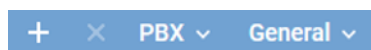




Fig. 97: Toolbar PBX module


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

<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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.

SIP
×

< Details* PHONEapp Configuration Web Service >

Name*

PBX type

Maximum length of extensions

Country code ☒ Select from list

☐ Enter manually

Area code*

Net code*

Non Phone IPs

No records found
Add Delete

IPs to be Ignored

No records found
Add Delete

MACs to be Ignored

No records found
Add Delete

Save

Reset

Fig. 98: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This <i>name</i> 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: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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. 25: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.

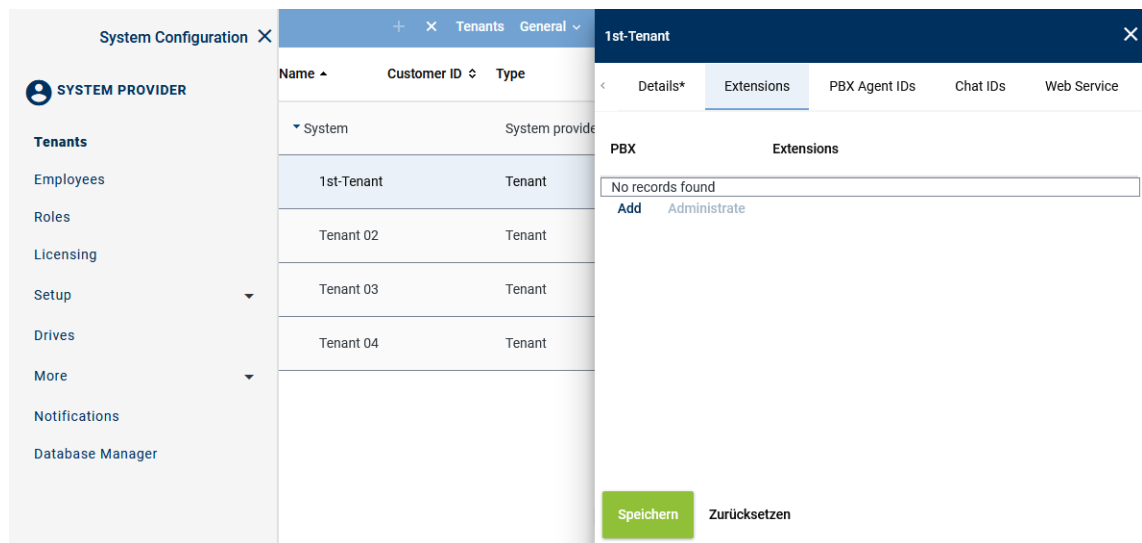


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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.



Name	Customer ID	Type
System		System provider
1st-Tenant		Tenant
Tenant 02		Tenant
Tenant 03		Tenant
Tenant 04		Tenant

1st-Tenant

Details* Extensions PBX Agent IDs Chat IDs Web Service

PBX Extensions

No records found

Add Administrate

Speichern Zurücksetzen

Fig. 99: 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:

Add Extensions ✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

Extension or extension range separated by
", " or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 100: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> ZIP TXT CSV <p>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.</p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

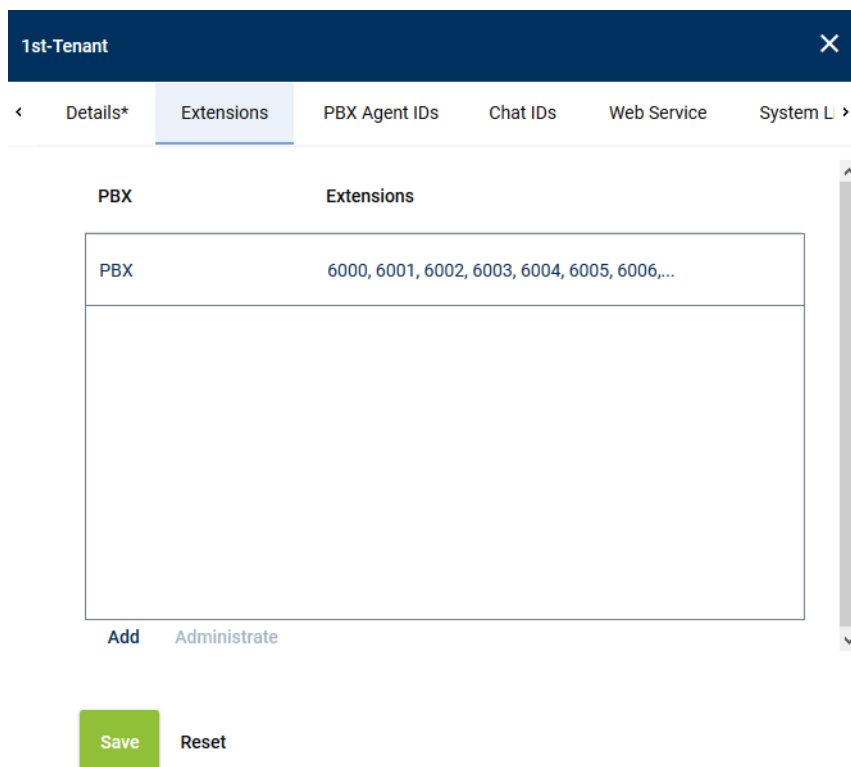
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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 detected, 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.



The screenshot shows a web interface for configuring extensions. At the top, there's a header '1st-Tenant' with a close button. Below it is a navigation bar with tabs: 'Details*', 'Extensions' (selected), 'PBX Agent IDs', 'Chat IDs', 'Web Service', and 'System L'. The main content area has a table with two columns: 'PBX' and 'Extensions'. The 'PBX' column has a single entry 'PBX'. The 'Extensions' column has a single entry '6000, 6001, 6002, 6003, 6004, 6005, 6006,...'. Below the table, there are two buttons: 'Add' and 'Administrate'. At the bottom of the interface, there are two buttons: 'Save' and 'Reset'.

Fig. 101: Remove extensions

2. Click the button *Administrate*.

- 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. 102: Select extensions

- To remove the selected extensions, 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.

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

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

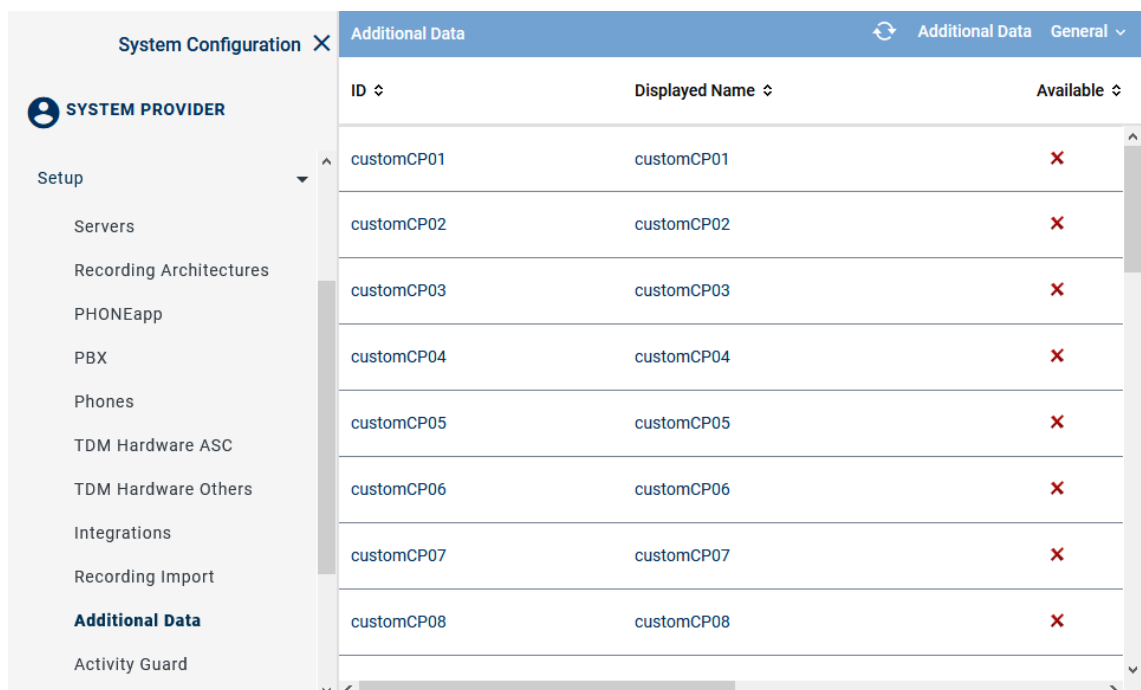


Fig. 103: Additional Data module main view

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

Change display name






Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	

Fig. 104: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 105: 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:

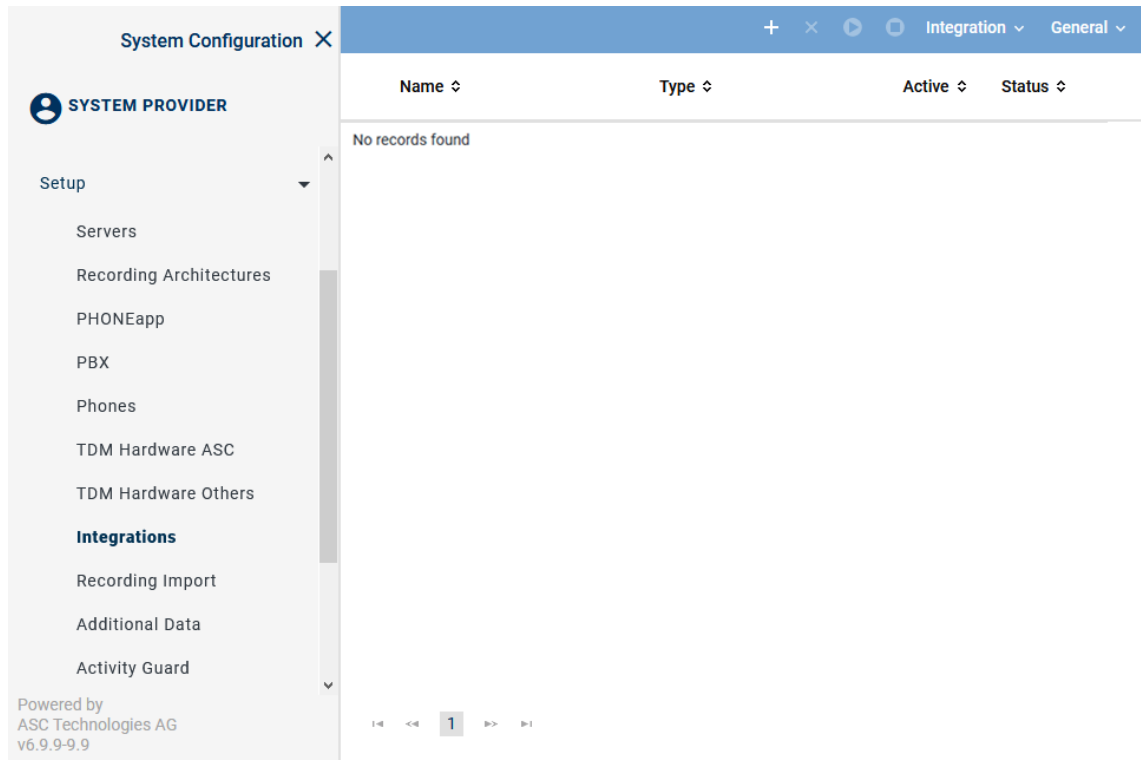




Fig. 106: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module


The toolbar offers the following functions.



Fig. 107: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

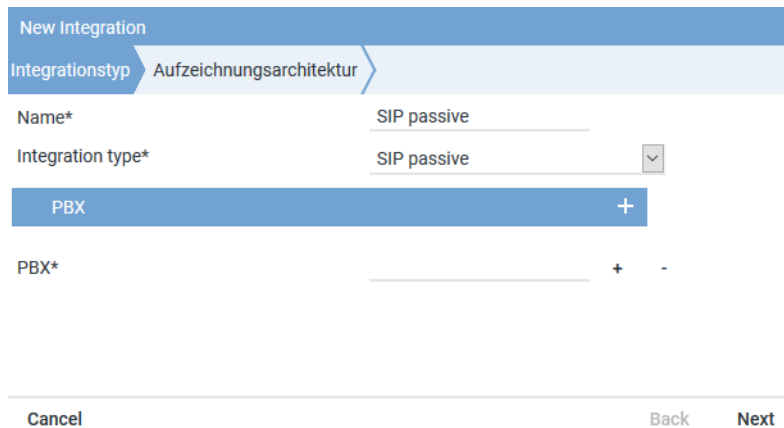



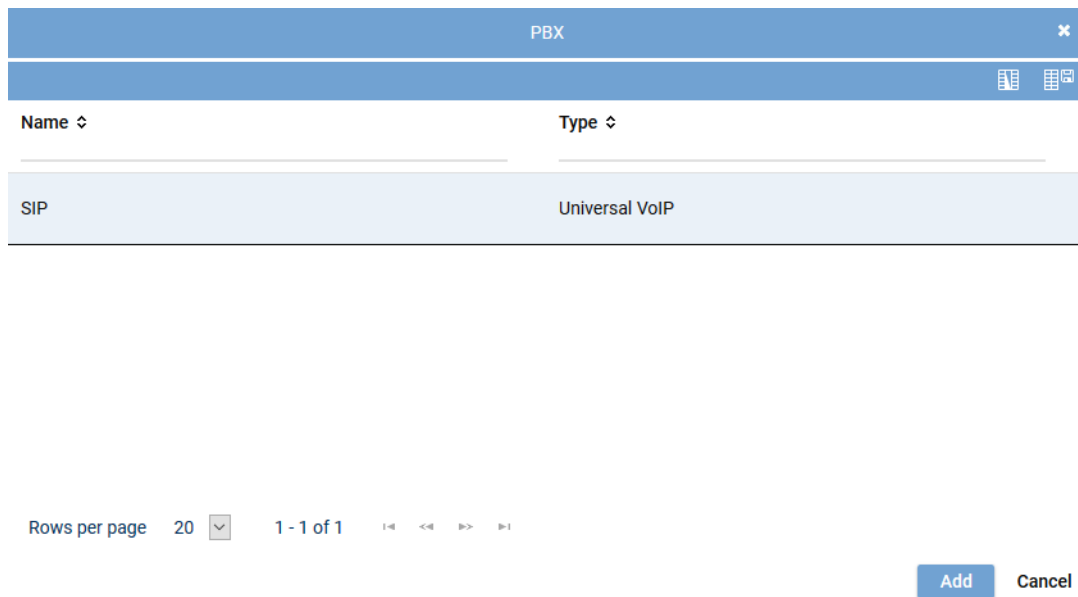
Fig. 108: Create integration type

- Enter the following parameters:

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

Tab. 26: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

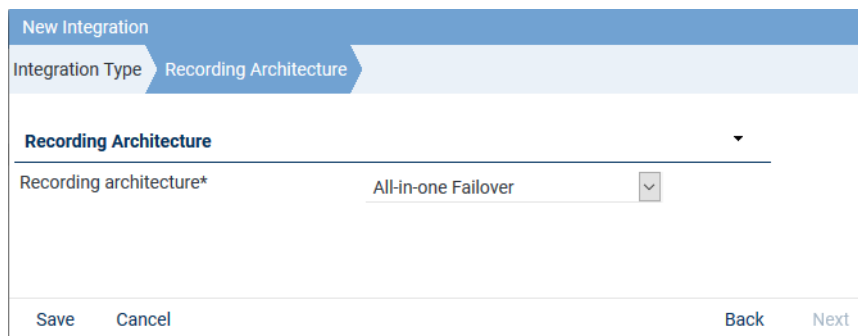
Add Cancel

Fig. 109: Integrations - 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.



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Failover

Save Cancel Back Next

Fig. 110: 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:







SIP passive		SIP passive	X	
Step	Configuration			
Configure recording architecture	✓ 			
Configure recording servers	X 			
Configure add-on	✓ 			
Configure miscellaneous settings	✓ 			

Fig. 111: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture

Details *


Recording architecture*
All-in-one Failover

Save Cancel

Fig. 112: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.

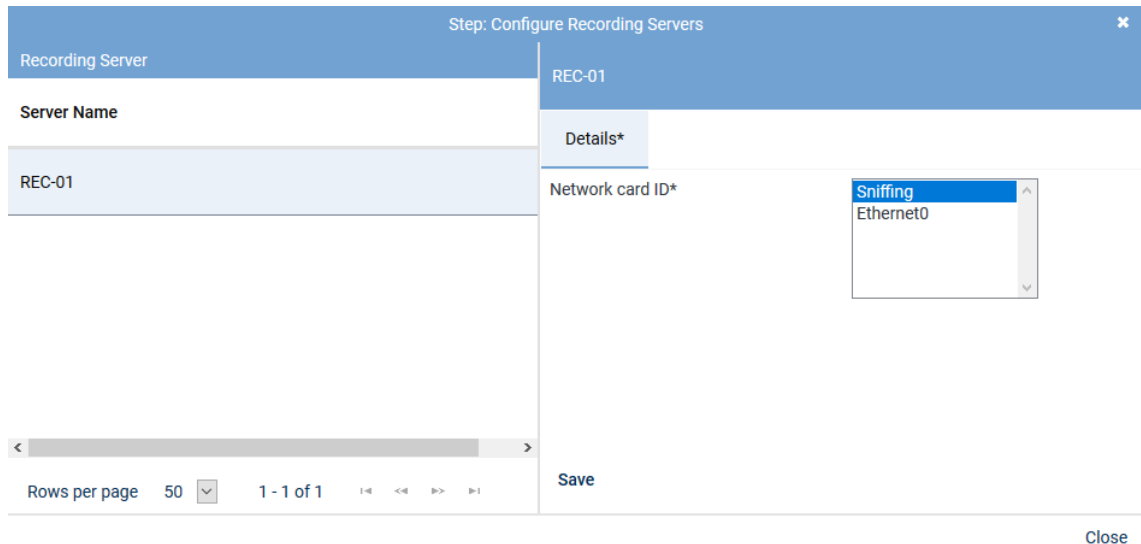


Fig. 113: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
<i>Network card ID</i>	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 27: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 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 CTIconnect 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.

CTIconnect for Genesys T-Server

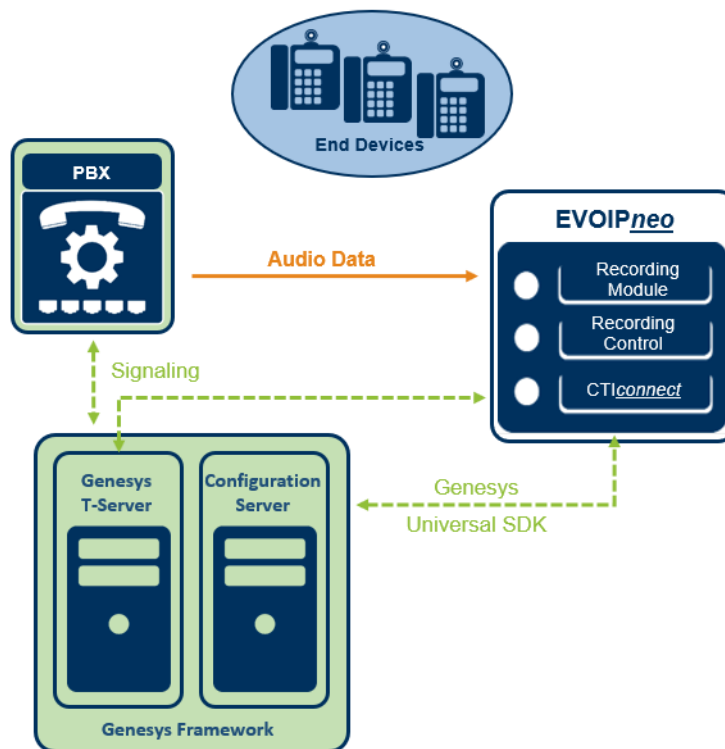


Fig. 114: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

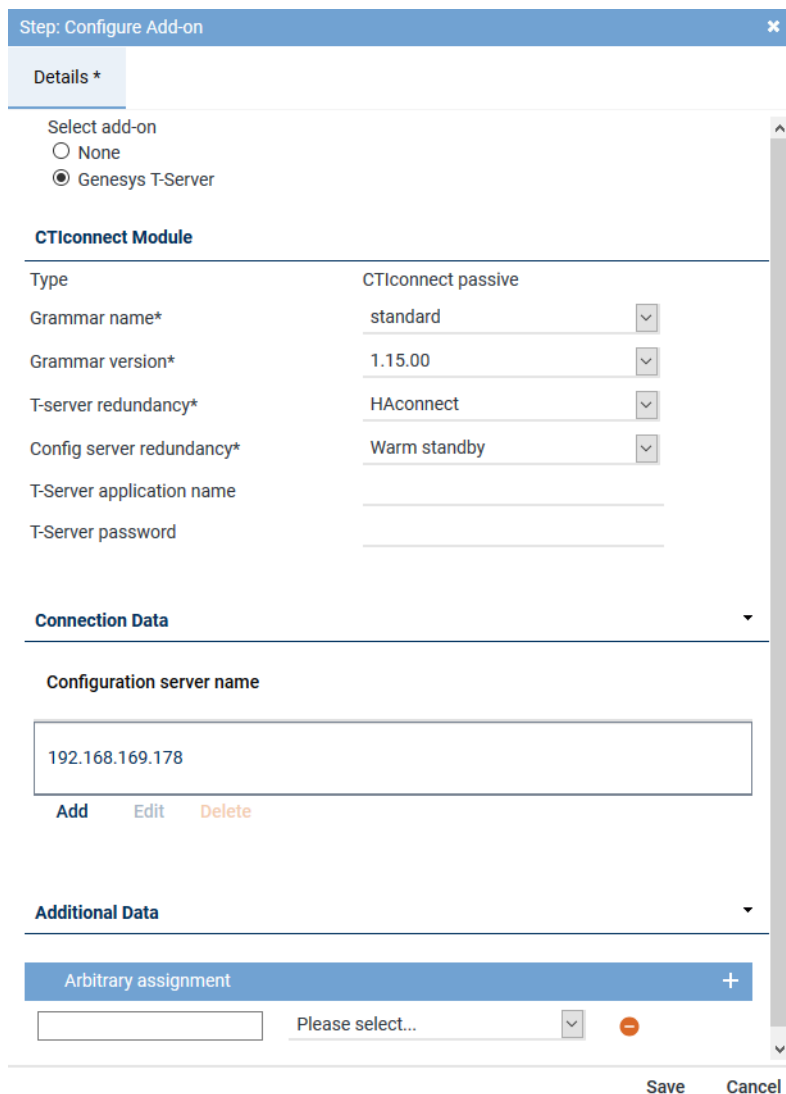
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name

192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment

Please select...

Save Cancel

Fig. 115: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	<p>Select the redundancy which is used from the drop-down list.</p> <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	<p>From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.</p> <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 28: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 116: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 29: 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.

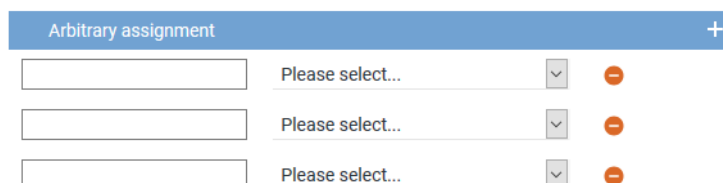



Fig. 117: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

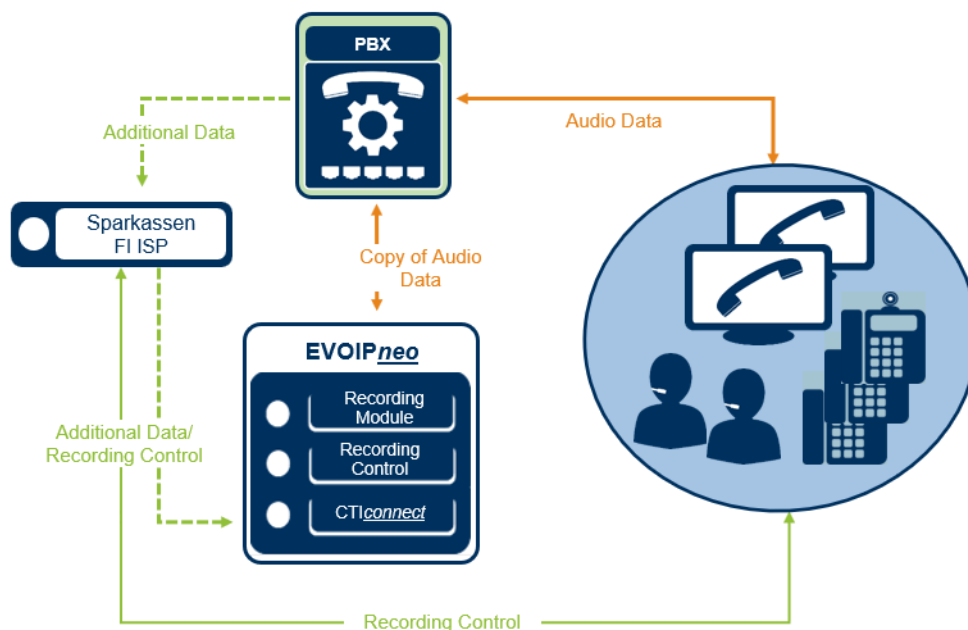



Fig. 118: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

<input style="width: 90%;" type="text"/>	Please select...	▼	⊖
<input style="width: 90%;" type="text"/>	Please select...	▼	⊖
<input style="width: 90%;" type="text"/>	Please select...	▼	⊖

Save Cancel

Fig. 119: Configure add-on for Sparkassen FI ISP

Group field CTIconnect Module

- 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. 30: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 31: 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 CTIconnect 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.

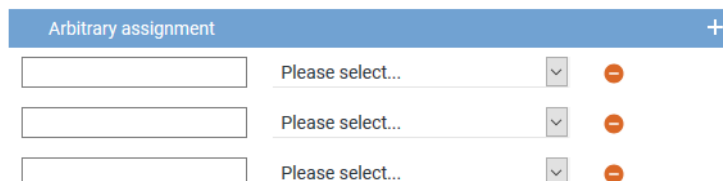



Fig. 120: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

Add Edit Delete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

Save Cancel

Fig. 121: Configure add-on for OSCC

Group field CTIconnect Module

- 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

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

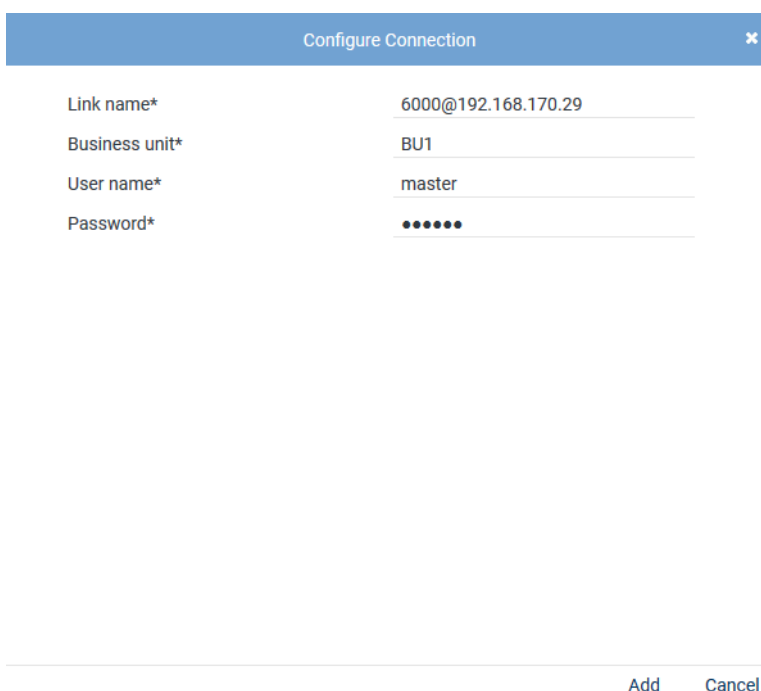


Fig. 122: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 33: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

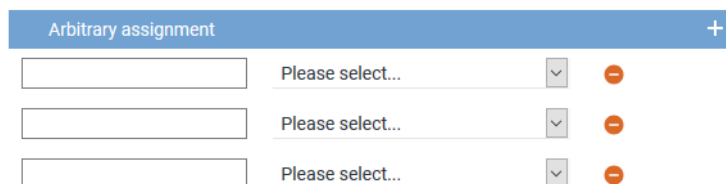





Fig. 123: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 124: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.













	SIP passive	SIP passive		
Step		Configuration		
Configure recording architecture				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 125: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✓	✓

Fig. 126: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✗	✓

Fig. 127: Deactivate integration

- 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.

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

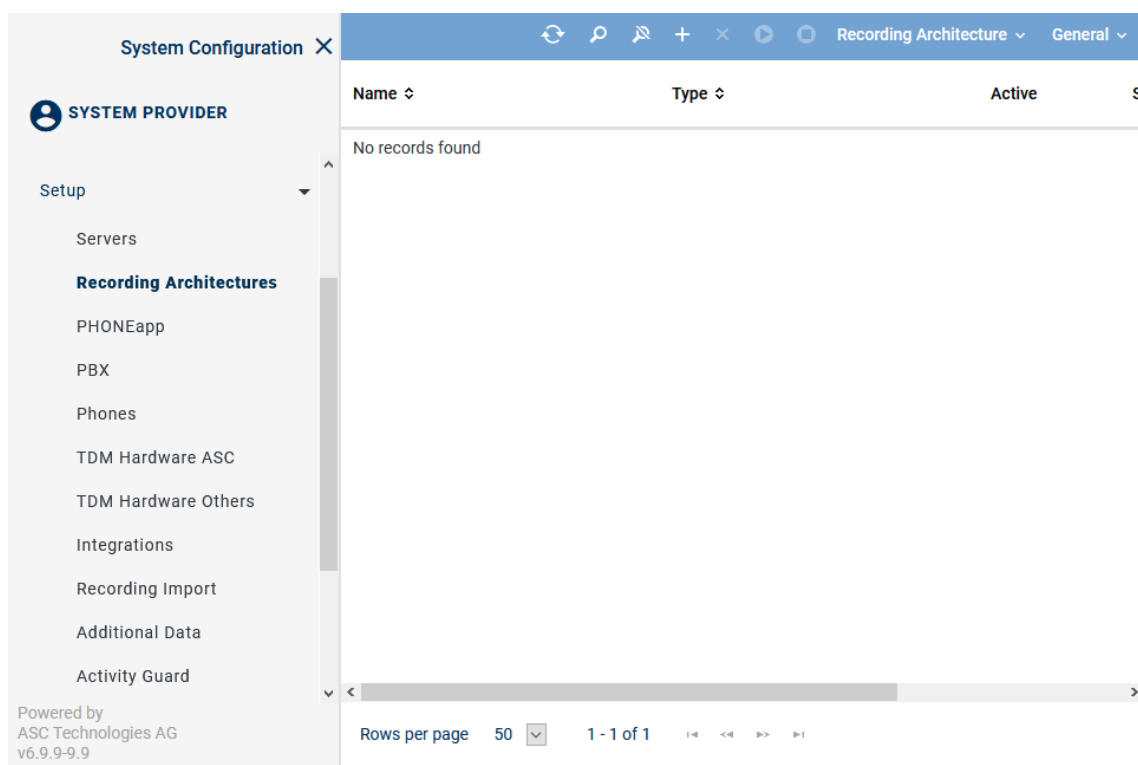




Fig. 128: Recording architectures - main view

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. <div> ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div>
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. <div> ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined. </div>
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. 129: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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*.

- 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. 130: Create recording architecture - All-in-one Parallel Recording

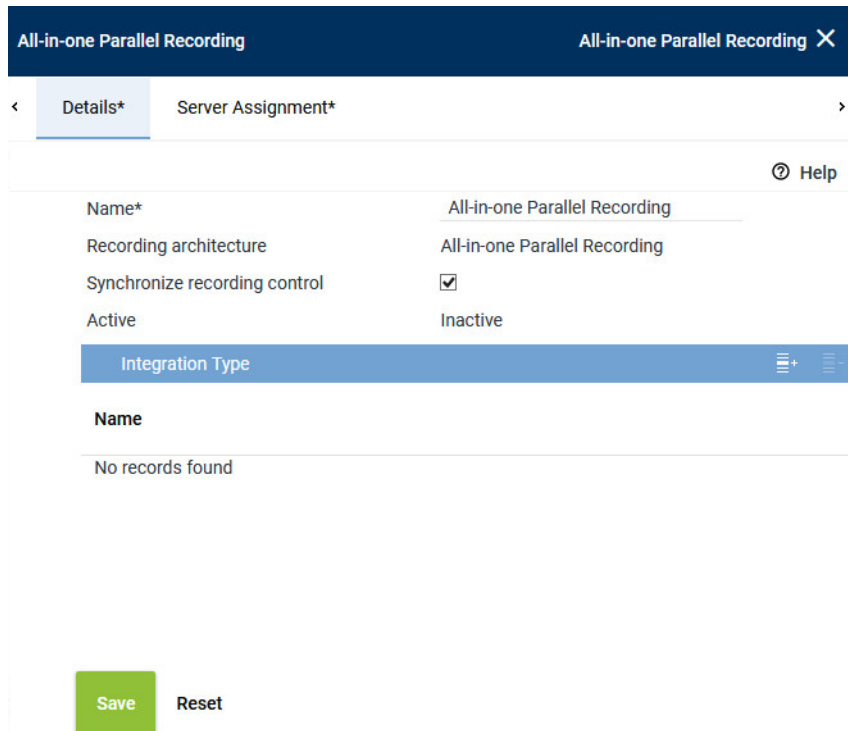
- In the entry field *Name*, enter a descriptive name for the recording architecture.

- 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.

- Click on the button *OK*.

⇒ Your entries now appear in the detail view.



The screenshot shows a configuration window titled 'All-in-one Parallel Recording'. It has two tabs: 'Details*' (selected) and 'Server Assignment*'. In the 'Details*' tab, there are four fields: 'Name*' with the value 'All-in-one Parallel Recording', 'Recording architecture' with the value 'All-in-one Parallel Recording', 'Synchronize recording control' with a checked checkbox, and 'Active' with the value 'Inactive'. Below these fields is a section titled 'Integration Type' which contains a table with one column 'Name'. The table is empty, and a message 'No records found' is displayed below it. At the bottom of the window are two buttons: 'Save' (green) and 'Reset' (grey).


Fig. 131: Recording architecture - tab Details - All-in-one Parallel Recording

- 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 Synchronization recording control.

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 method 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 Duplicates in parallel recording architectures.

Add integration type

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

Integration Type

×

Name

SIP passive

Add

Cancel

Fig. 132: Select integration type



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

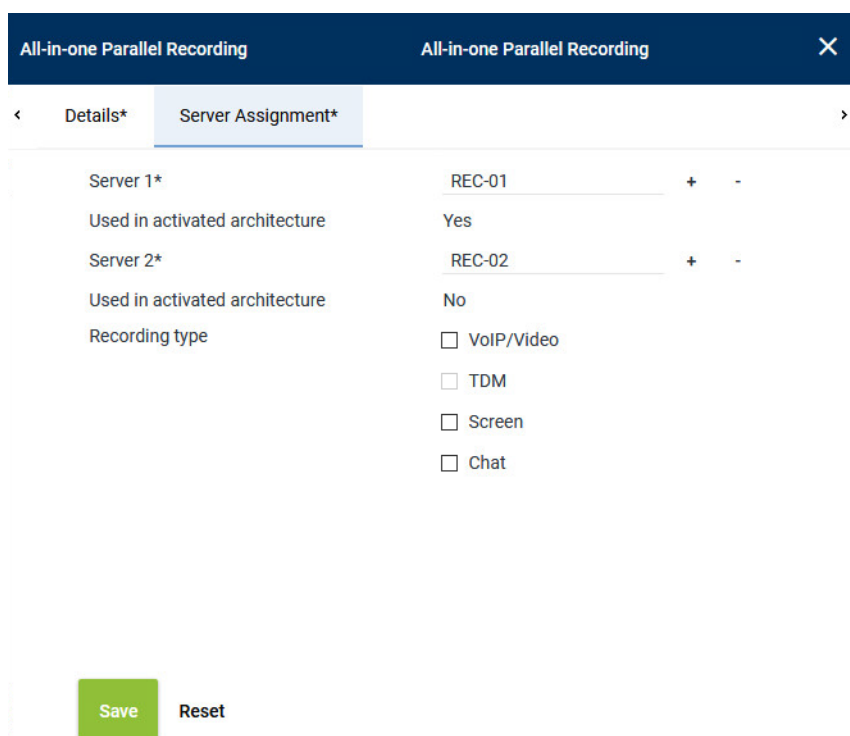


Any number of integration types can be assigned to a recording architecture.

2. Select *SIP passive* 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 view.

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*.



All-in-one Parallel Recording		All-in-one Parallel Recording	
<div> <div>Details*</div> <div>Server Assignment*</div> </div>			
Server 1*	REC-01	+	-
Used in activated architecture	Yes		
Server 2*	REC-02	+	-
Used in activated architecture	No		
Recording type	<input type="checkbox"/> VoIP/Video <input type="checkbox"/> TDM <input type="checkbox"/> Screen <input type="checkbox"/> Chat		
<div> <div>Save</div> <div>Reset</div> </div>			

Fig. 133: Recording Architecture - tab Server Assignment

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



Servers		
Name ↕	IP Address ↕	Path ↕
REC-01	192.168.173.171	C:\
REC-02	192.168.173.172	C:\

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 134: Recording Architecture - assign server - example


- 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.

- 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.

Recording type

☒ VoIP/Video

☒ TDM

☒ Screen

☒ Chat




Fig. 135: 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 tool-bar becomes active.
3. To activate the recording architecture, click on the icon  (*Activate*).
⇒ In the column *Active*, the icon  (*Active*) appears.










     General ▾			
Name ▾	Type ▾	Active	Standby active ▾
All-in-one Parallel Recording	All-in-one Parallel Recording		

Fig. 136: 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 [Configure duplicate detection](#).



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:

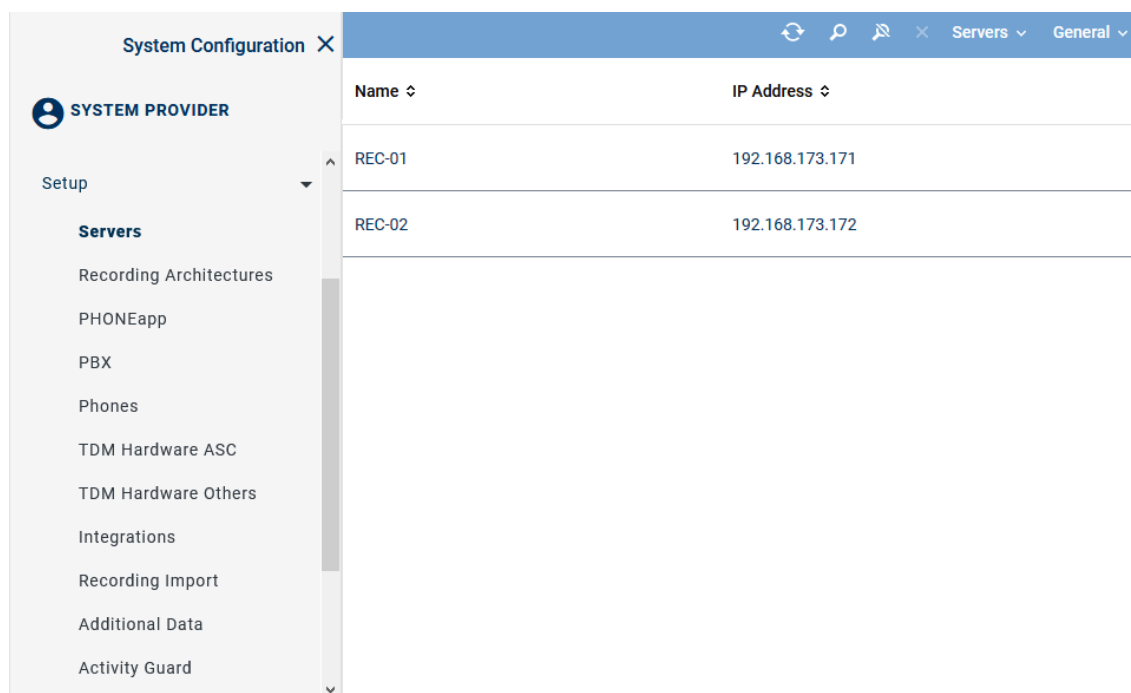


Fig. 137: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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.

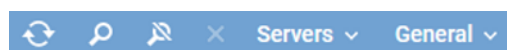








Fig. 138: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.

	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 128 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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.

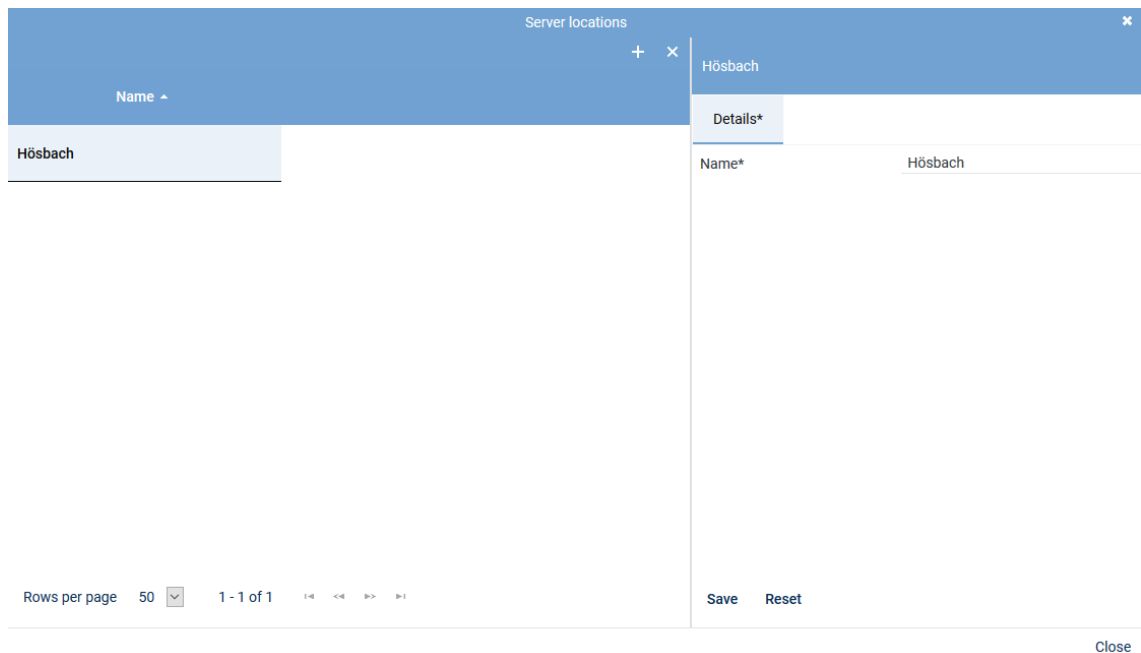



Fig. 139: Add server locations

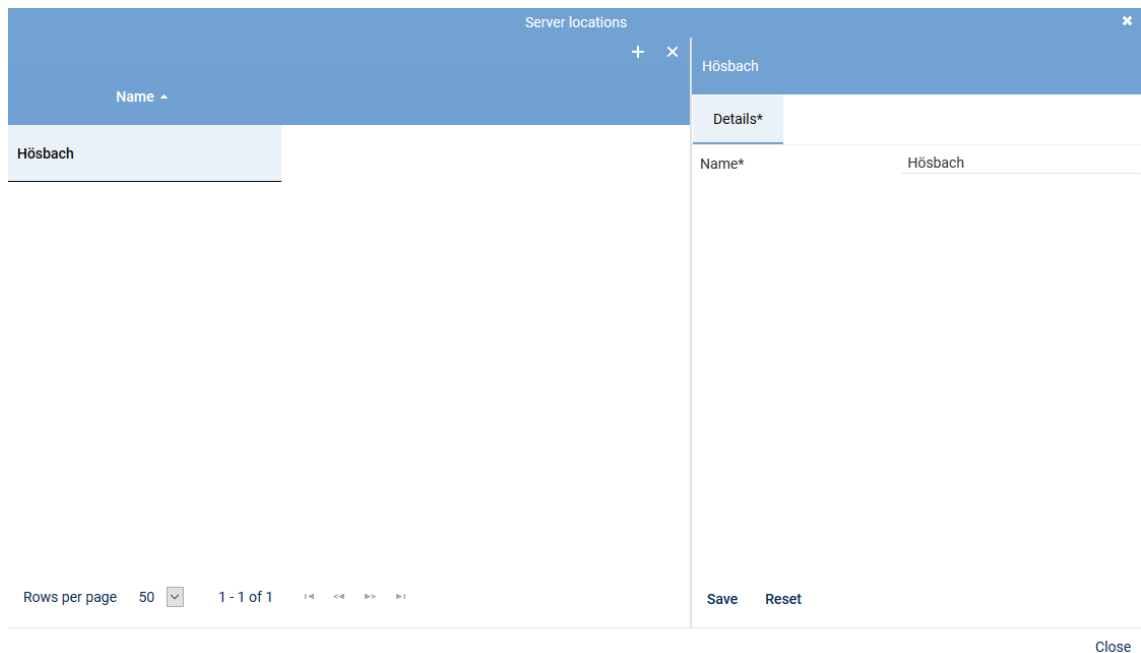
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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



Server locations

Name
Hörsbach

Details*


Name* Hörsbach

Rows per page 50 1 - 1 of 1

Save Reset

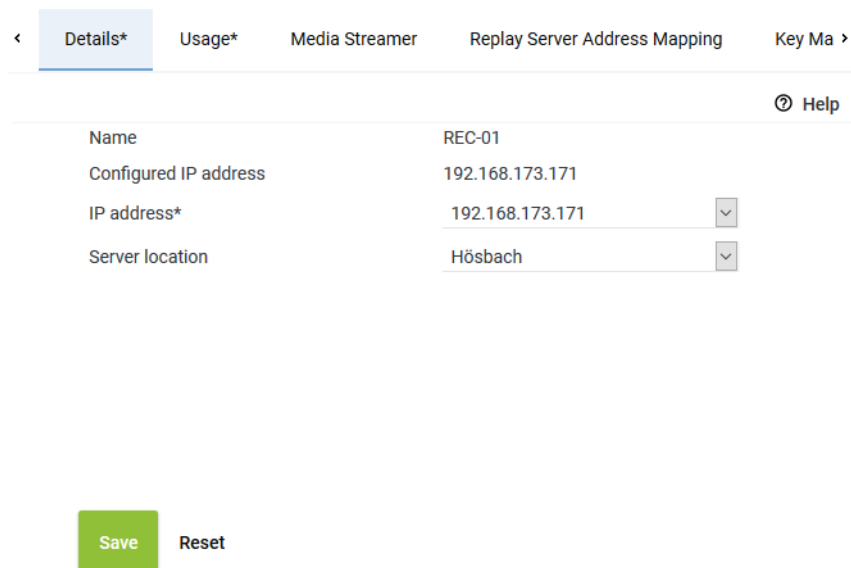
Close

Fig. 140: Delete server location

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

Tab Details

- 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.



Details* Usage* Media Streamer Replay Server Address Mapping Key Ma >

Help

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171
Server location	Hörsbach

Save Reset

Fig. 141: Servers - tab Details

- From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
- 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.

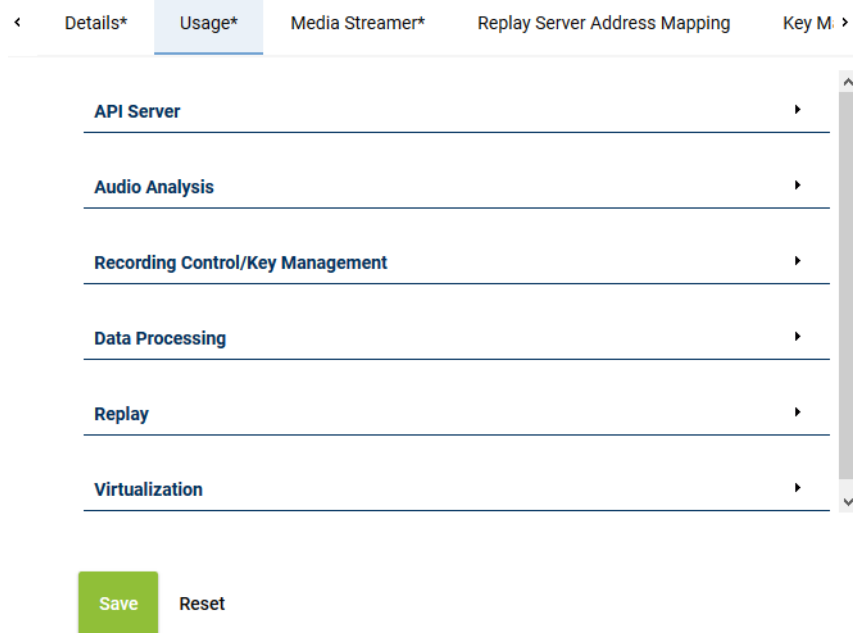


Fig. 142: Servers - tab usage

Group field API Server

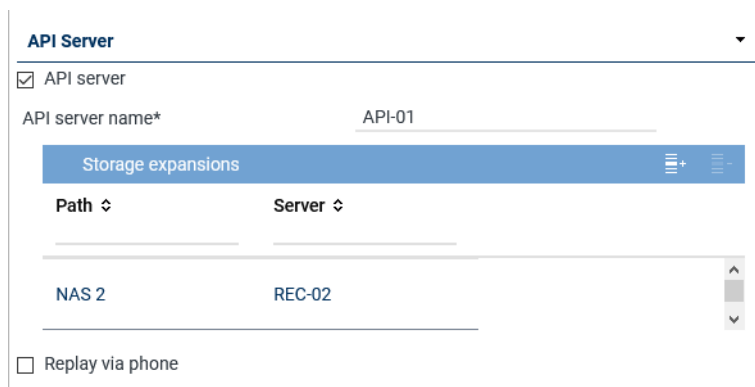




Fig. 143: Group field API Server

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
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 141.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 133. • By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list. <p>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.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 140. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.

Storage Expansion for Replay				
Device Type	Name	Path	Free Disk Space	Server
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 144: 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

Audio Analysis

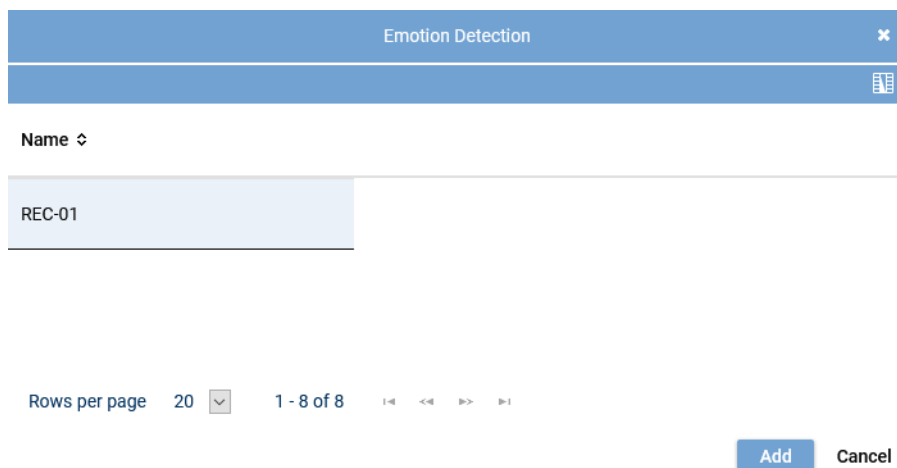
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 145: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis. <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function. <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> 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. 34: Configure audio analysis



Emotion Detection

Name ↕

REC-01

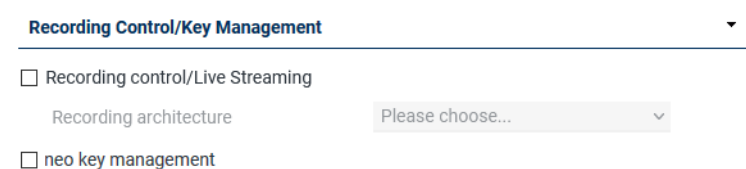
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 146: Select server for emotion detection

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

Group field Recording Control/Key Management



Recording Control/Key Management

☐ Recording control/Live Streaming

Recording architecture Please choose...

☐ neo key management

Fig. 147: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 35: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server

☒ Import

Recording architecture

Fig. 148: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 137. By clicking on the icon  (Remove), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

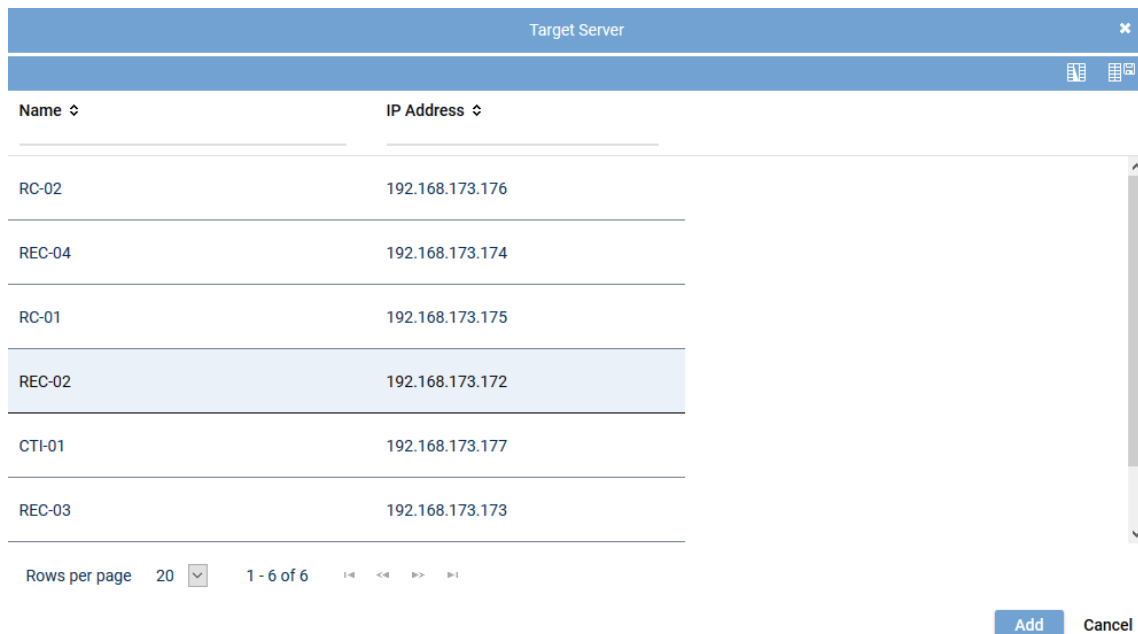
Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 137. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <i>Replay server</i> 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. <p>NOTICE! For the export from Neo to Neo, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <i>Recording architecture</i> 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. 36: 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.



Name	IP Address
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173

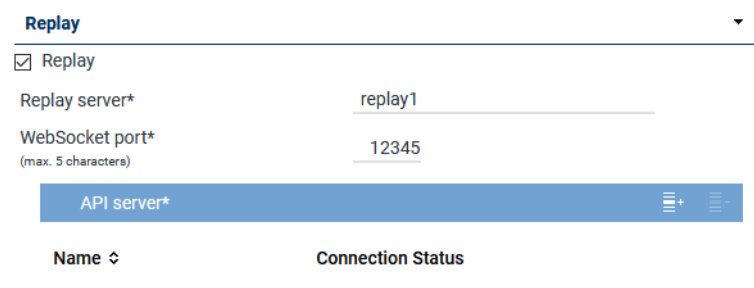
Fig. 149: Select server



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





Replay

☒ Replay

Replay server*



WebSocket port*
(max. 5 characters)

API server*  

Name	Connection Status
------	-------------------

Fig. 150: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . 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
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 138. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 37: 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. 151: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 131](#).

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. 152: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <i>licensing.asc.de</i> If you enter this domain, there is no key management.

Parameter	Value/Description
	<ul style="list-style-type: none"> <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 38: Configure virtualization



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.

- 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.

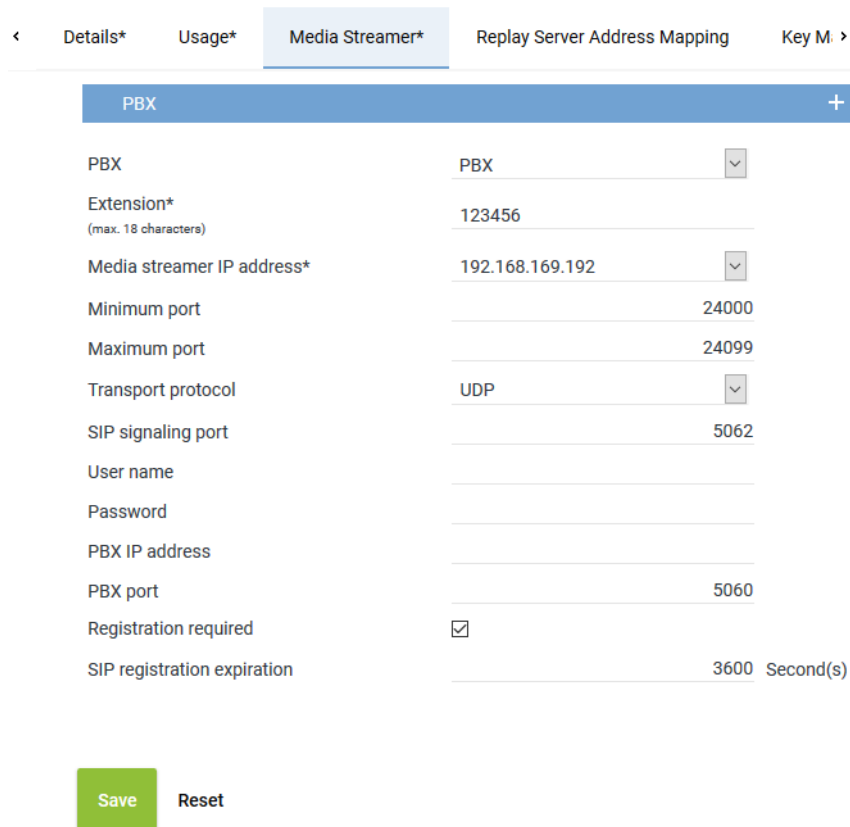
Tab Media Streamer

- 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*.



< Details* Usage* **Media Streamer*** Replay Server Address Mapping Key M. >

PBX +

PBX	PBX	▼
Extension*	123456	
(max. 18 characters)		
Media streamer IP address*	192.168.169.192	▼
Minimum port	24000	
Maximum port	24099	
Transport protocol	UDP	▼
SIP signaling port	5062	
User name		
Password		
PBX IP address		
PBX port	5060	
Registration required	<input checked="" type="checkbox"/>	
SIP registration expiration	3600	Second(s)

Save Reset

Fig. 153: Servers module - tab Media Streamer

- 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.
------------	--

	<p>If no PBX has been created in the system yet, you can create a PBX via the blue bar <i>PBX</i>, see chapter "Create PBX", p. 146.</p>
<i>Extension</i>	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

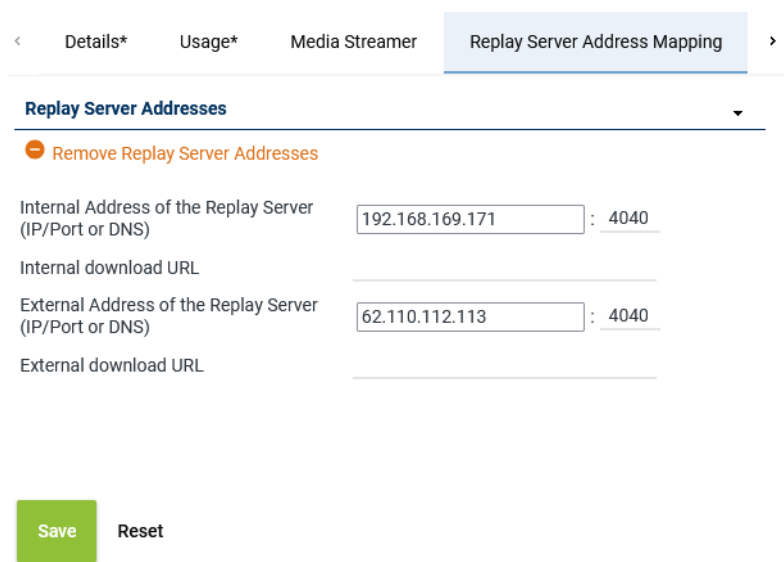



Fig. 154: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

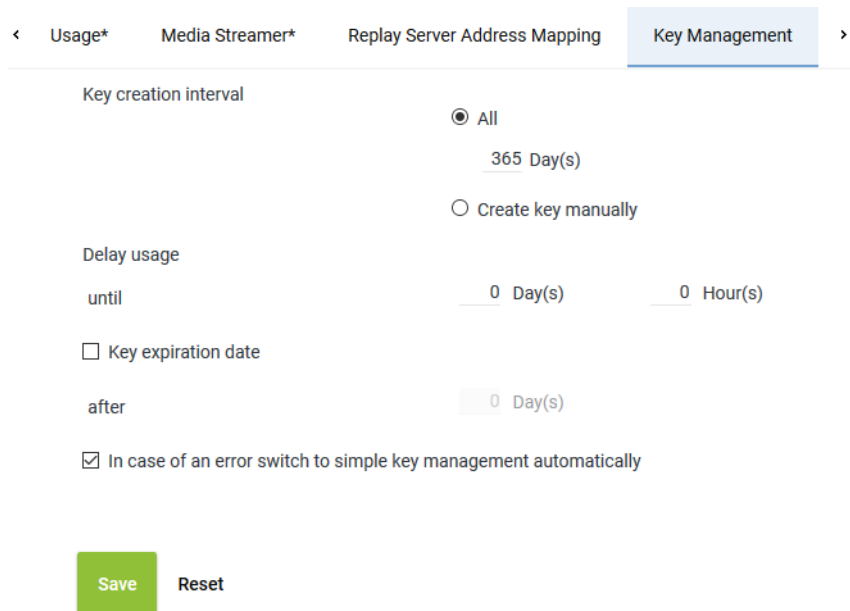


Fig. 155: Servers module - tab Key Management

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.

<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p> <p>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo key management does not work (e. g. if the service <i>DongleMan</i> 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.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = 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 <i>Usage</i>.</p>



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*

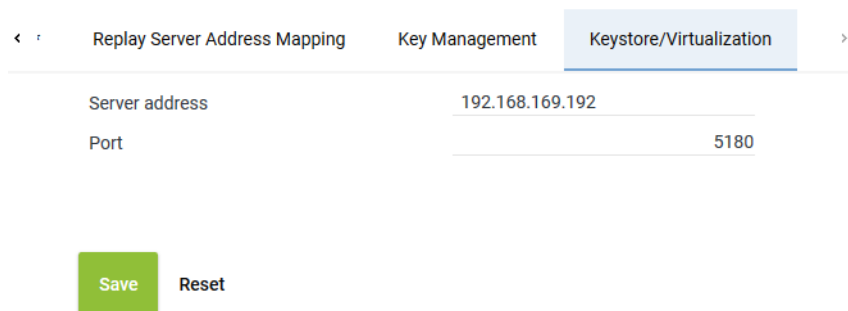
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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.



The screenshot shows a web interface for configuring the Keystore/Virtualization tab. At the top, there are three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is selected. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom, there are two buttons: 'Save' (green) and 'Reset' (gray).

Fig. 156: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management:
-----------------------	--

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	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*.

- 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.

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

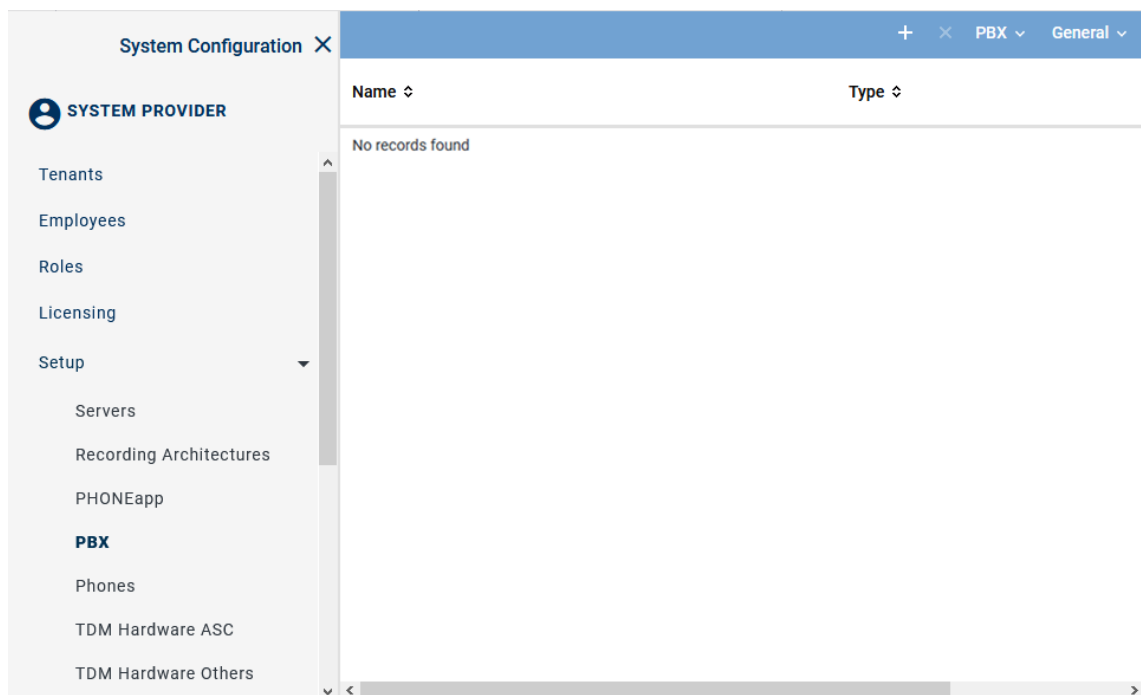


Fig. 157: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

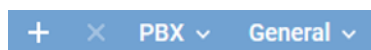




Fig. 158: Toolbar PBX module


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

<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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.

SIP
×

< Details* PHONEapp Configuration Web Service >

Name* SIP

PBX type Universal VoIP

Maximum length of extensions 4 v

Country code
☒ Select from list
United States (1) v
☐ Enter manually

Area code* 6021

Net code* 5963

Non Phone IPs

No records found
Add Delete

IPs to be Ignored

No records found
Add Delete

MACs to be Ignored

No records found
Add Delete

Save
Reset

Fig. 159: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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 <i>094</i>.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 39: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.

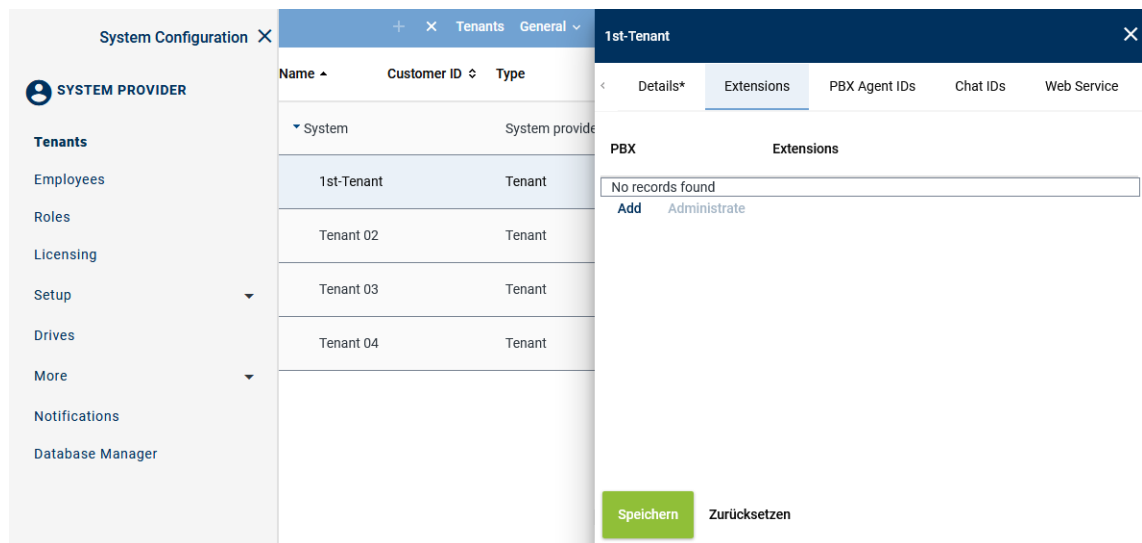


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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.



Name	Customer ID	Type
System		
1st-Tenant		Tenant
Tenant 02		Tenant
Tenant 03		Tenant
Tenant 04		Tenant

1st-Tenant

Details* Extensions PBX Agent IDs Chat IDs Web Service

PBX Extensions

No records found

Add Administrate

Speichern Zurücksetzen

Fig. 160: 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:

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

Extension or extension range separated by
", " or "; (e. g. 3434,3535; 4000-4100)



6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 161: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> • ZIP • TXT • CSV <p>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.</p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	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 detected, 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.

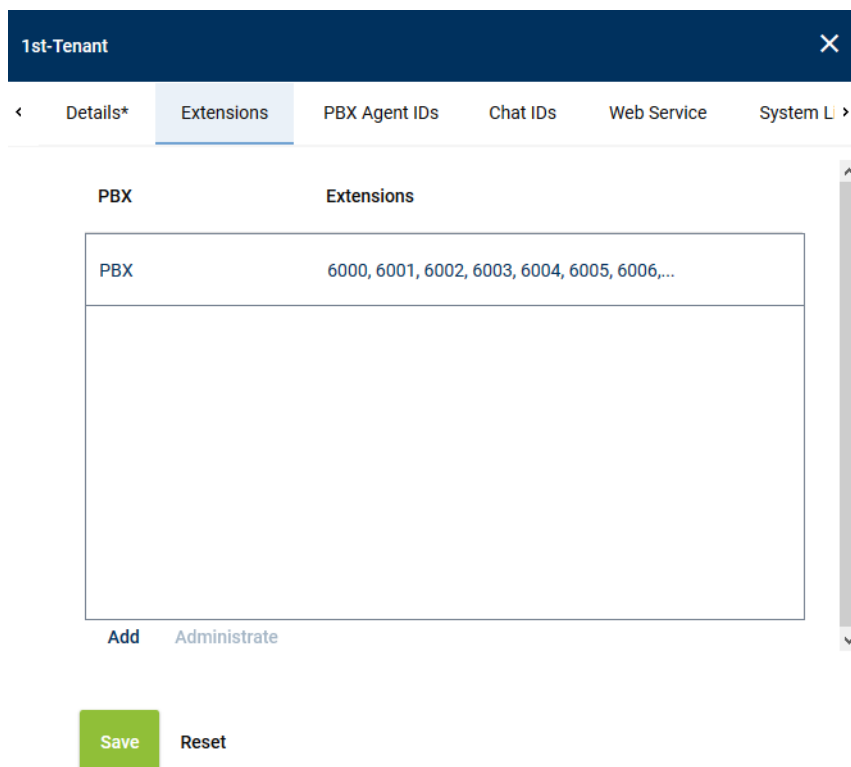


Fig. 162: Remove extensions

2. Click the button *Administrate*.

- 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. 163: Select extensions

- To remove the selected extensions, 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.

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

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

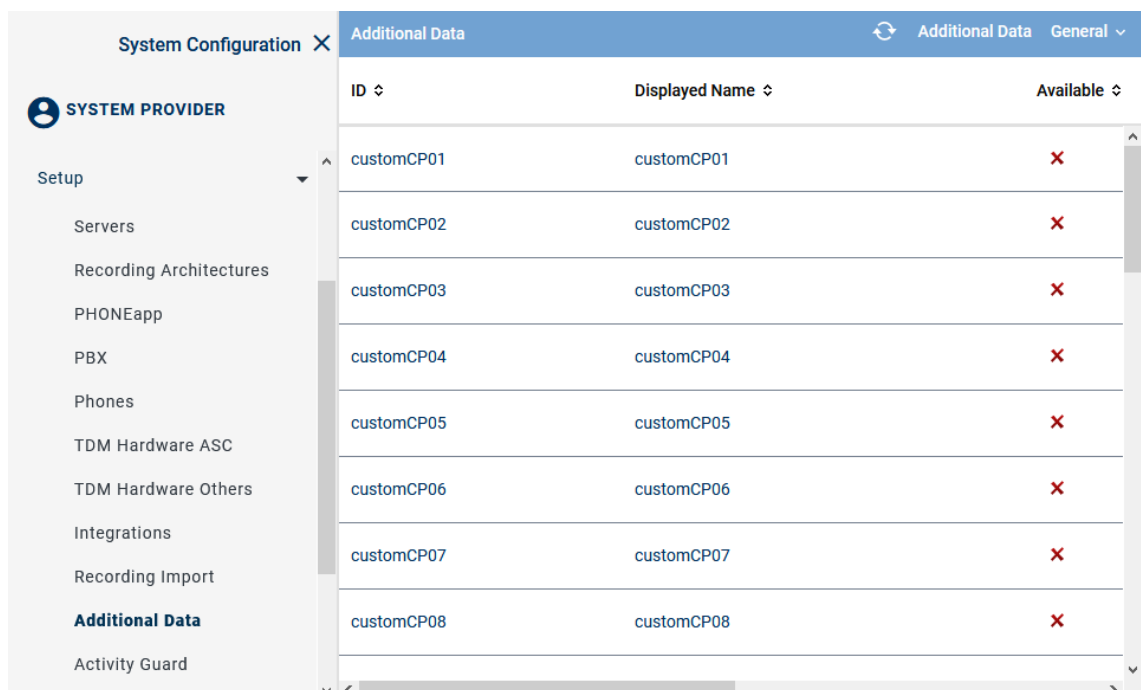


Fig. 164: Additional Data module main view

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

Change display name







Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 165: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 166: 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 an 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:

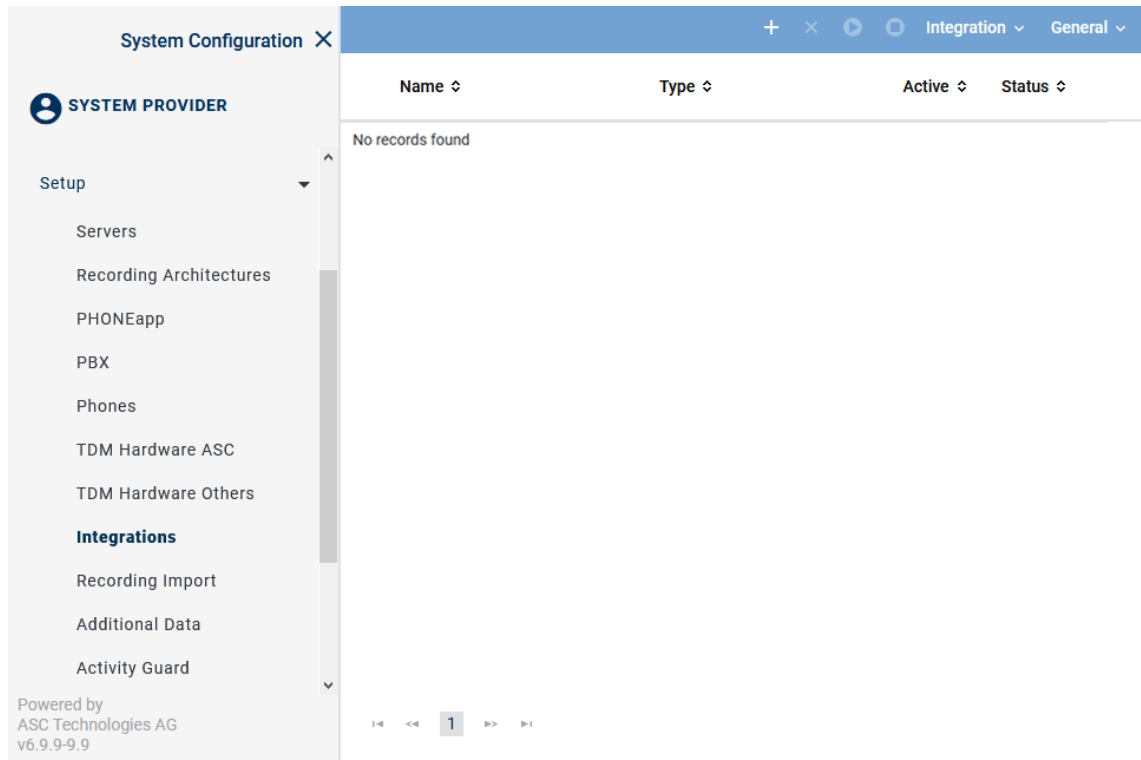




Fig. 167: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module


The toolbar offers the following functions.



Fig. 168: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

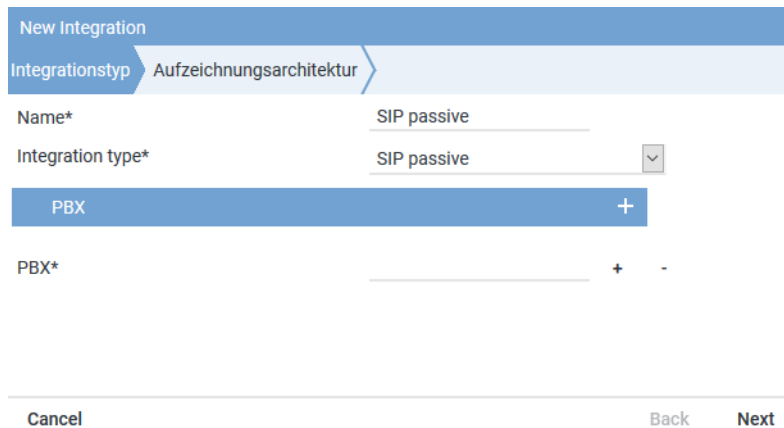



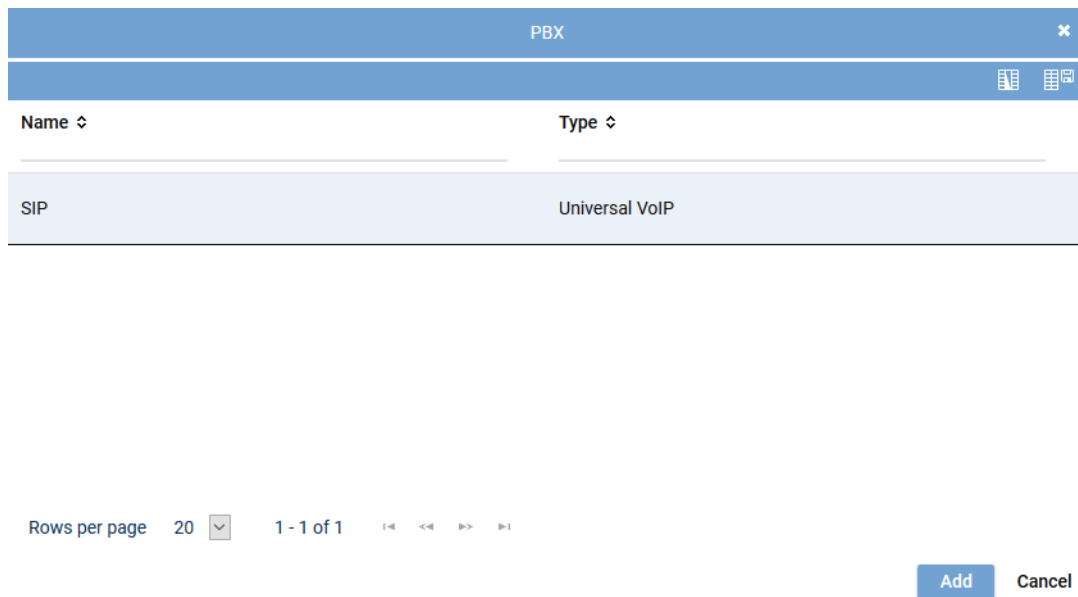
Fig. 169: Create integration type

- Enter the following parameters:

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

Tab. 40: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

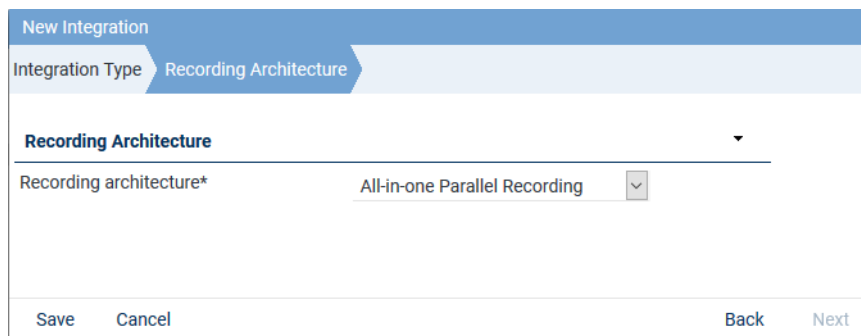
Add Cancel

Fig. 170: Integrations - 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.



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Parallel Recording

Save Cancel Back Next

Fig. 171: 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 Duplicates in parallel recording architectures.

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:







SIP passive		SIP passive	X	
Step	Configuration			
Configure recording architecture	✓ 			
Configure recording servers	X 			
Configure add-on	✓ 			
Configure miscellaneous settings	✓ 			

Fig. 172: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture

Details *


Recording architecture*
All-in-one Parallel Recording

Save Cancel

Fig. 173: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.

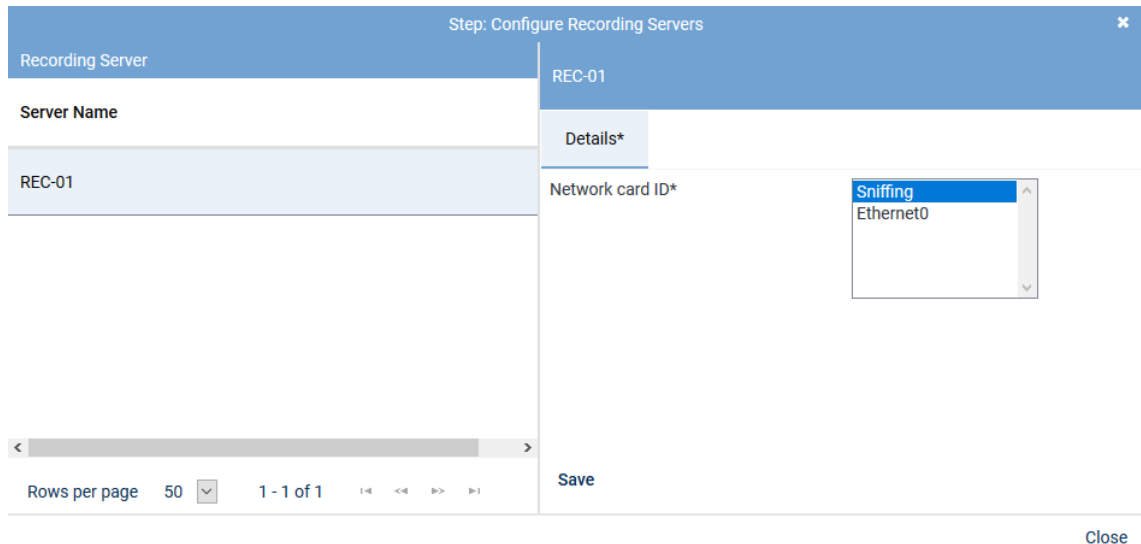


Fig. 174: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
<i>Network card ID</i>	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 41: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 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 CTIconnect 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.

CTIconnect for Genesys T-Server

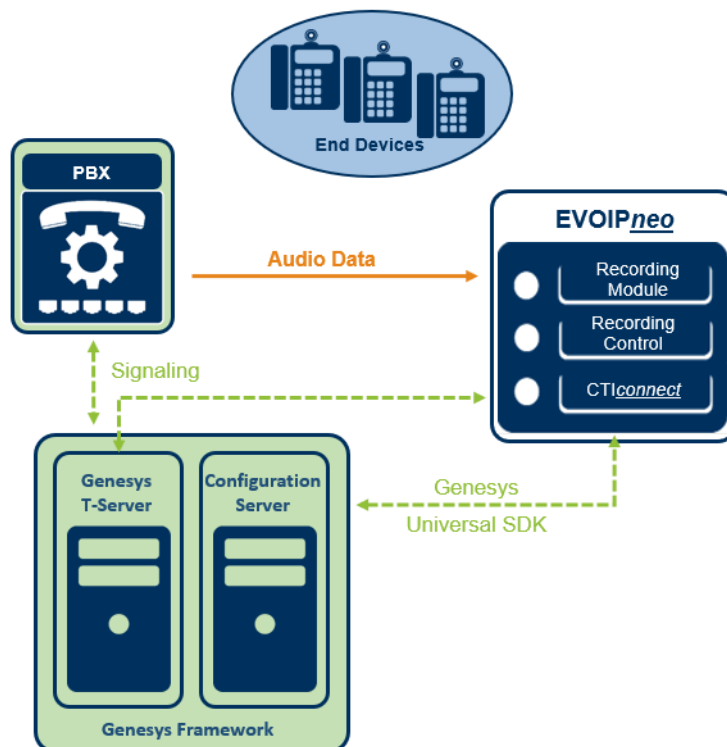


Fig. 175: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

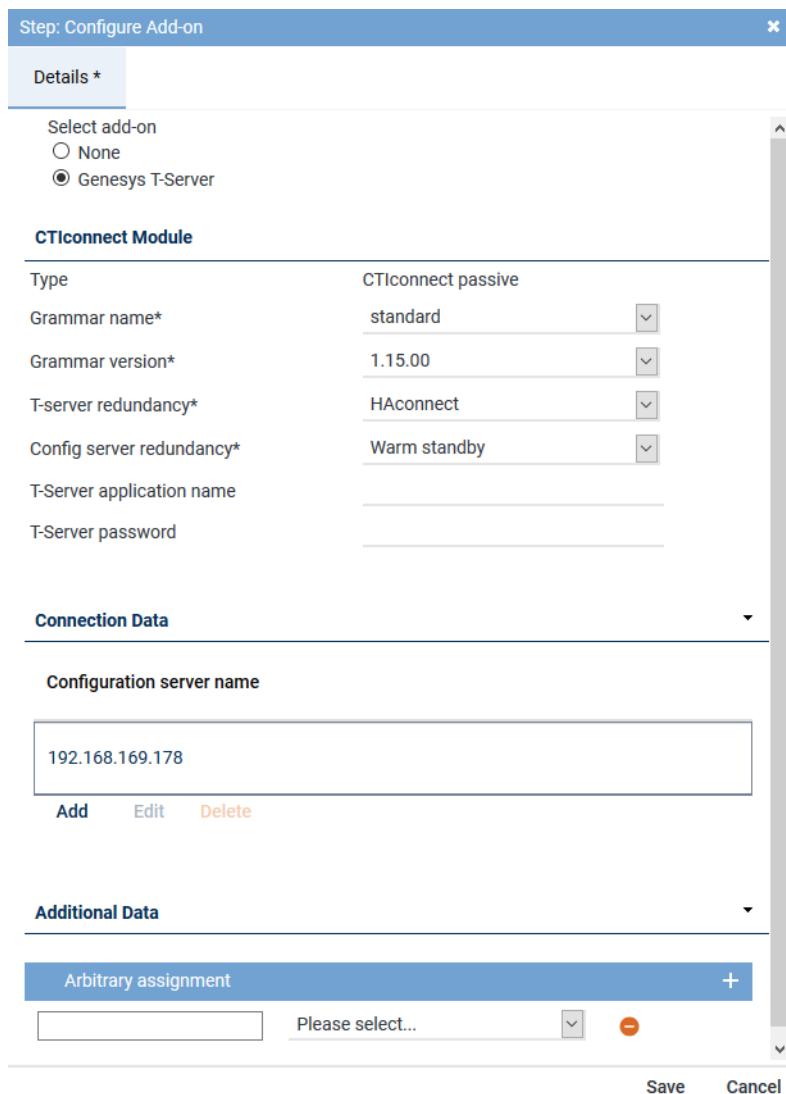
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name
192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment +

Please select...

Save Cancel

Fig. 176: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI <u>connect</u> 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.
<i>T-Server password</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI <u>connect</u> 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. 42: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 177: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 43: 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.

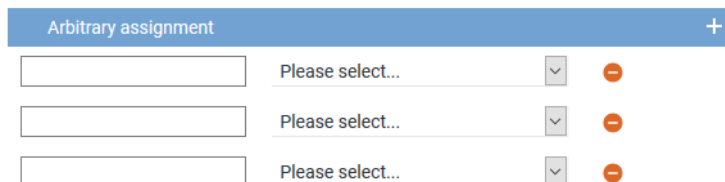



Fig. 178: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

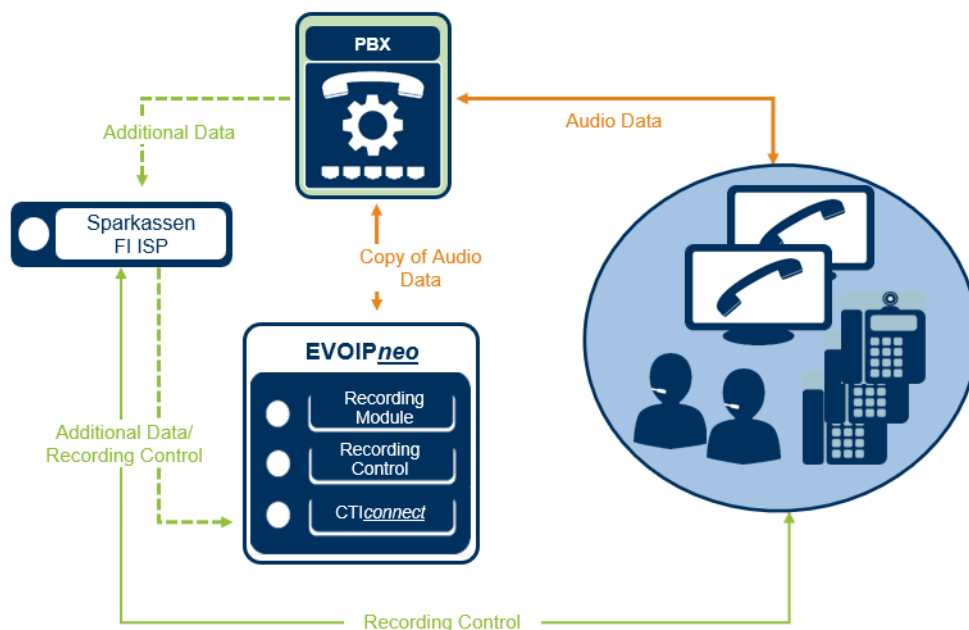



Fig. 179: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

<input style="width: 90%;" type="text"/>	Please select...	▼	○
<input style="width: 90%;" type="text"/>	Please select...	▼	○
<input style="width: 90%;" type="text"/>	Please select...	▼	○

Save Cancel

Fig. 180: 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. 44: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 45: 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 CTIconnect 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.

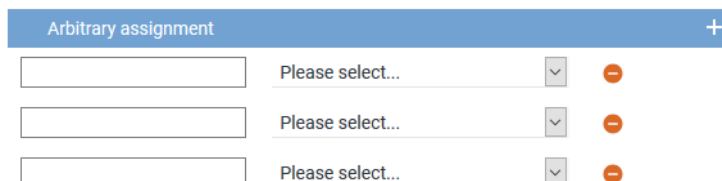



Fig. 181: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

AddEditDelete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

SaveCancel

Fig. 182: Configure add-on for OSCC

Group field CTIconnect Module

- 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. 46: Configure CTIconnect module

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

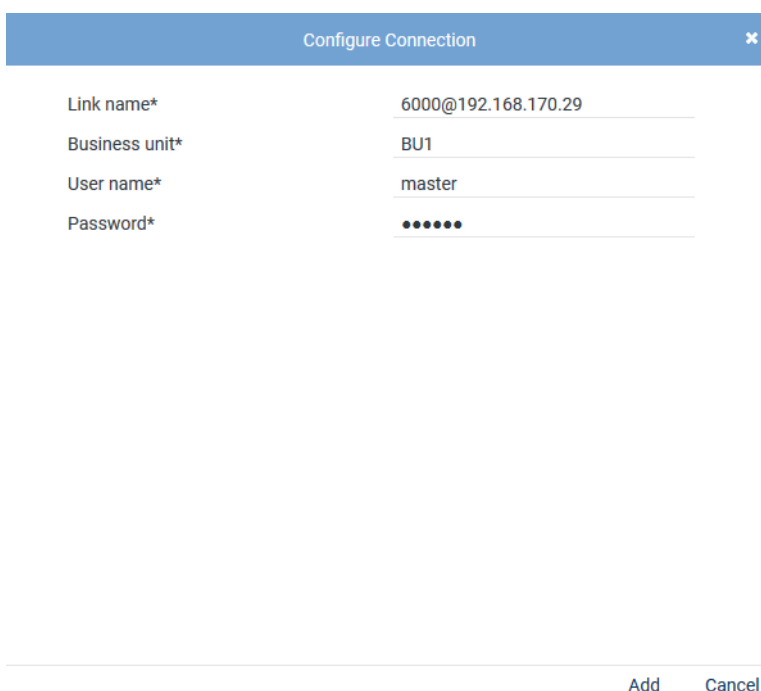


Fig. 183: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 47: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

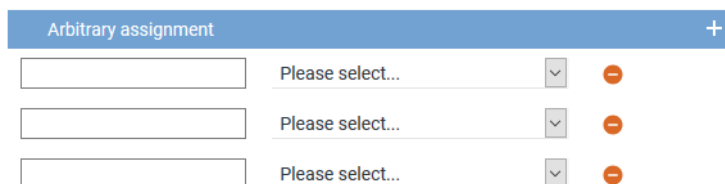





Fig. 184: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 185: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.












	SIP passive	SIP passive		
Step	Configuration			
Configure recording architecture	 			
Configure recording servers	 			
Configure add-on	 			
Configure miscellaneous settings	 			

Fig. 186: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✓	✓

Fig. 187: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✗	✓

Fig. 188: Deactivate integration

- 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.

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

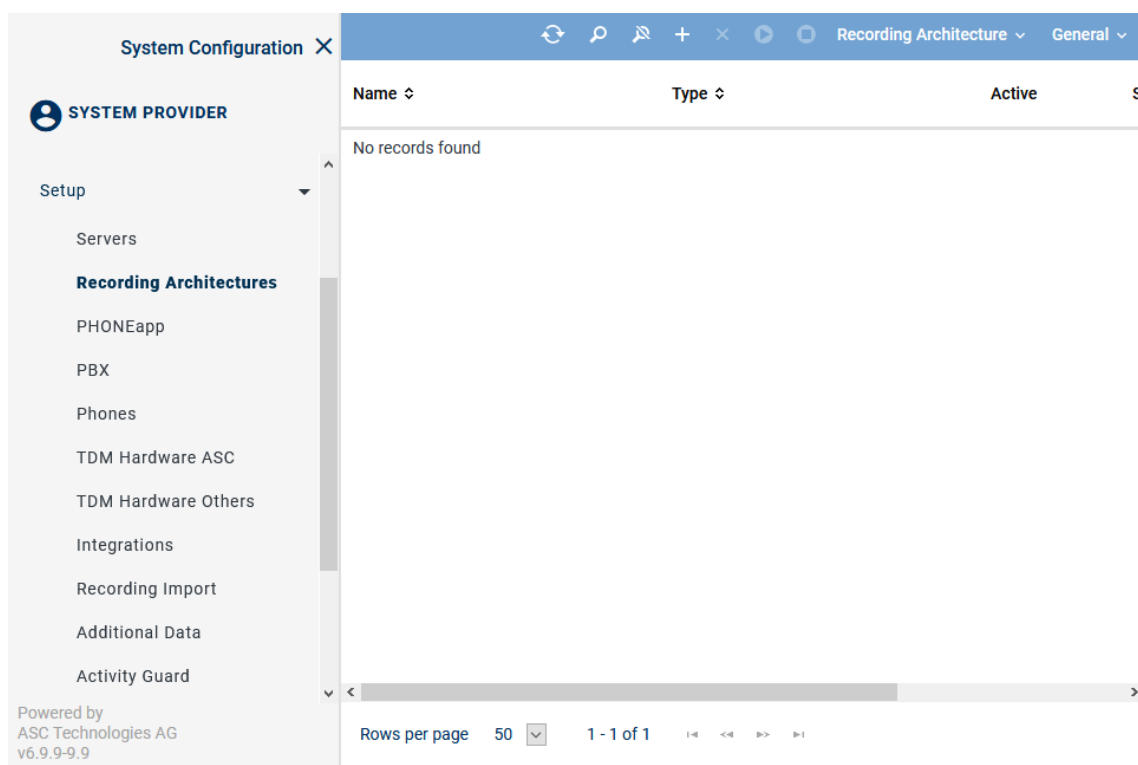




Fig. 189: Recording architectures - main view

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. <div> ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div>
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. <div> ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined. </div>
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. 190: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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 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*.

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

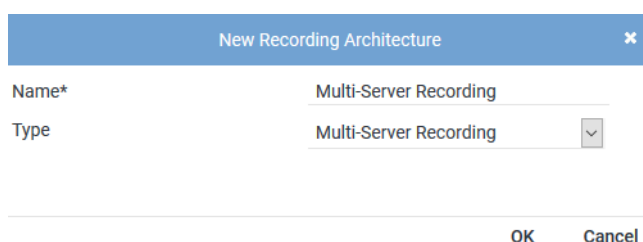
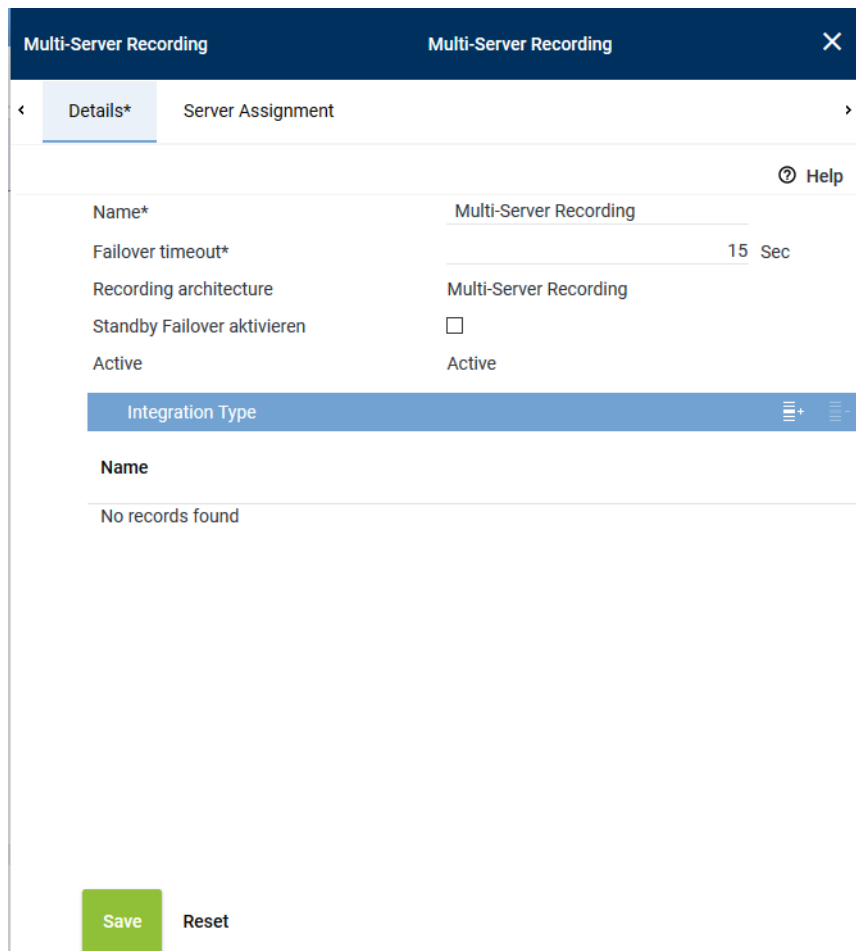


Fig. 191: Create recording architecture - Multi-Server Recording

- 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.



The screenshot shows a configuration window titled "Multi-Server Recording" with a close button (X) in the top right. Below the title bar, there are two tabs: "Details*" (selected) and "Server Assignment". A "Help" icon is in the top right of the content area. The form contains the following fields:

- Name***: Multi-Server Recording
- Failover timeout***: 15 Sec
- Recording architecture**: Multi-Server Recording
- Standby Failover aktivieren**: ☐
- Active**: Active

Below these fields is a section titled "Integration Type" with a list icon and a plus sign. Underneath, there is a "Name" label and a message "No records found". At the bottom left, there are two buttons: "Save" (green) and "Reset".


Fig. 192: 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.

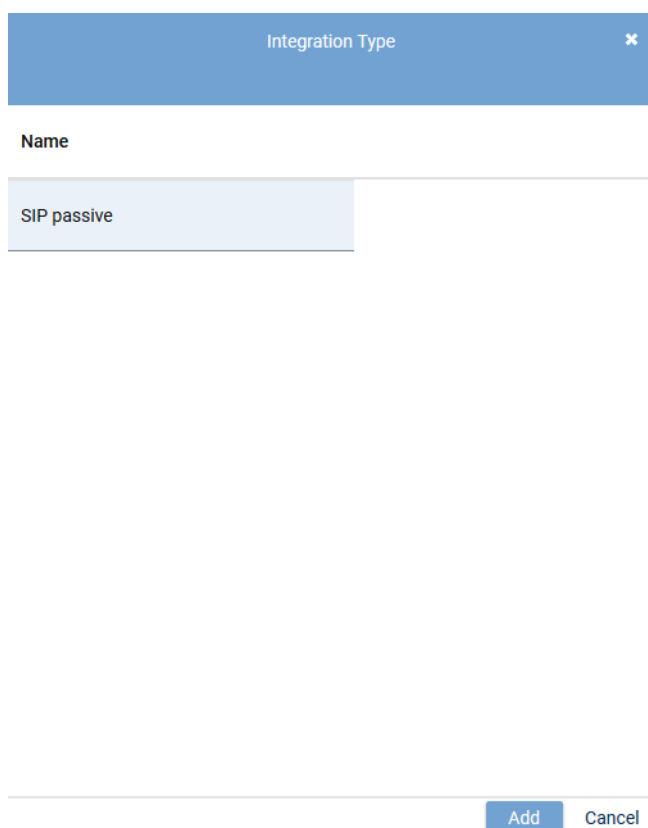


Fig. 193: Select integration type



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 passive* 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 view.

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 CTIconnect

In this group field, you can configure recording control. You can configure two different servers or the same server for this.

Multi-Server Recording
Multi-Server Recording

Details*
Server Assignment*

Recording Control and CTIconnect

Recording Control*	RC-01	+	-
Used in activated architecture	No		
CTIconnect*	RC-01	+	-
Used in activated architecture	No		

Recording Server

Recording Server

Server
Standby

REC-01	REC-02
--------	--------

Save
Reset

Fig. 194: Recording architecture - tab Server Assignment

- Click on the button next to the entry field *Recording Control*.
⇒ The window *Servers* appears.


Servers

Name	IP Address	Path
RC-02	192.168.173.176	C:\
REC-01	192.168.173.171	C:\
REC-04	192.168.173.174	C:\
REC-02	192.168.173.172	C:\
RC-01	192.168.173.175	C:\
CTI-01	192.168.173.177	C:\
CTI-02	192.168.173.178	C:\

Rows per page 20 1 - 8 of 8

Add
Cancel

Fig. 195: 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 .

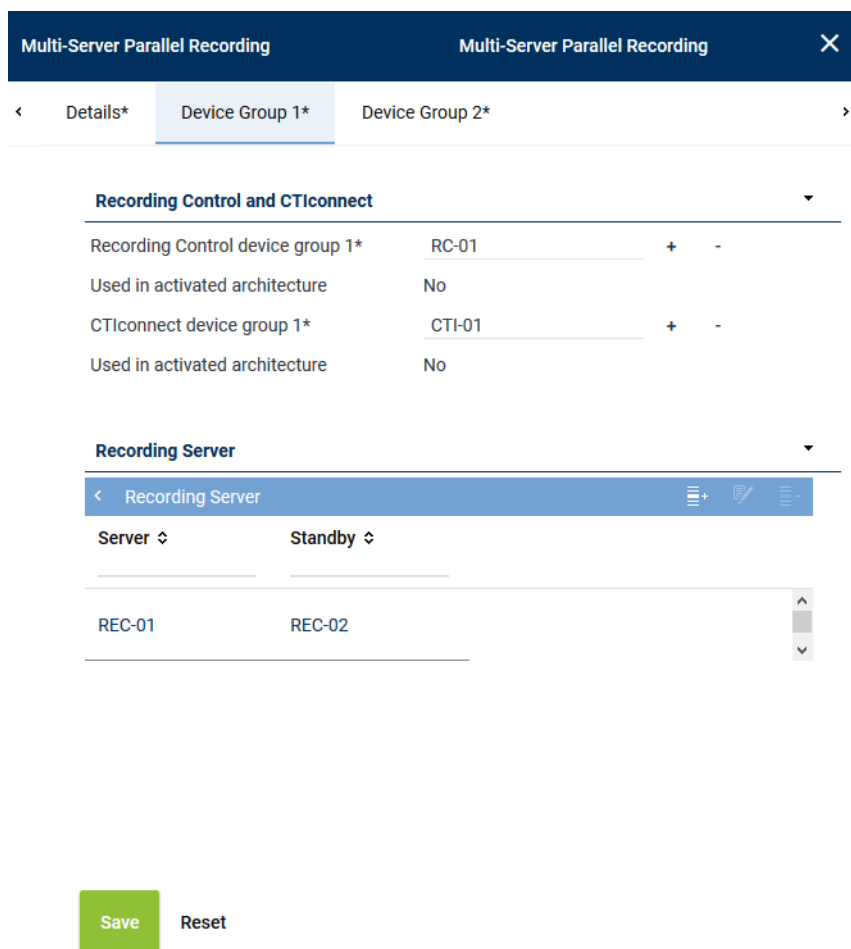


A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the *CTIconnect module* in the entry field *CTIconnect*.

Group field Recording Server

1. In the table headline *Recording Server*, click on the icon .
- ⇒ The following window appears:






Multi-Server Parallel Recording ×

< Details* Device Group 1* Device Group 2* >

Recording Control and CTIconnect ▼

Recording Control device group 1*	RC-01	+	-
Used in activated architecture	No		
CTIconnect device group 1*	CTI-01	+	-
Used in activated architecture	No		



Recording Server ▼



< Recording Server   

Server ↕	Standby ↕
REC-01	REC-02




Save **Reset**

Fig. 196: 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.










     Recording Architecture ▾ General ▾			
Name ▾	Type ▾	Active ▾	Standby active ▾
Multi-Server Recording	Multi-Server Recording		

Fig. 197: 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.

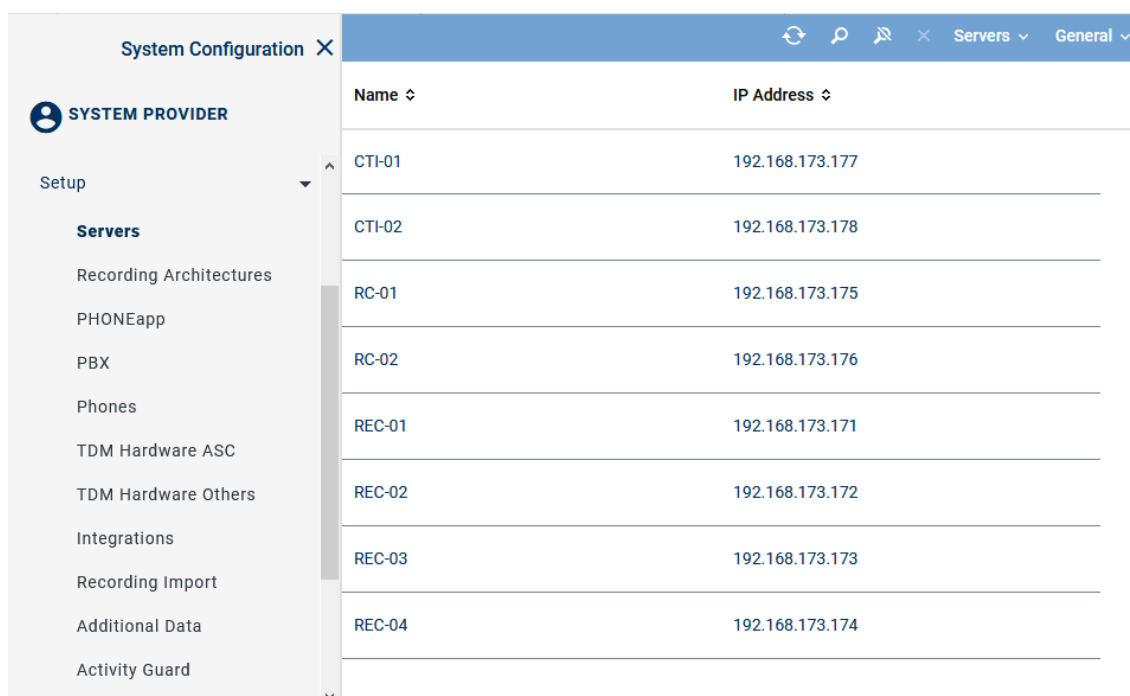


If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

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:



Name	IP Address
CTI-01	192.168.173.177
CTI-02	192.168.173.178
RC-01	192.168.173.175
RC-02	192.168.173.176
REC-01	192.168.173.171
REC-02	192.168.173.172
REC-03	192.168.173.173
REC-04	192.168.173.174

Fig. 198: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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. 199: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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. 182.
	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: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	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

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

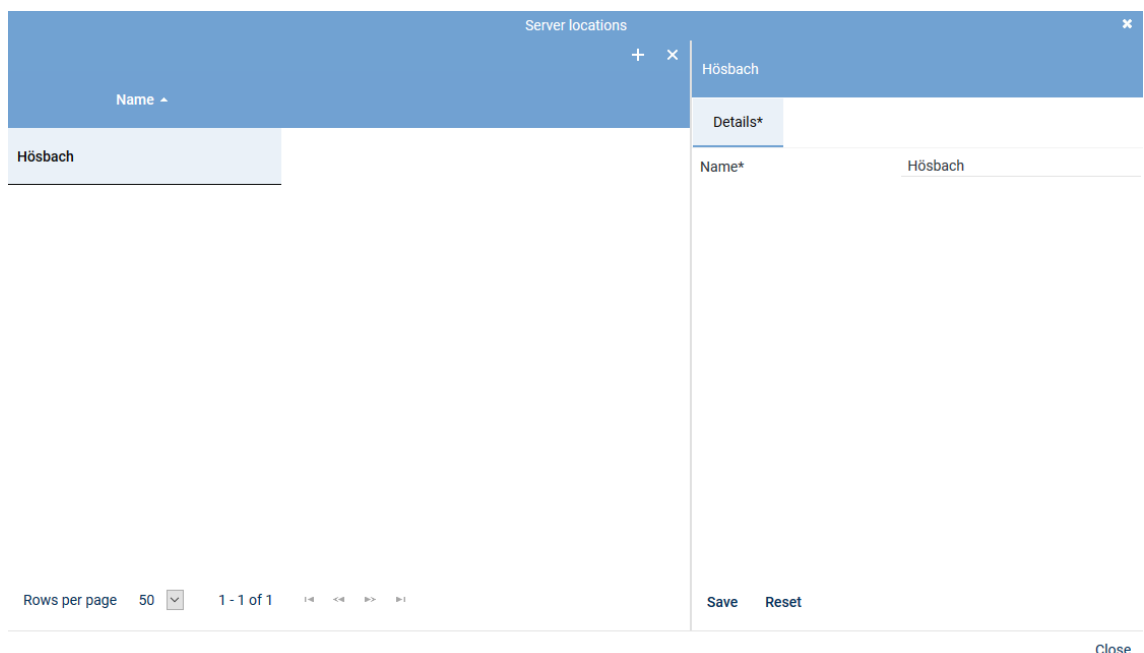



Fig. 200: Add server locations

- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.

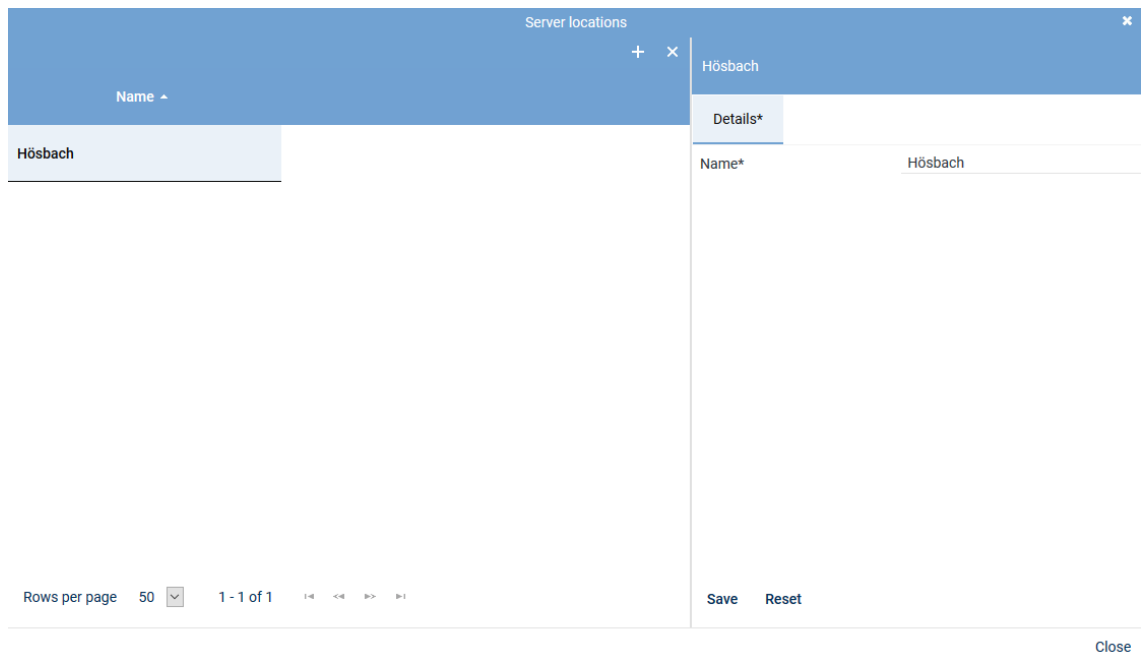
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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.



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a toolbar with a "+" icon and a "x" icon. The main area is divided into two panes. The left pane contains a table with one row: "Hösbach". The right pane has a tab labeled "Details*" and a form with a label "Name*" and a text input field containing "Hösbach". At the bottom of the window, there are buttons for "Save", "Reset", and "Close".

Fig. 201: 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.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
Key Ma >

? Help

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171 <input type="button" value="v"/>
Server location	Hörsbach <input type="button" value="v"/>

Fig. 202: Servers - tab Details

- From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
- Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.
- Click on the button **Save** if the entries are correct.

Tab Usage

- 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.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

API Server	▶
Audio Analysis	▶
Recording Control/Key Management	▶
Data Processing	▶
Replay	▶
Virtualization	▶

Fig. 203: Servers - tab usage

Group field API Server

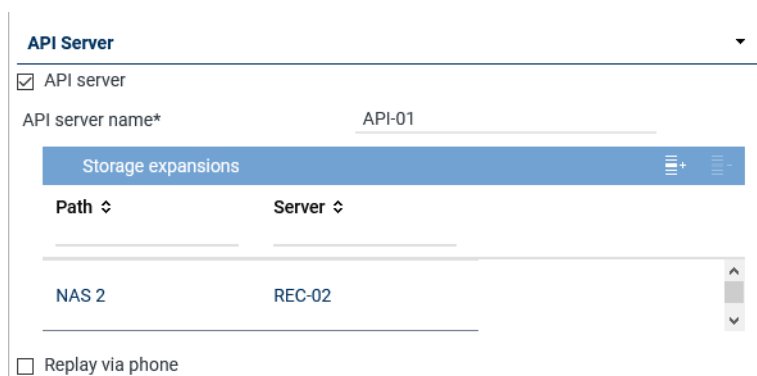




Fig. 204: Group field API Server

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
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 195.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List</i> <i>Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 186. By clicking on the icon  (<i>Remove</i>), 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.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 193. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.

Storage Expansion for Replay				
Device Type	Name	Path	Free Disk Space	Server
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page: 20  1 - 1 of 1



 

Fig. 205: Select storage expansion

- 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

Audio Analysis

☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 206: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> 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. 48: Configure audio analysis

Emotion Detection

Name

REC-01

Rows per page 20

1 - 8 of 8

<<

<

>

>>

Add

Cancel

Fig. 207: Select server for emotion detection

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

Group field Recording Control/Key Management

Recording Control/Key Management

☐ Recording control/Live Streaming

Recording architecture Please choose...

☐ neo key management

Fig. 208: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 49: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 209: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list</p>

Parameter	Value/Description
	<p><i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 190. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 190. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> 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. <p>NOTICE! For the export from Neo to Neo, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> 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. <p>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.</p>

Tab. 50: Data storage

Add target server to a list

- In the toolbar of the list *Target Server*, click on the icon  (*Add*).
- 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.

Target Server	
Name ↕	IP Address ↕
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173

Rows per page 20 1 - 6 of 6

Add Cancel

Fig. 210: Select server



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

- 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

Replay

☒ Replay

Replay server*

WebSocket port*


(max. 5 characters)


API server*

+
 -

Name ↕	Connection Status
--------	-------------------

Fig. 211: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. 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.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 192.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (Remove), you can remove selected API servers from the list.

Tab. 51: 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.
- To assign an [API](#) server, click on the icon  (Add) in the toolbar of the list *API Server*.
 - Select the server from the list on which the [API](#) service is running.



Fig. 212: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 185](#).

- 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

Virtualization

☐ VM without Trusted License

Fig. 213: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <i>licensing.asc.de</i> If you enter this domain, there is no key management. • <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 52: Configure virtualization



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*.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

PBX +

PBX	PBX	▼
Extension* (max. 18 characters)	123456	
Media streamer IP address*	192.168.169.192	▼
Minimum port	24000	
Maximum port	24099	
Transport protocol	UDP	▼
SIP signaling port	5062	
User name		
Password		
PBX IP address		
PBX port	5060	
Registration required	<input checked="" type="checkbox"/>	
SIP registration expiration	3600	Second(s)

Save
Reset

Fig. 214: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>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. 199.</p>
Extension	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>

<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box Registration required.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
>

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 215: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

< Usage* Media Streamer* Replay Server Address Mapping
Key Management >

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage
until

0 Day(s)

0 Hour(s)

☐ Key expiration date
after

0 Day(s)

☒ In case of an error switch to simple key management automatically

Save Reset

Fig. 216: Servers module - tab Key Management

<i>Key creation interval</i>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> • <i>All</i> 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 • <i>Create key manually</i> Select that a key is supposed to be generated manually. <p>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.</p>
<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p>

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*

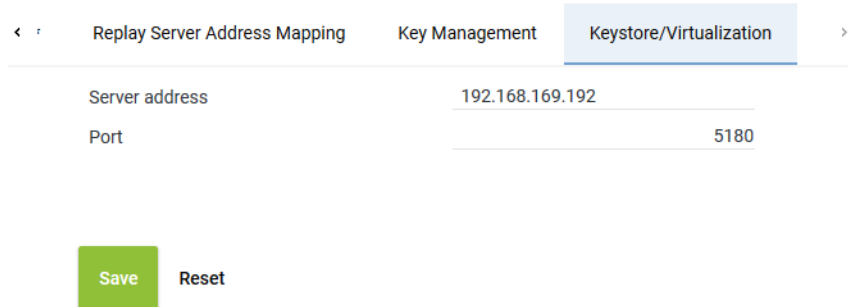
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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.



The screenshot shows a configuration interface with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is active. It contains two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. Below the fields are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 217: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management: IP address of the server where the service <i>DongleMan</i> has been installed.
Port	<p>Enter the port for the connection.</p> <p>5180 = Dongle Manager</p> <p>8181 = ASC License Management System</p>



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:

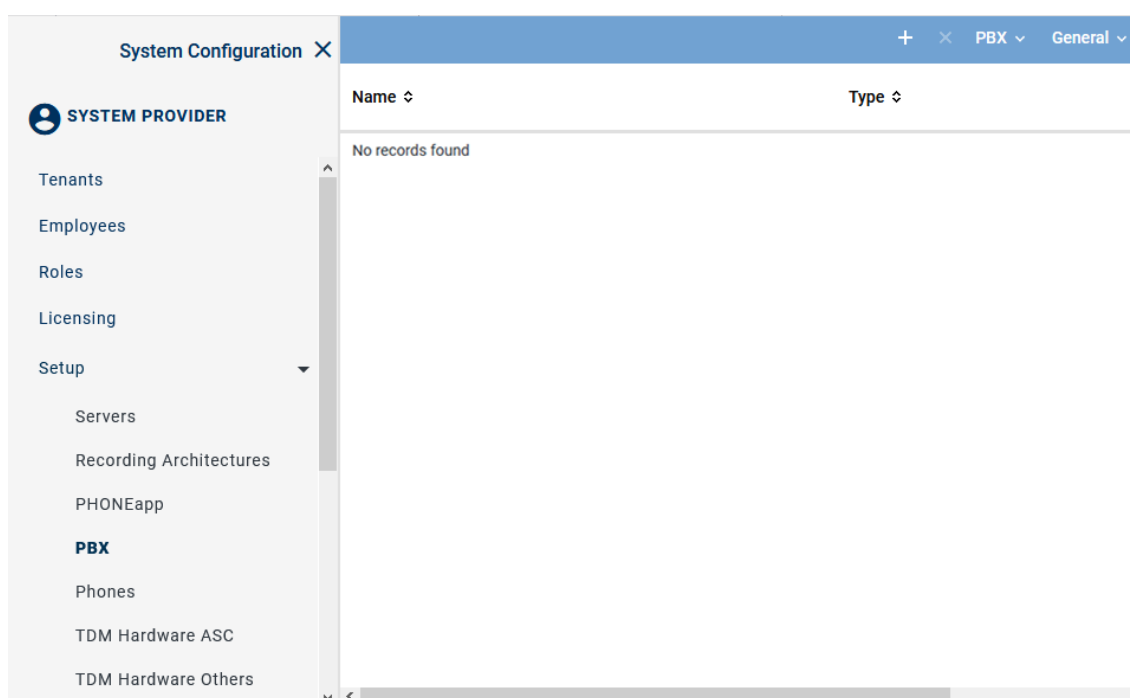




Fig. 218: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 219: Toolbar PBX module

	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administratre Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

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

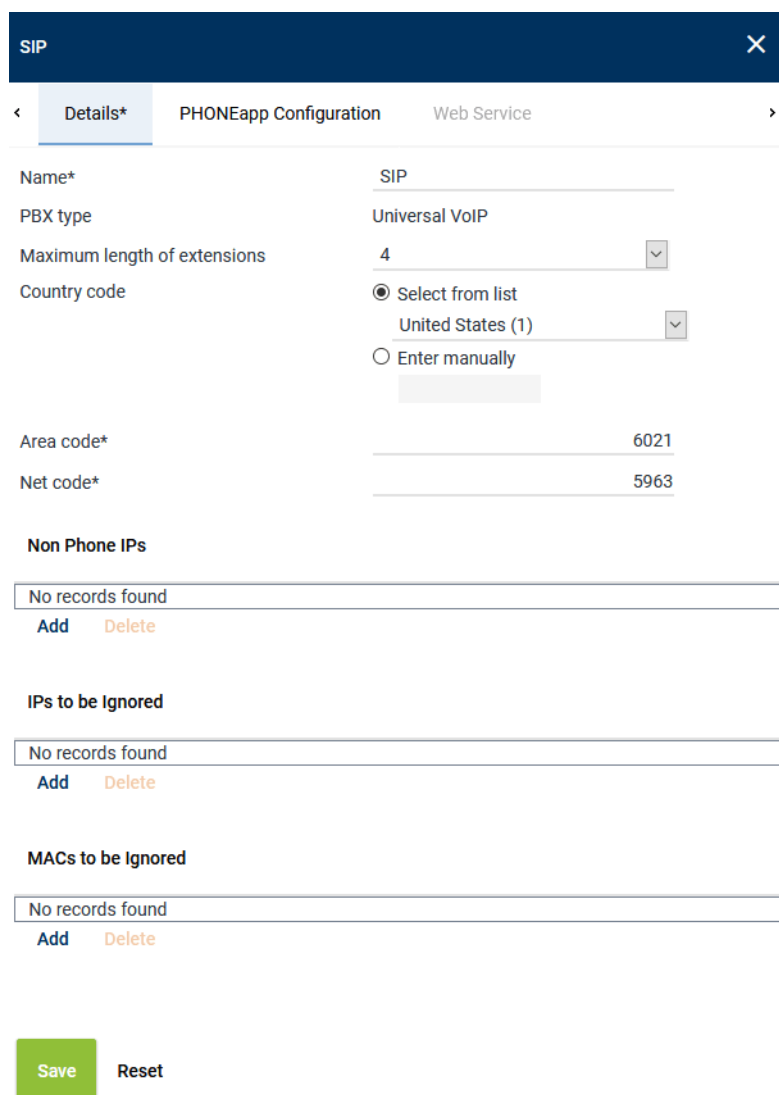


Fig. 220: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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 <i>094</i>.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.

Parameter	Value/Description
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 53: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.

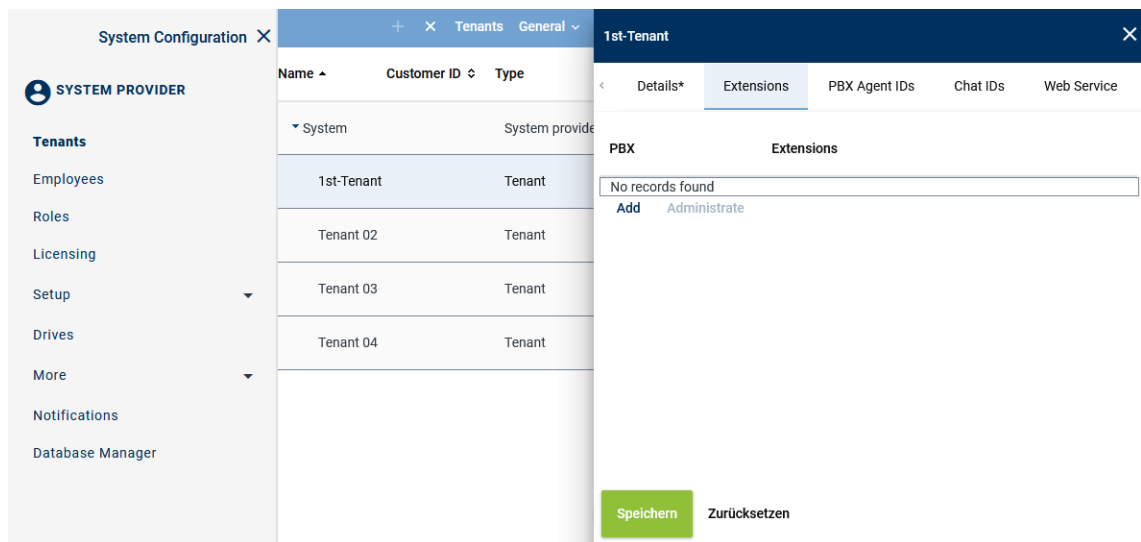


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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.



Name	Customer ID	Type
System		System provider
1st-Tenant		Tenant
Tenant 02		Tenant
Tenant 03		Tenant
Tenant 04		Tenant

1st-Tenant

Details* Extensions PBX Agent IDs Chat IDs Web Service

PBX Extensions

No records found

Add Administrate

Speichern Zurücksetzen

Fig. 221: 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:

Add Extensions ✕

PBX

PBX ▼

☐ File import

☐ File contains a headline

File name

...

☒ Manual entry

Extension or extension range separated by
", " or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 222: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> ZIP TXT CSV <p>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.</p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP_{neo} passive for SIP - neo 7.x Rev. 1

204 / 358

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 detected, 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.

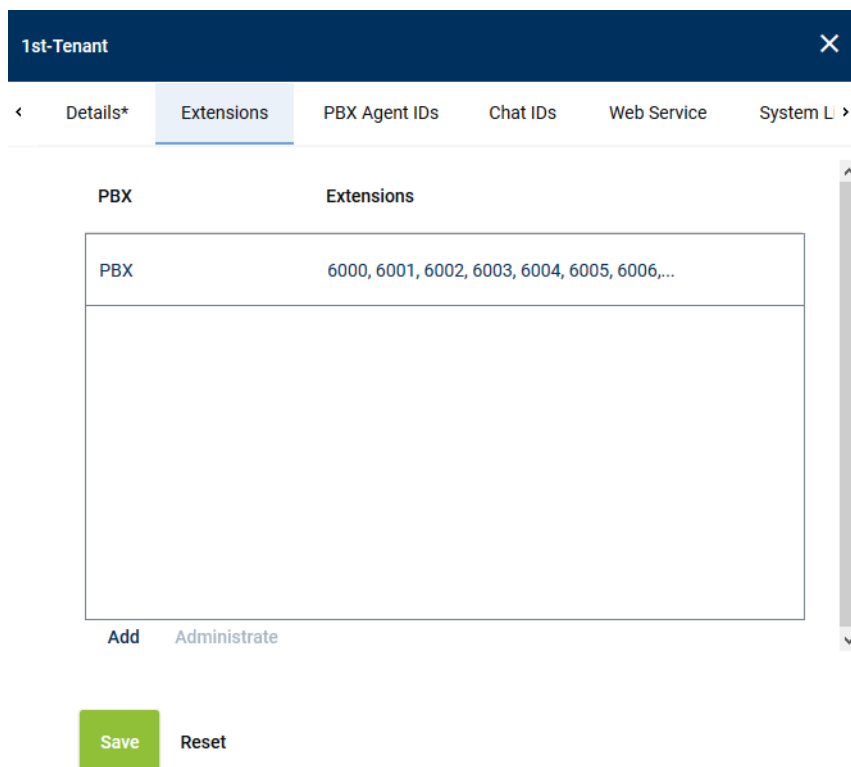


Fig. 223: Remove extensions

2. Click the button *Administrate*.

- 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.

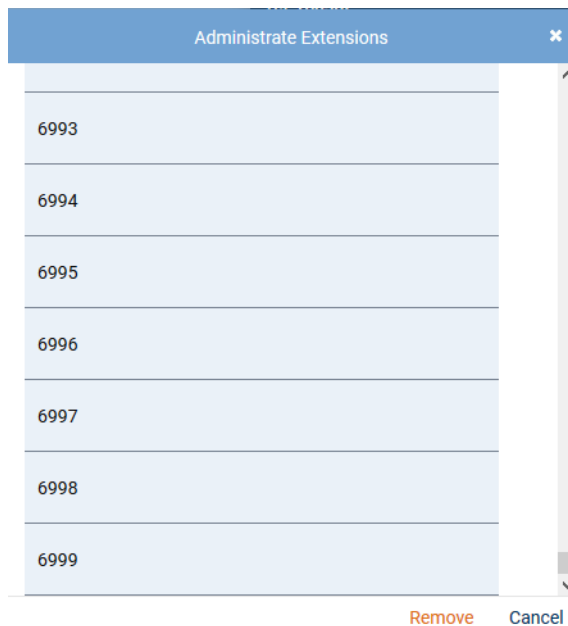


Fig. 224: Select extensions

- To remove the selected extensions, 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.

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

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

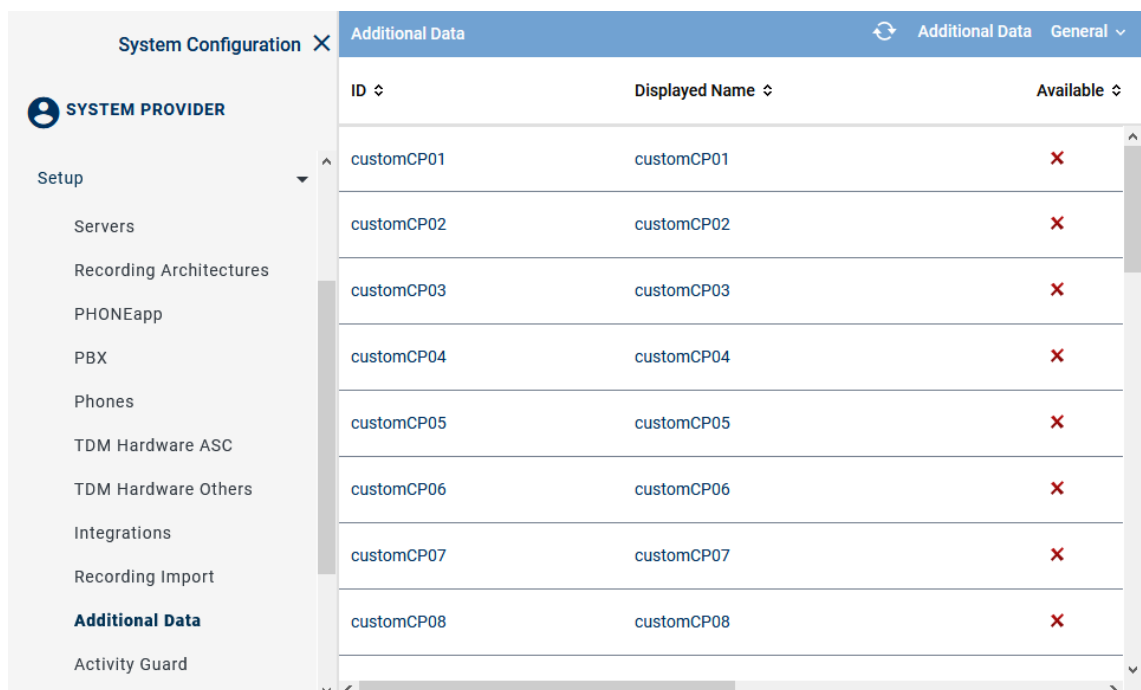


Fig. 225: Additional Data module main view

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

Change display name







Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 226: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 227: 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:

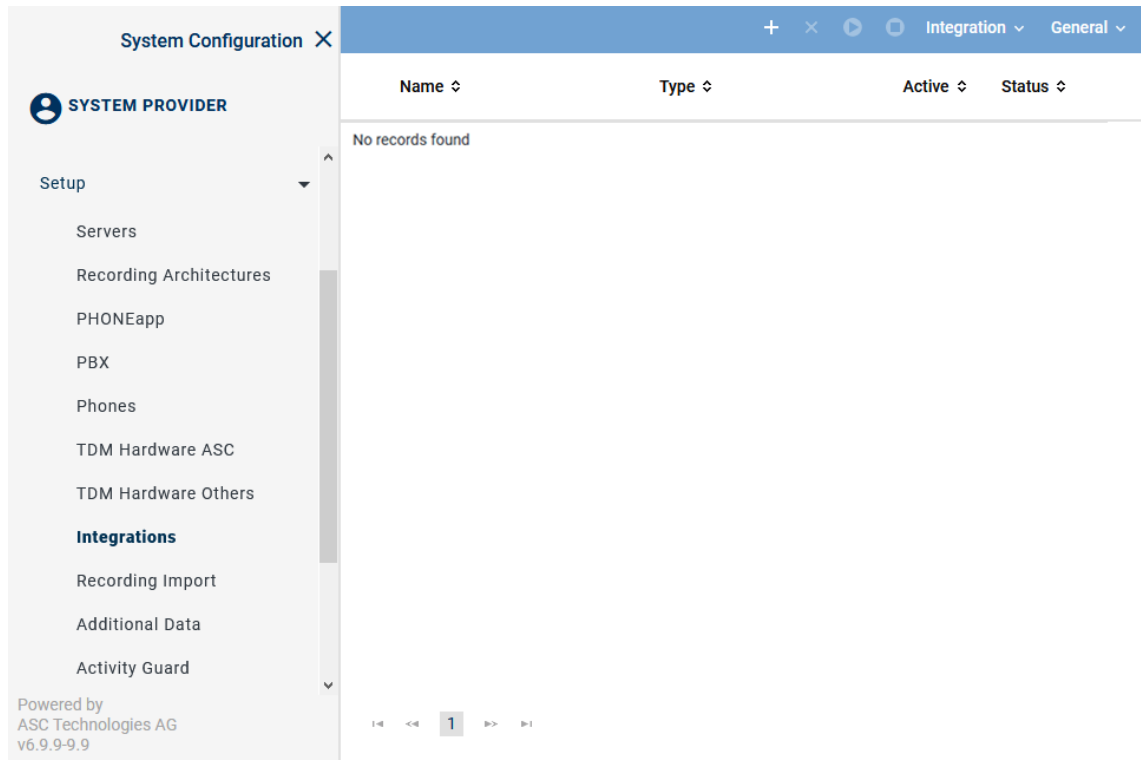




Fig. 228: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module

The toolbar offers the following functions.

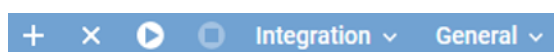







Fig. 229: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

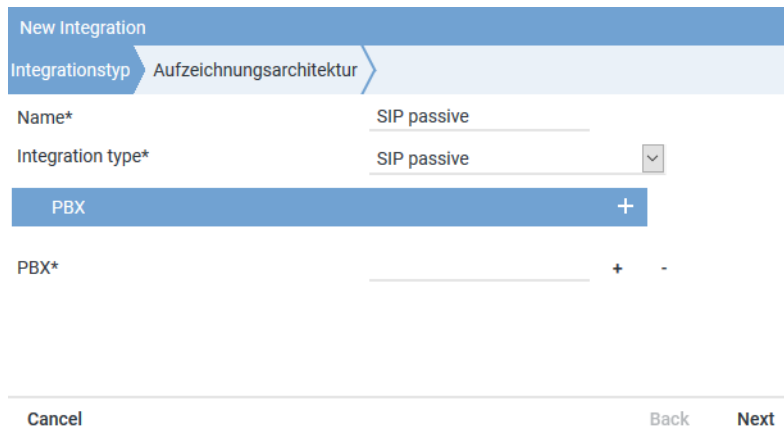



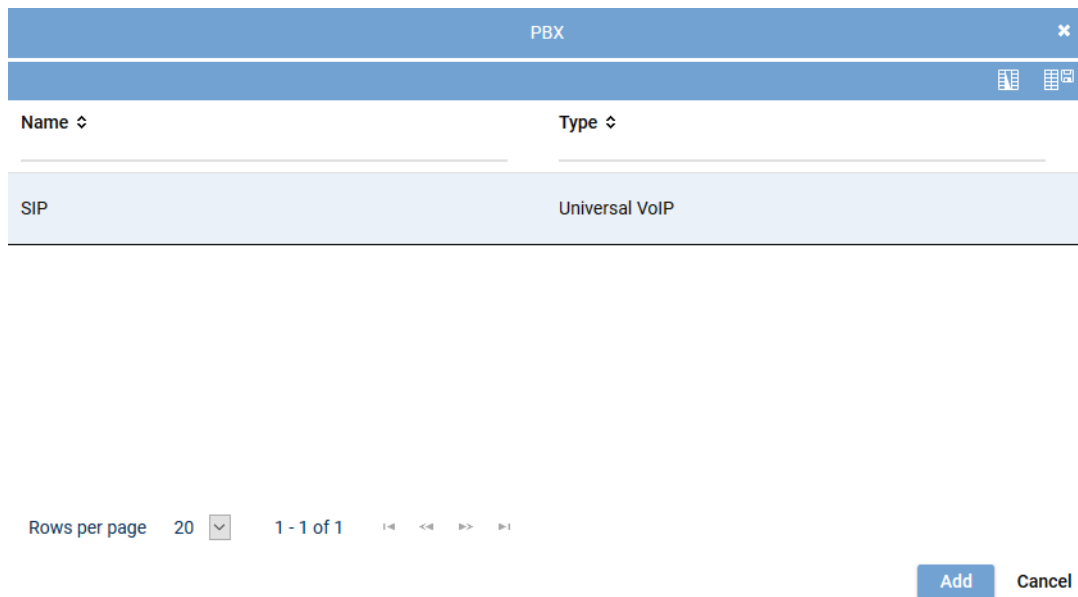
Fig. 230: Create integration type

- Enter the following parameters:

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

Tab. 54: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



Name	Type
SIP	Universal VoIP

Rows per page: 20 | 1 - 1 of 1 | < > >> <<

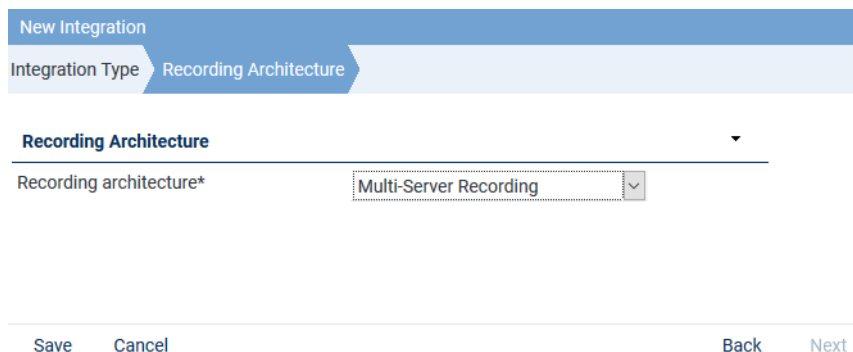
[Add](#) [Cancel](#)

Fig. 231: Integrations - 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.



New Integration

Integration Type | **Recording Architecture**

Recording Architecture

Recording architecture* | Multi-Server Recording

[Save](#) [Cancel](#) [Back](#) [Next](#)

Fig. 232: 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:






<div> <div>SIP passive</div> <div>SIP passive</div> <div>✗</div> <div>⚙️</div> </div>	
Step	Configuration
Configure recording architecture	✓ 
Configure recording servers	✗ 
Configure add-on	✓ 
Configure miscellaneous settings	✓ 

Fig. 233: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture ✕

Details *


Recording architecture*

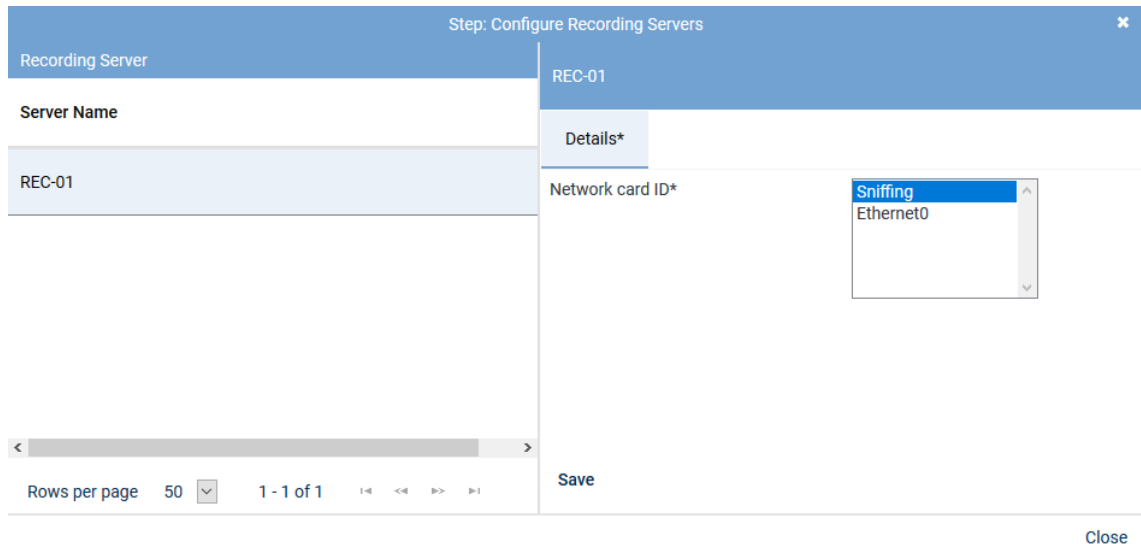
Save Cancel

Fig. 234: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.



Step: Configure Recording Servers

Recording Server	REC-01
Server Name	REC-01

Details*

Network card ID*

Sniffing
Ethernet0

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 235: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
Network card ID	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 55: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 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 CTIconnect 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.

CTIconnect for Genesys T-Server

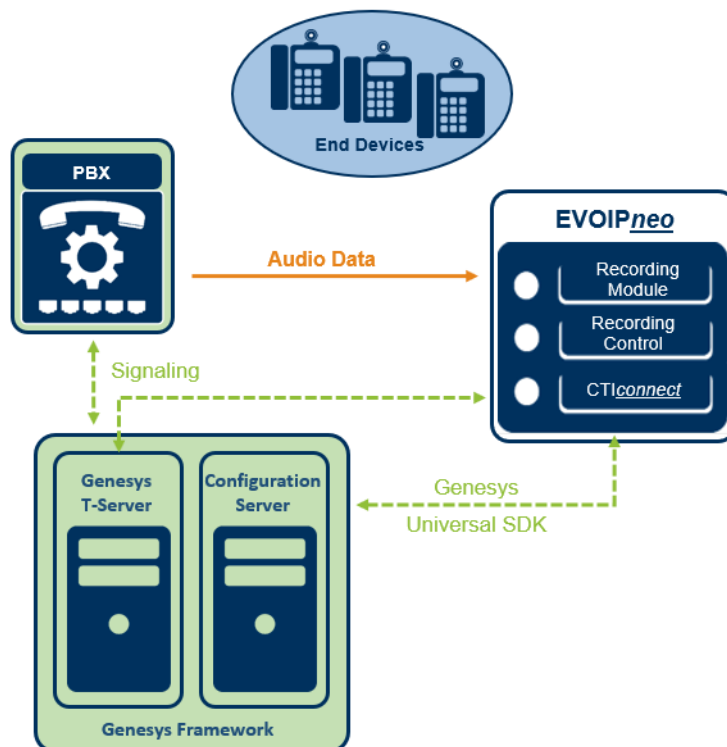


Fig. 236: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

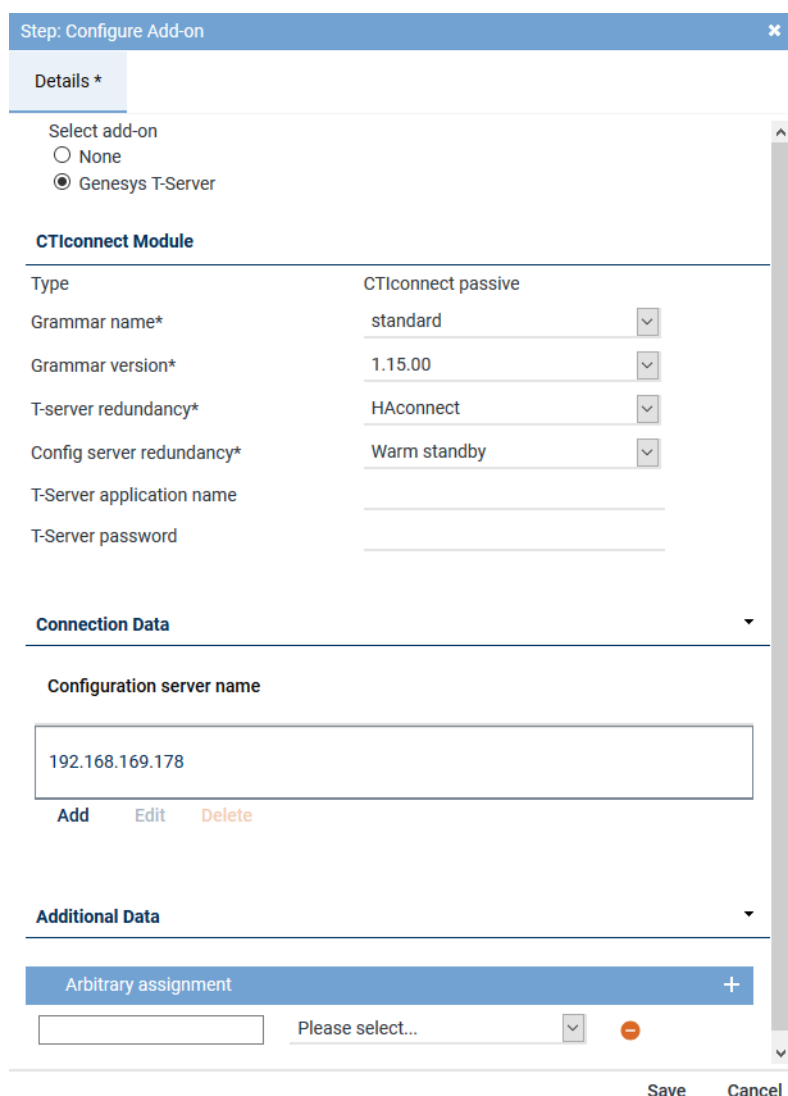
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name

192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment +

Please select...

Save Cancel

Fig. 237: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI <u>connect</u> 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.
<i>T-Server password</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI <u>connect</u> 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. 56: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 238: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 57: 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.

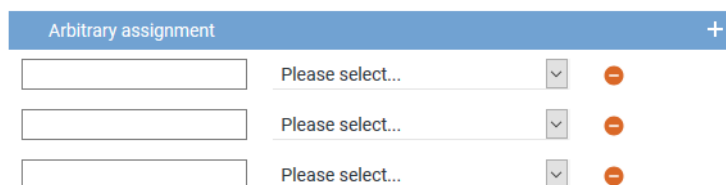



Fig. 239: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

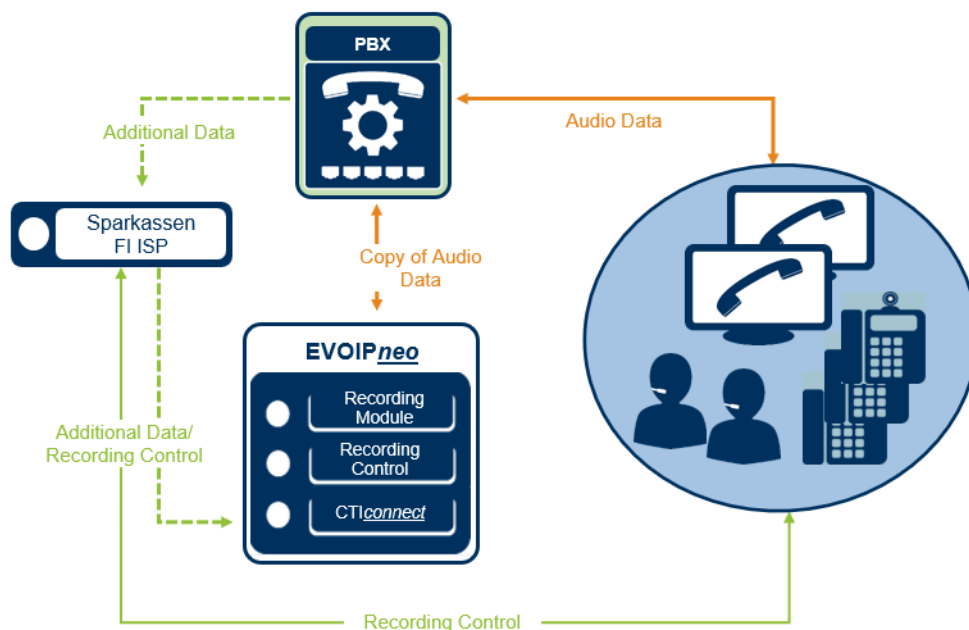



Fig. 240: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

	Please select...	▼	⊖
	Please select...	▼	⊖
	Please select...	▼	⊖

Save Cancel

Fig. 241: 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. 58: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 59: 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 CTIconnect 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.

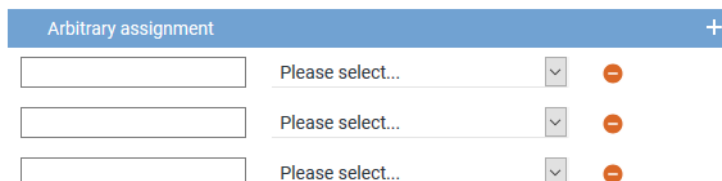



Fig. 242: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

Add Edit Delete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

Save Cancel

Fig. 243: Configure add-on for OSCC

Group field CTIconnect Module

- 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. 60: Configure CTIconnect module

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

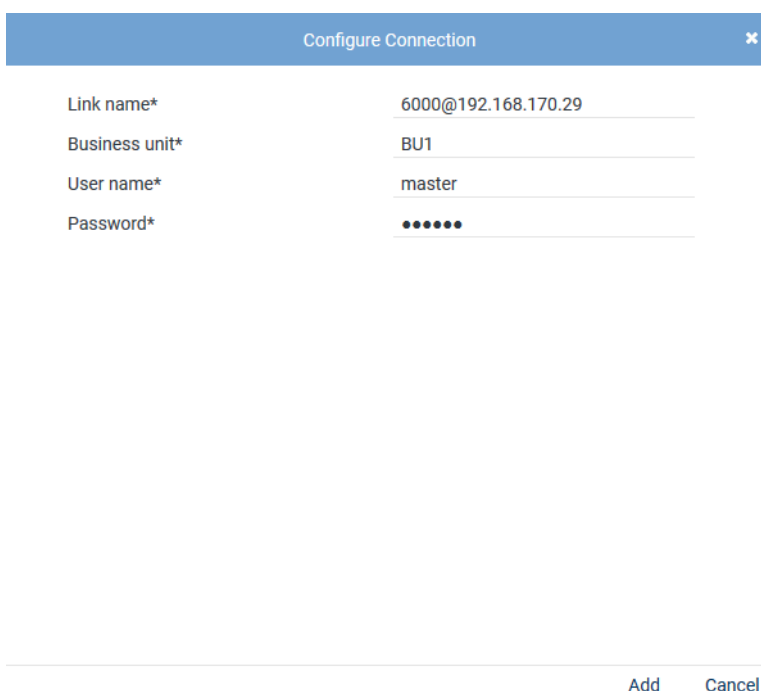


Fig. 244: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 61: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

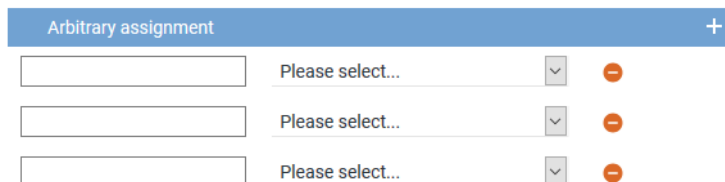





Fig. 245: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 246: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.












	SIP passive	SIP passive		
Step		Configuration		
Configure recording architecture				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 247: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✓	✓

Fig. 248: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✗	✓

Fig. 249: Deactivate integration

- 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.

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

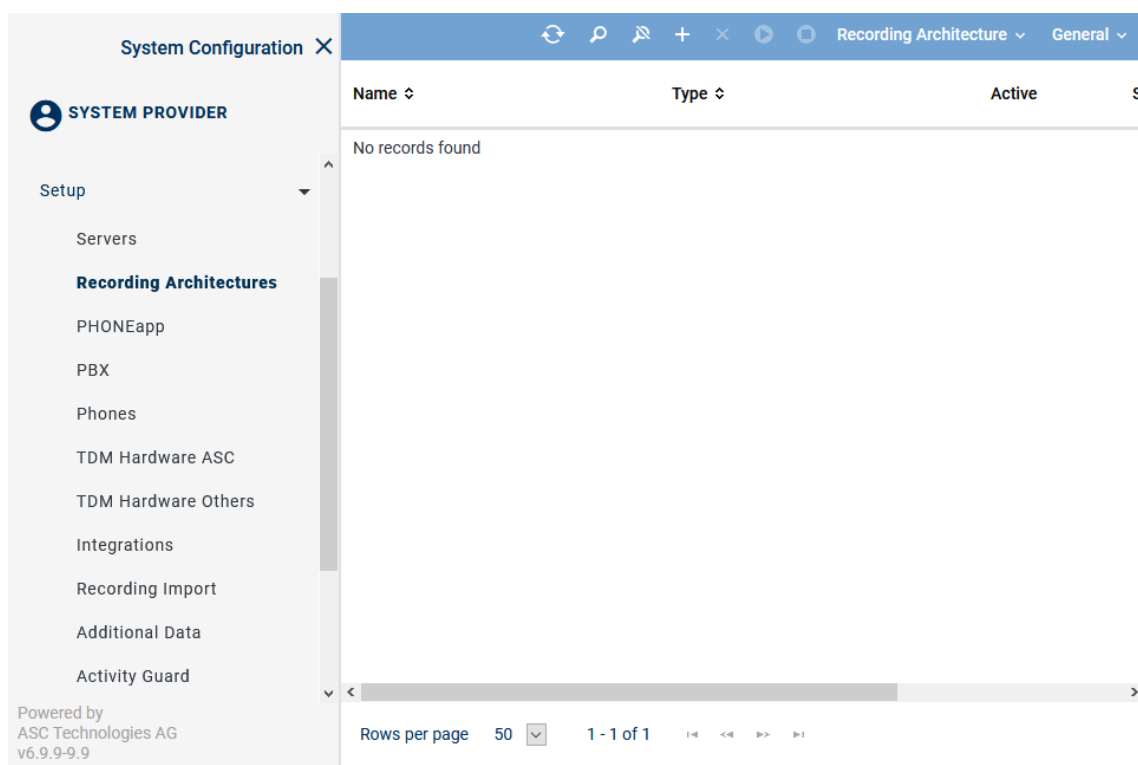




Fig. 250: Recording architectures - main view

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. <div> ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div>
Standby Active	Shows whether the standby server is active for one or several recording components in the recording architecture. <div> ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined. </div>
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. 251: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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 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*.

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

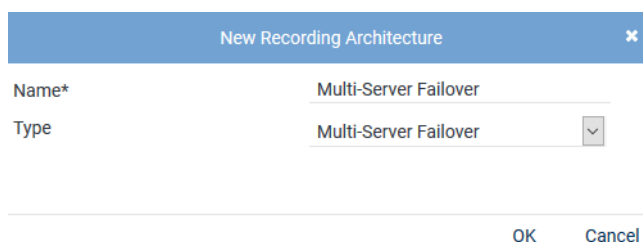


Fig. 252: Create recording architecture - Multi-Server Failover

- 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.

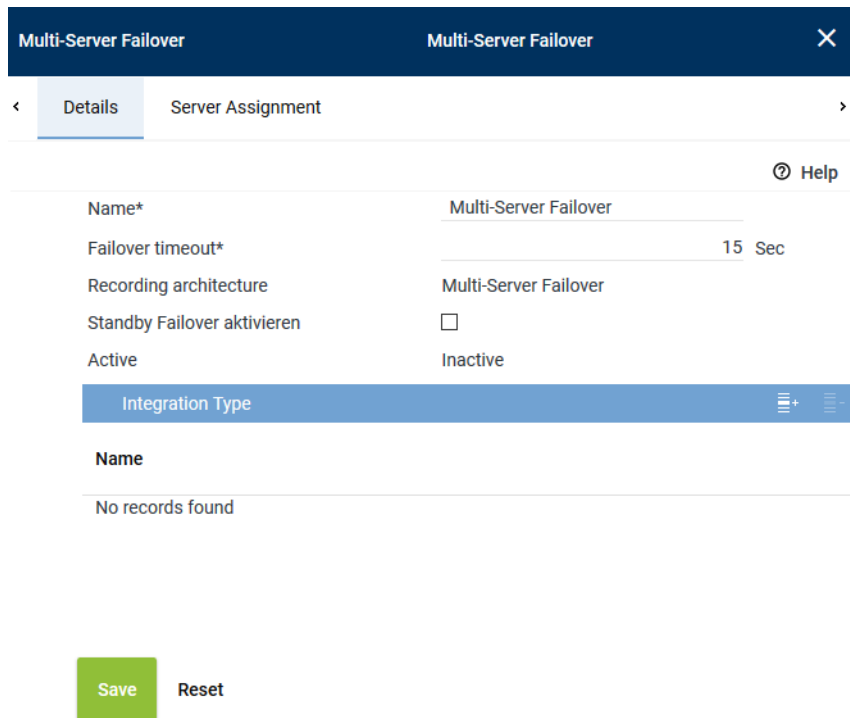


Fig. 253: Recording architecture - tab Details - Multi-Server Failover

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 Standby management for failover architectures.

<i>Failover timeout</i>	<p>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 <i>OK</i> within this time, then the failover process is not triggered.</p> <p>NOTICE! Check these parameters after an update and set the timeout to 15 seconds, if required.</p>
<i>Activate standby failover</i>	<p>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.</p> <p>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.</p> <p>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.</p>
<i>Active</i>	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.

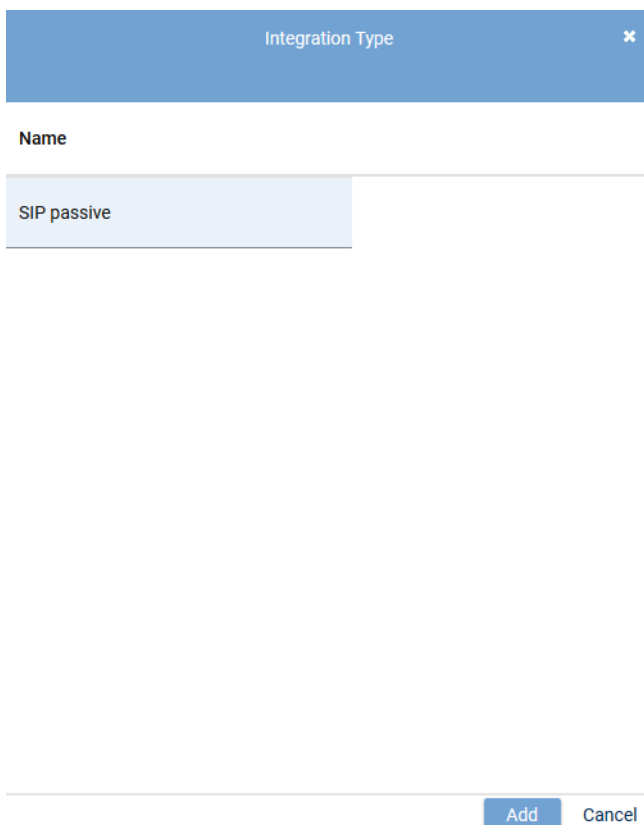


Fig. 254: Select integration type



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 passive* 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 view.

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 CTIconnect

In this group field, you can configure recording control You can configure two different server for this purpose or select the same server.

Multi-Server Failover
Multi-Server Failover
X

<
Details*
Server Assignment*
>

Recording Control and CTIconnect

Recording Control*	RC-01	+	-
Used in activated architecture	No		
CTIconnect*	RC-01	+	-
Used in activated architecture	No		

Standby Server

Recording Control standby*	RC-02	+	-
Used in activated architecture	No		
CTIconnect standby*	RC-02	+	-
Used in activated architecture	No		

Recording Server

<
Recording Server
+
-

Server ↕	Standby ↕
REC-01	REC-02

Save
Reset

Fig. 255: Recording Architecture - tab Server Assignment


- Click on the button **+** behind the entry field *Recording control*.
⇒ The window *Servers* appears.

Servers		
Name ↕	IP Address ↕	Path ↕
RC-02	192.168.173.176	C:\
REC-01	192.168.173.171	C:\
REC-04	192.168.173.174	C:\
REC-02	192.168.173.172	C:\
RC-01	192.168.173.175	C:\
CTI-01	192.168.173.177	C:\
CTI-02	192.168.173.178	C:\

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 256: 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 *CTIconnect module* in the entry field *CTIconnect*.

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:

Multi-Server Parallel Recording

Multi-Server Parallel Recording

×

<

Details*

Device Group 1*

Device Group 2*

>

Recording Control and CTIconnect

▼

Recording Control device group 1*	RC-01	+	-
Used in activated architecture	No		
CTIconnect device group 1*	CTI-01	+	-
Used in activated architecture	No		

Recording Server

▼

<

Recording Server

+

✎



⋮

Server ↕	Standby ↕
REC-01	REC-02

Save



Reset

Fig. 257: Add Recording Server




- 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.
- 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.
- 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.



- Click on the button *OK* to close the window.
 - ⇒ The name of the server now appears in the detail view.
- To edit the assignment subsequently, click on the icon . To delete an assignment, click on the icon .
- If you would like to add further recording servers, repeat the steps described above.

Activate recording architecture

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

Recording Architecture ▾ General ▾			
Name ▾	Type ▾	Active ▾	Standby active ▾
Multi-Server Failover	Multi-Server Failover	✓	✗

Fig. 258: Recording architecture - activate recording architecture

- 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 Standby Management.



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.

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

System Configuration X		Servers ▾ General ▾	
SYSTEM PROVIDER		Name ▾	IP Address ▾
Setup		CTI-01	192.168.173.177
Servers		CTI-02	192.168.173.178
Recording Architectures		RC-01	192.168.173.175
PHONEapp		RC-02	192.168.173.176
PBX		REC-01	192.168.173.171
Phones		REC-02	192.168.173.172
TDM Hardware ASC		REC-03	192.168.173.173
TDM Hardware Others		REC-04	192.168.173.174
Integrations			
Recording Import			
Additional Data			
Activity Guard			

Fig. 259: 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.

<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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.

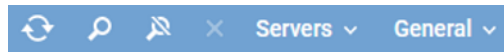







Fig. 260: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 235 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

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

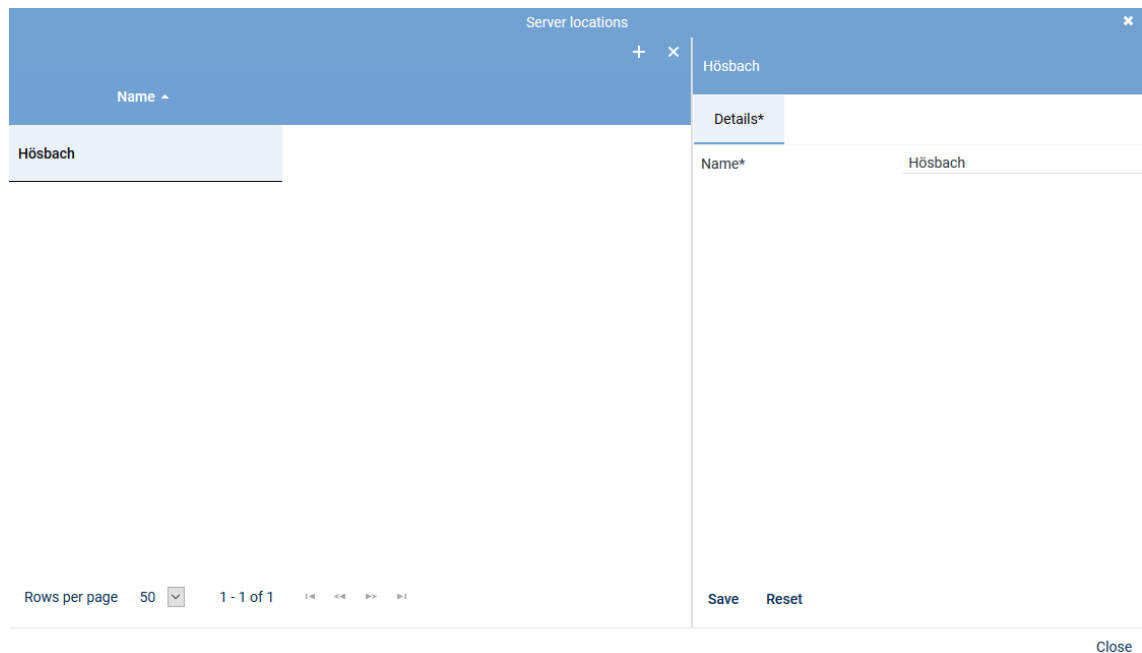



Fig. 261: Add server locations

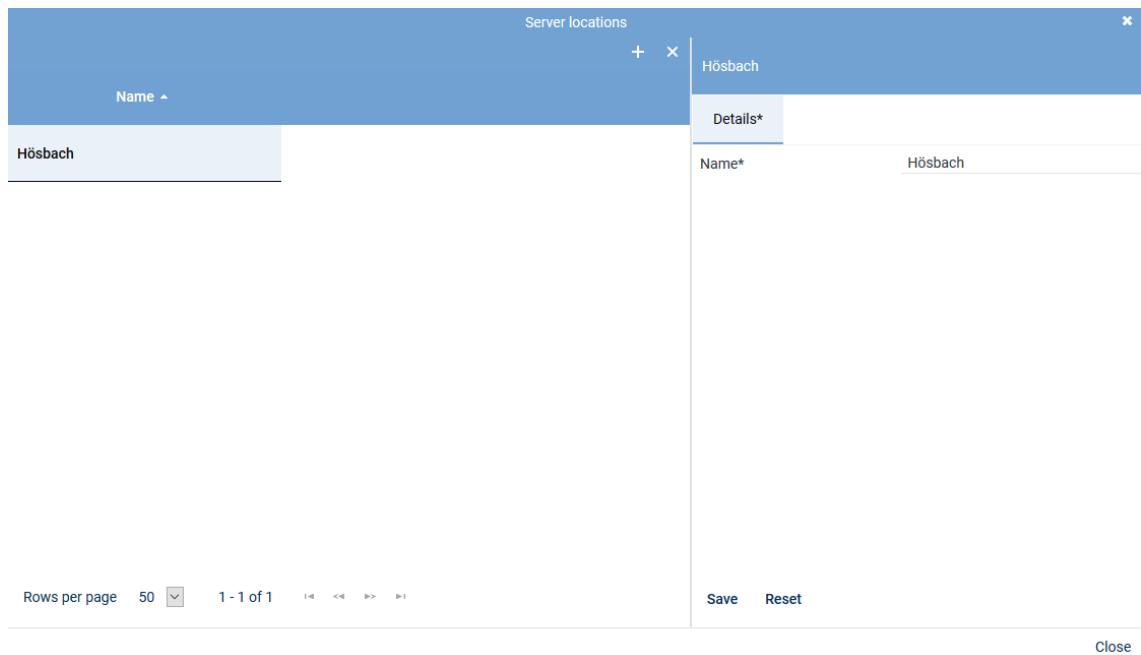
- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.
- To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
- To add further locations, repeat the last 3 steps.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

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



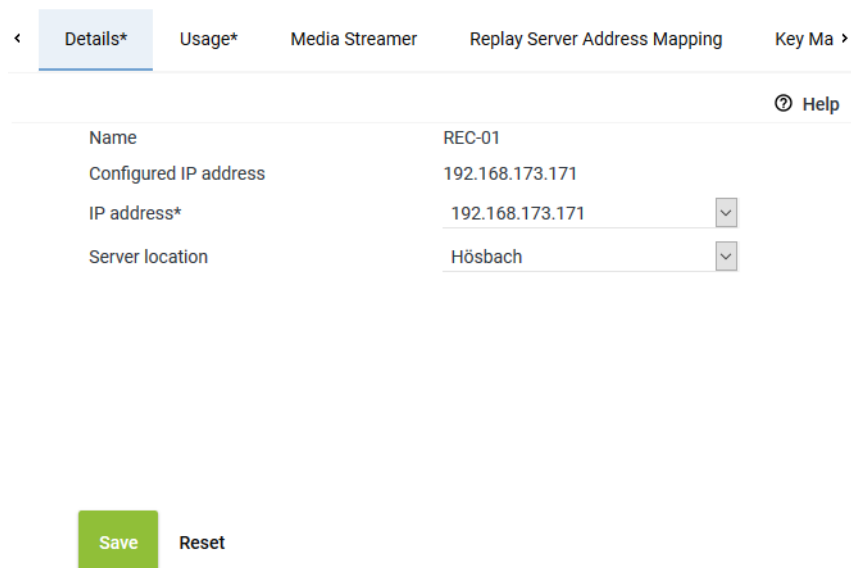
The screenshot shows a window titled "Server locations" with a close button (x) in the top right. Inside, there's a table with a header "Name" and one row containing "Hörsbach". To the right of the table is a "Details*" tab. Below the table, there's a pagination bar showing "Rows per page 50" and "1 - 1 of 1". At the bottom right of the window, there are "Save" and "Reset" buttons, and a "Close" button outside the window frame.

Fig. 262: 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.



The screenshot shows a window titled "Servers - tab Details" with a close button (x) in the top right. The window has a tabbed interface with "Details*" selected. Below the tabs, there's a "Help" icon. The main content area contains a table with the following fields:

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171 
Server location	Hörsbach 

At the bottom left, there are "Save" and "Reset" buttons.

Fig. 263: 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.

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

Tab Usage

- 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.

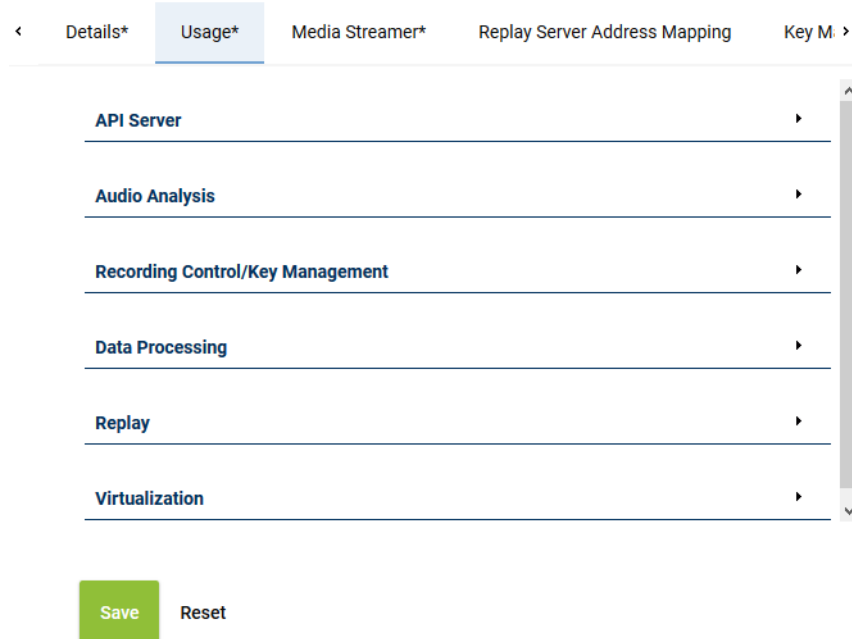


Fig. 264: Servers - tab usage

Group field API Server

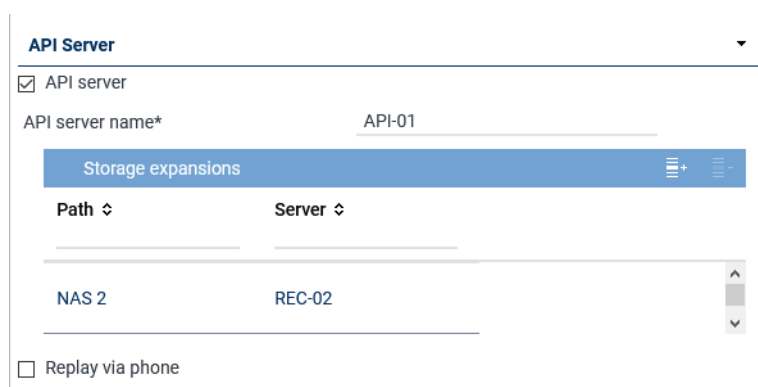




Fig. 265: Group field API Server

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.

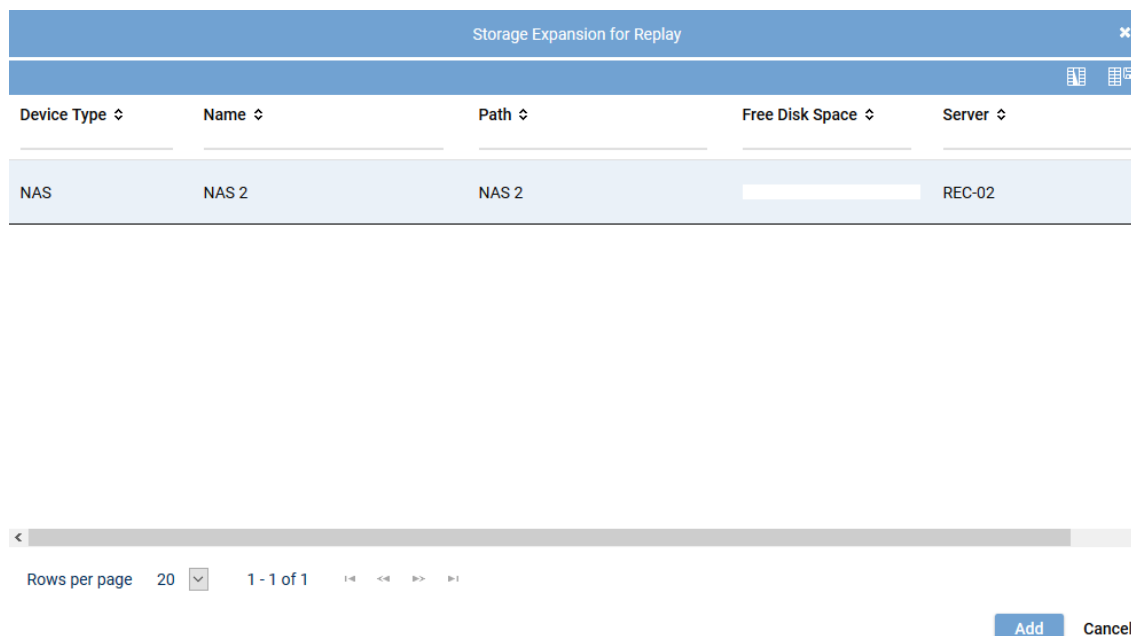
Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

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

Parameter	Value/Description
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 248.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 240. • By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list. <p>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.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 247. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.



Device Type	Name	Path	Free Disk Space	Server
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 266: 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




Audio Analysis

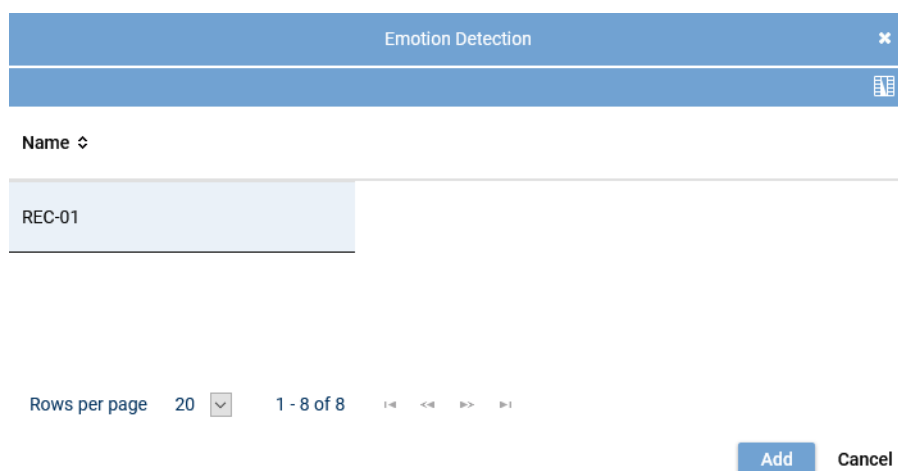
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 267: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis. <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function. <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> 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. 62: Configure audio analysis



Emotion Detection

Name ↕

REC-01

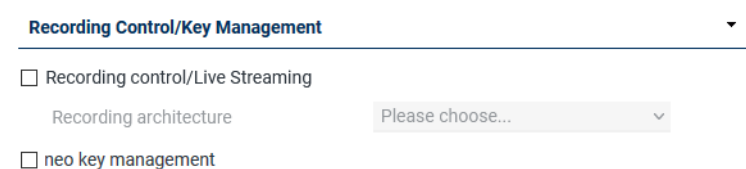
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 268: Select server for emotion detection

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

Group field Recording Control/Key Management



Recording Control/Key Management

☒ Recording control/Live Streaming

Recording architecture Please choose...

☐ neo key management

Fig. 269: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 63: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start 0:00 ▼

End 4:00 ▼

Receives data from

Only Replay

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server Please choose... ▼

☒ Import

Recording architecture All-in-one Basic ▼

Fig. 270: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 244. By clicking on the icon  (Remove), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 244. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <i>Replay server</i> 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. <p>NOTICE! For the export from Neo to Neo, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <i>Recording architecture</i> 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. 64: 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.



Name	IP Address
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173

Rows per page: 20 | 1 - 6 of 6 | Add | Cancel

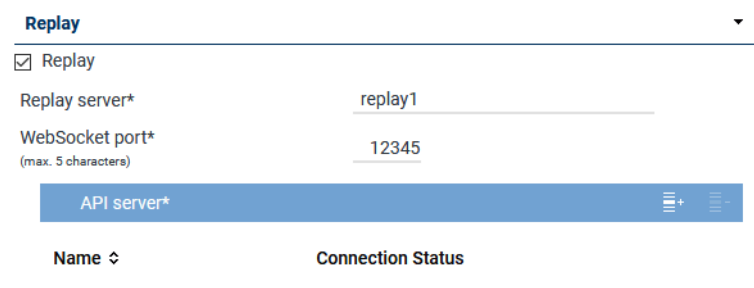
Fig. 271: Select server



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





Replay

☒ Replay

Replay server*



WebSocket port*
(max. 5 characters)

API server*  

Name	Connection Status
------	-------------------

Fig. 272: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . 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
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 245. • By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 65: 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.

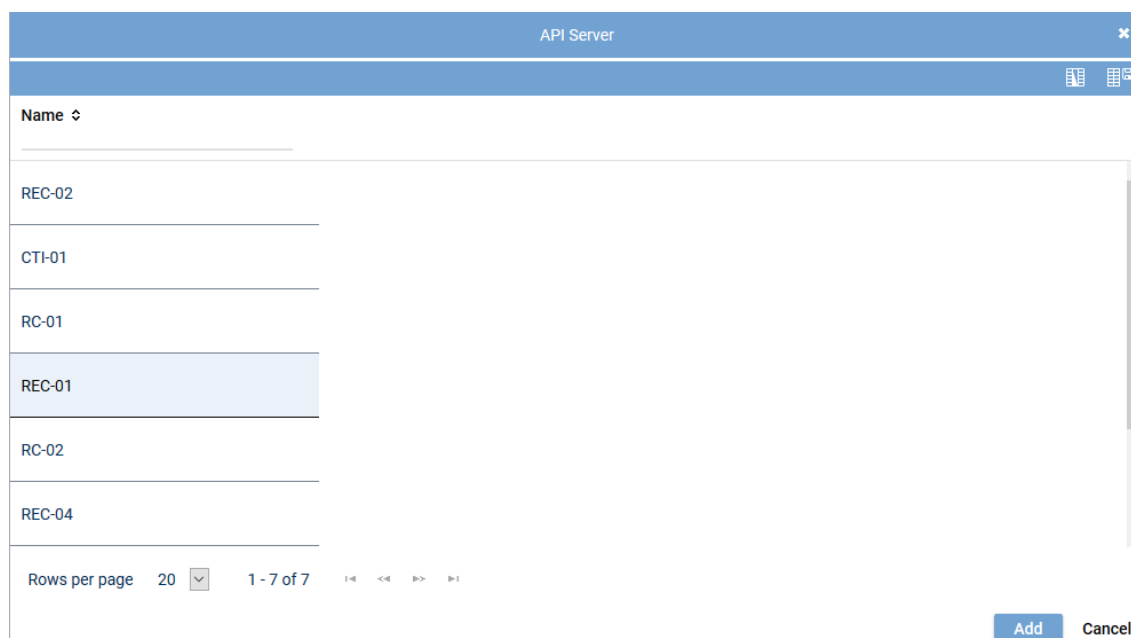


Fig. 273: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 238](#).

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. 274: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <code>TRUSTED_VIRTUALIZATION</code> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <code>licensing.asc.de</code> If you enter this domain, there is no key management.

Parameter	Value/Description
	<ul style="list-style-type: none"> <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 66: Configure virtualization



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.

- 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

- 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*.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

PBX +

PBX	PBX	<input type="button" value="v"/>
Extension*	123456	
<small>(max. 18 characters)</small>		
Media streamer IP address*	192.168.169.192	<input type="button" value="v"/>
Minimum port	24000	
Maximum port	24099	
Transport protocol	UDP	<input type="button" value="v"/>
SIP signaling port	5062	
User name		
Password		
PBX IP address		
PBX port	5060	
Registration required	<input checked="" type="checkbox"/>	
SIP registration expiration	3600	Second(s)

Save

Reset

Fig. 275: Servers module - tab Media Streamer

- 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.
------------	--

	<p>If no PBX has been created in the system yet, you can create a PBX via the blue bar <i>PBX</i>, see chapter "Create PBX", p. 253.</p>
<i>Extension</i>	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

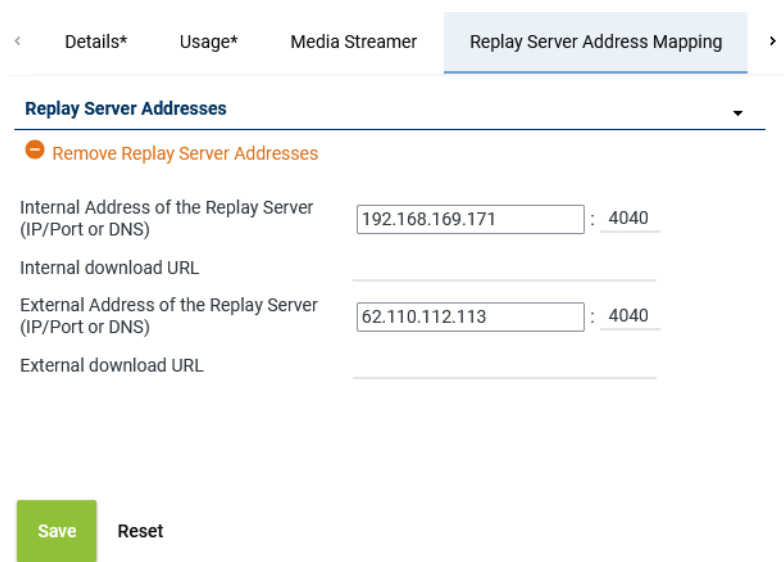



Fig. 276: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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.

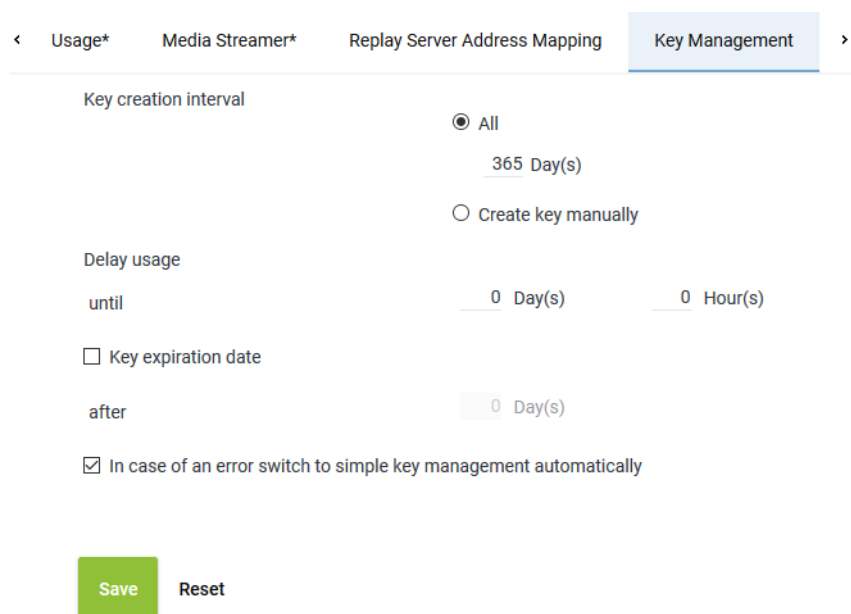


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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*.



< Usage* Media Streamer* Replay Server Address Mapping **Key Management** >

Key creation interval

☒ All
365 Day(s)

☐ Create key manually

Delay usage

until 0 Day(s) 0 Hour(s)

☐ Key expiration date

after 0 Day(s)

☒ In case of an error switch to simple key management automatically

Save Reset

Fig. 277: 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.

<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p> <p>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo key management does not work (e. g. if the service <i>DongleMan</i> 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.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = 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 <i>Usage</i>.</p>



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*

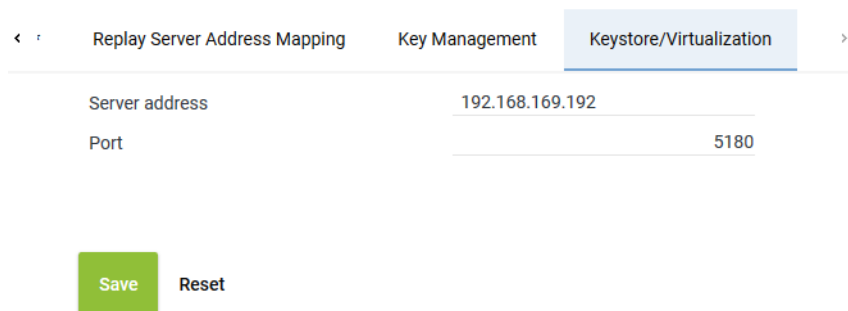
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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.



The screenshot shows a configuration window with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is active. It contains two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. Below the fields are two buttons: 'Save' (green) and 'Reset' (gray).

Fig. 278: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management:
-----------------------	--

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	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*.

- 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.

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

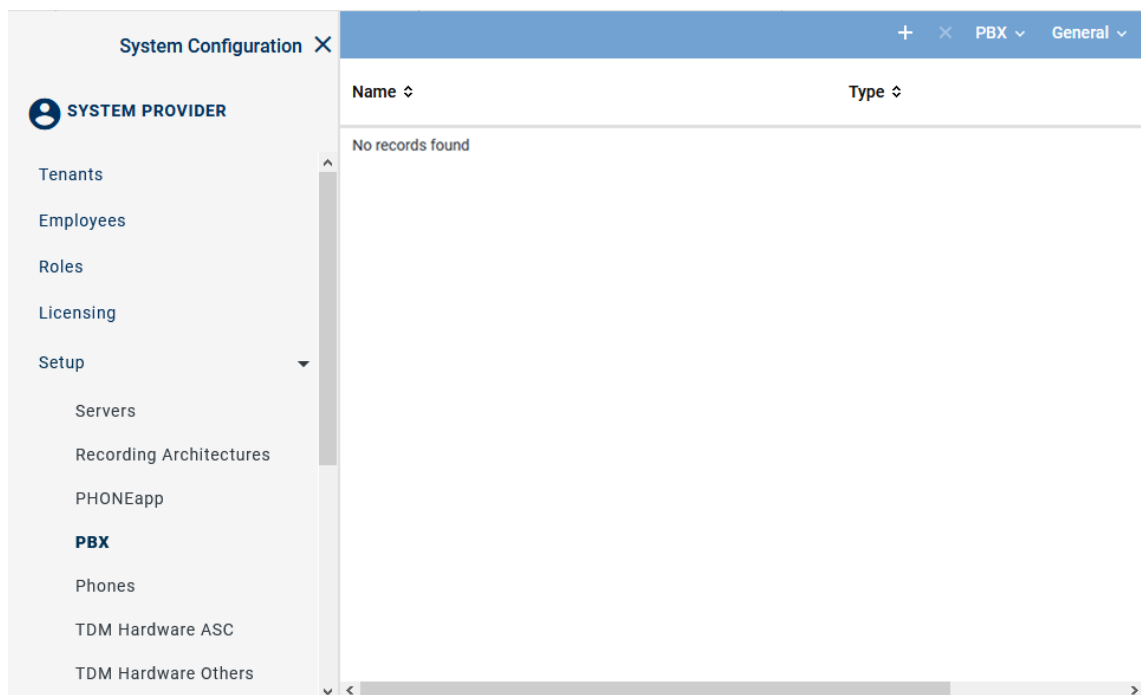


Fig. 279: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

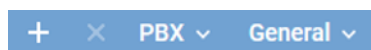




Fig. 280: Toolbar PBX module


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

<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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.

SIP
×

<
Details*
PHONEapp Configuration
Web Service
>

Name*

PBX type

Maximum length of extensions

Country code

Area code*

Net code*

SIP

Universal VoIP

4

☒ Select from list

United States (1)

☐ Enter manually

6021

5963

Non Phone IPs

No records found

Add
Delete

IPs to be Ignored

No records found

Add
Delete

MACs to be Ignored

No records found

Add
Delete

Save

Reset

Fig. 281: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 67: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.

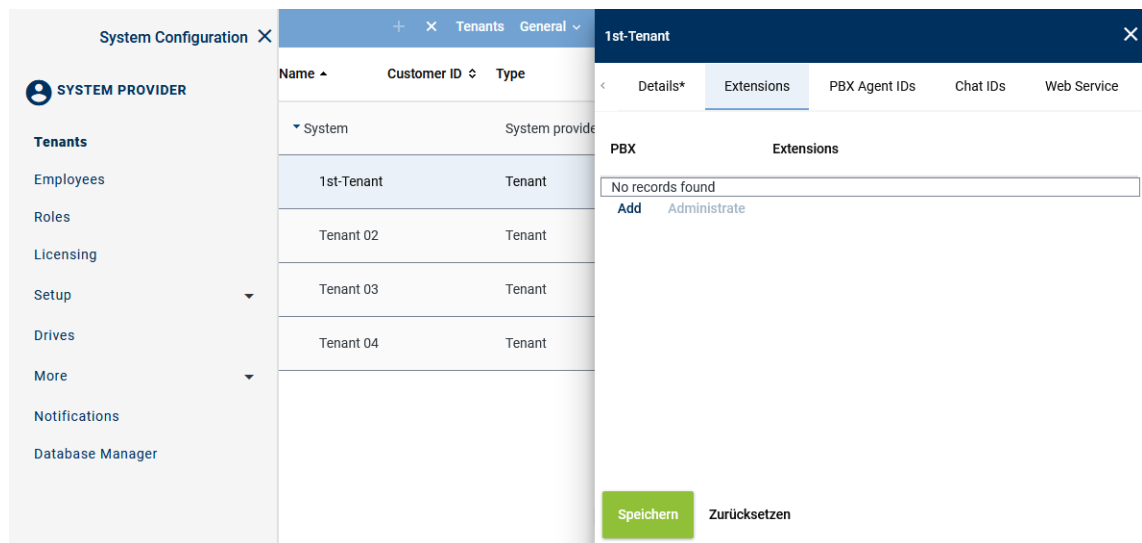


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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.



Name	Customer ID	Type
System		System provider
1st-Tenant		Tenant
Tenant 02		Tenant
Tenant 03		Tenant
Tenant 04		Tenant

Extensions

No records found

Add Administrate

Speichern Zurücksetzen

Fig. 282: 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:

Add Extensions ✕

PBX

PBX ▾

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

Extension or extension range separated by
", " or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 283: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> ZIP TXT CSV <p>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.</p>
<i>File contains a headline</i>	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
<i>File name</i>	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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 detected, 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.

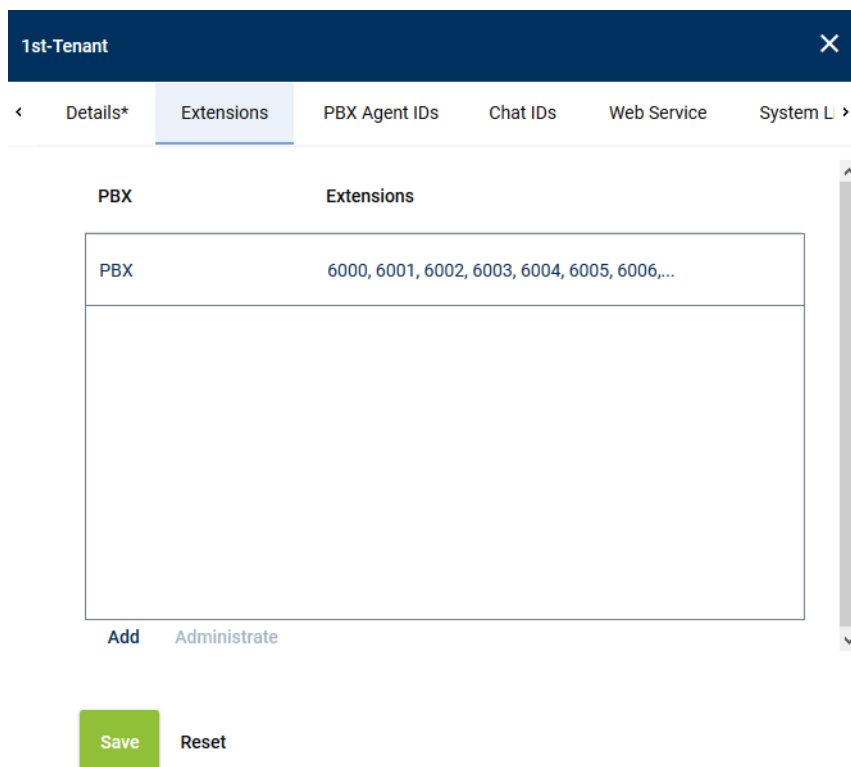


Fig. 284: Remove extensions

2. Click the button *Administrate*.

- 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. 285: Select extensions

- To remove the selected extensions, 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.

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

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

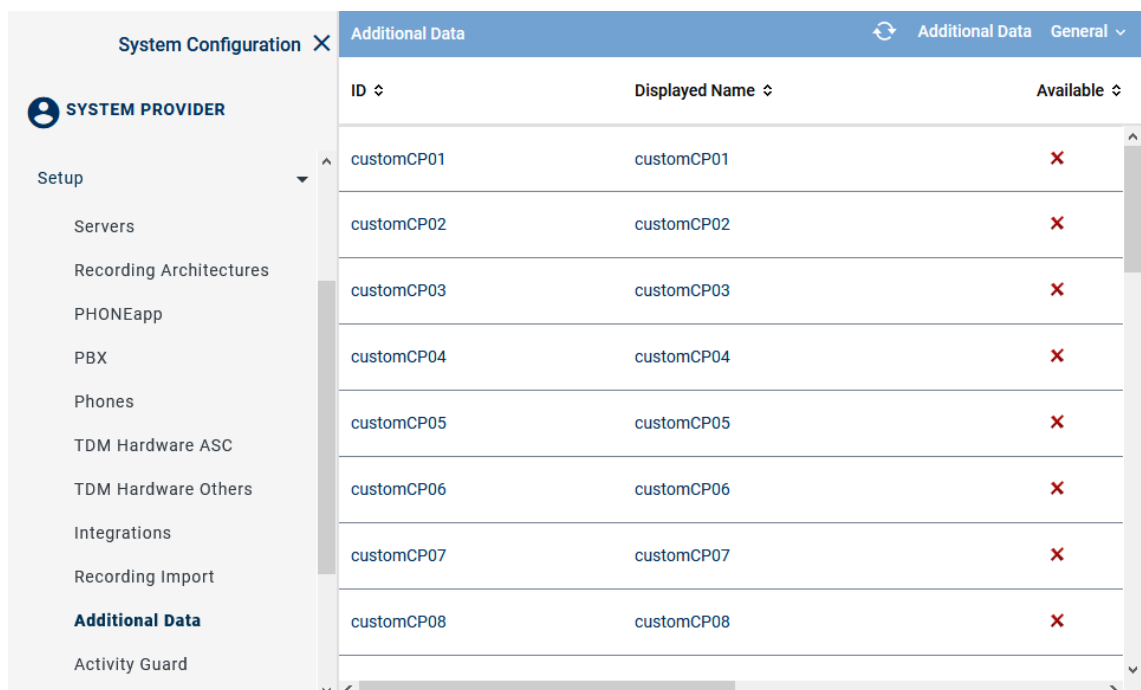


Fig. 286: Additional Data module main view

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

Change display name







Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 287: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 288: 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 an 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:

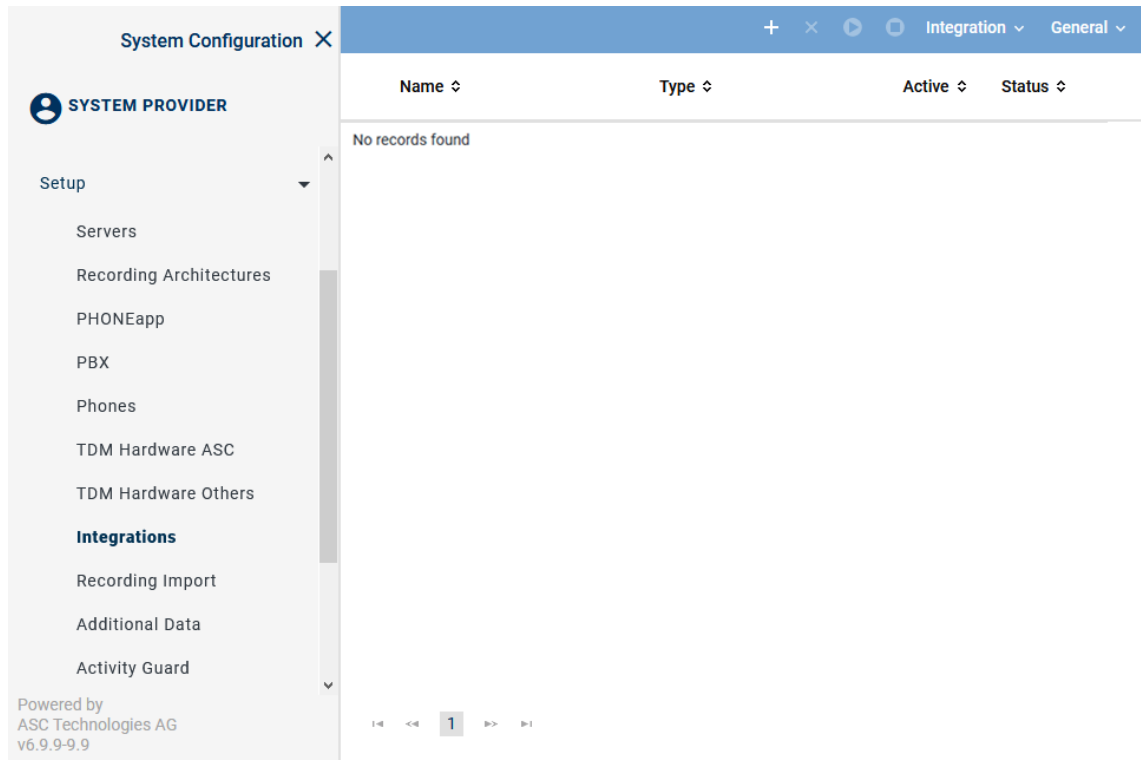




Fig. 289: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module


The toolbar offers the following functions.



Fig. 290: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

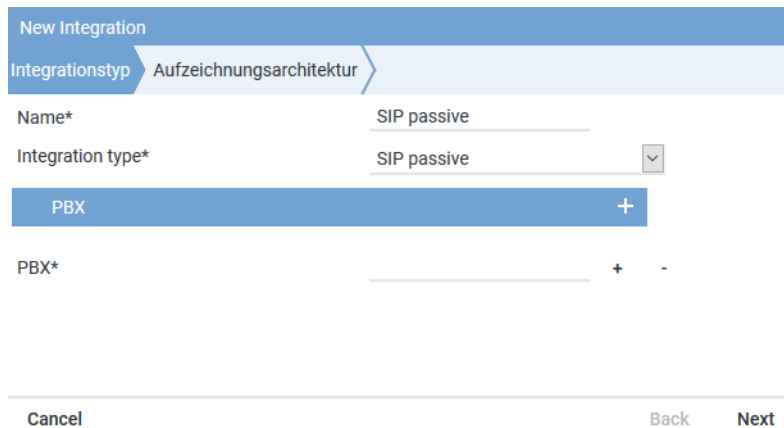



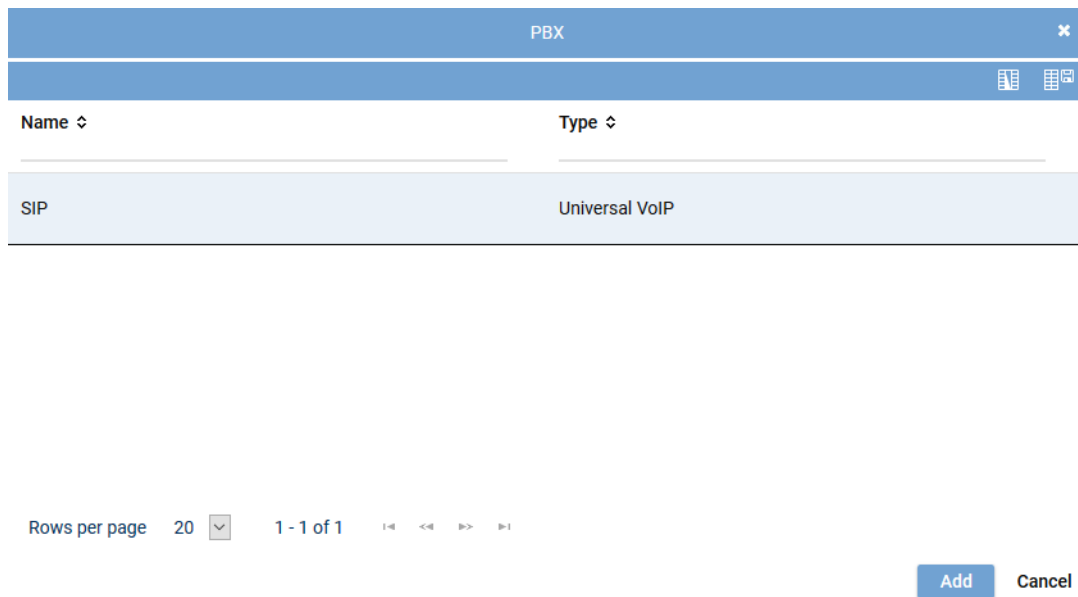
Fig. 291: Create integration type

- Enter the following parameters:

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

Tab. 68: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

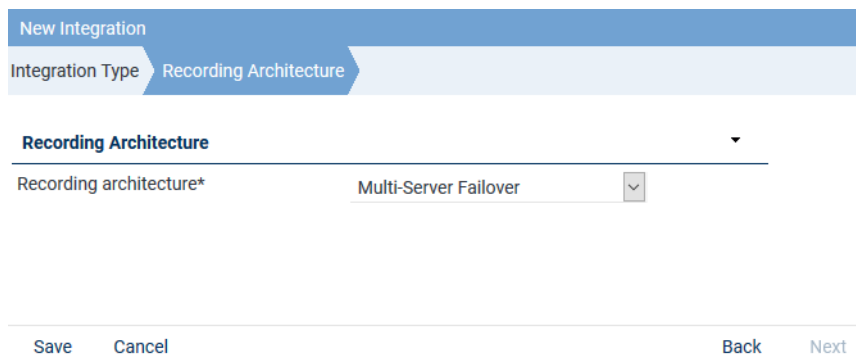
Add Cancel

Fig. 292: Integrations - 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.



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Failover

Save Cancel Back Next

Fig. 293: 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:






SIP passive		SIP passive	✗	⚙️
Step	Configuration			
Configure recording architecture	✓ 			
Configure recording servers	✗ 			
Configure add-on	✓ 			
Configure miscellaneous settings	✓ 			

Fig. 294: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture ✕

Details *


Recording architecture*

Save Cancel

Fig. 295: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.

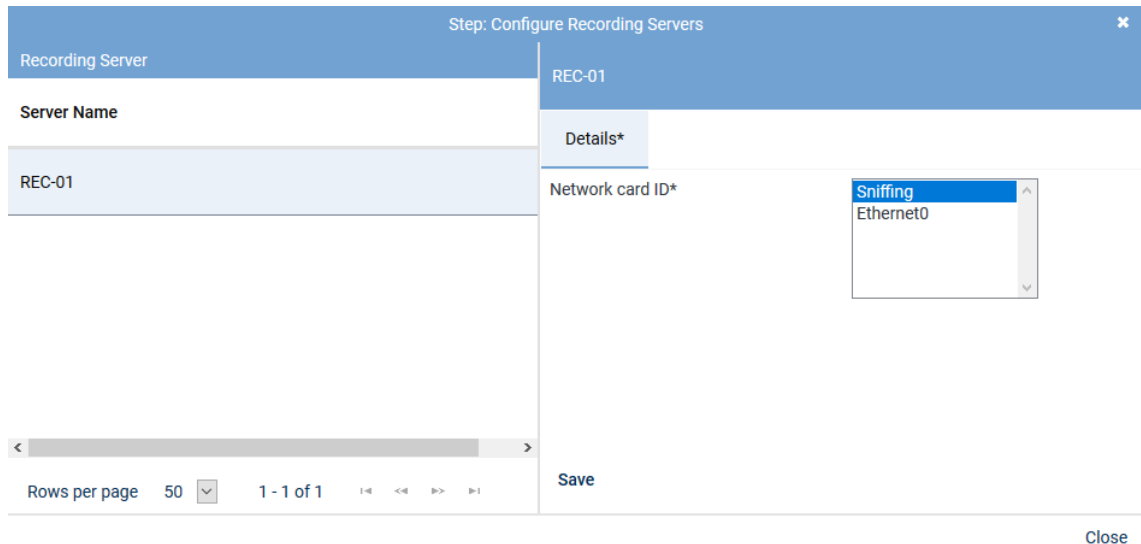


Fig. 296: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
<i>Network card ID</i>	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 69: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 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 CTIconnect 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.

CTIconnect for Genesys T-Server

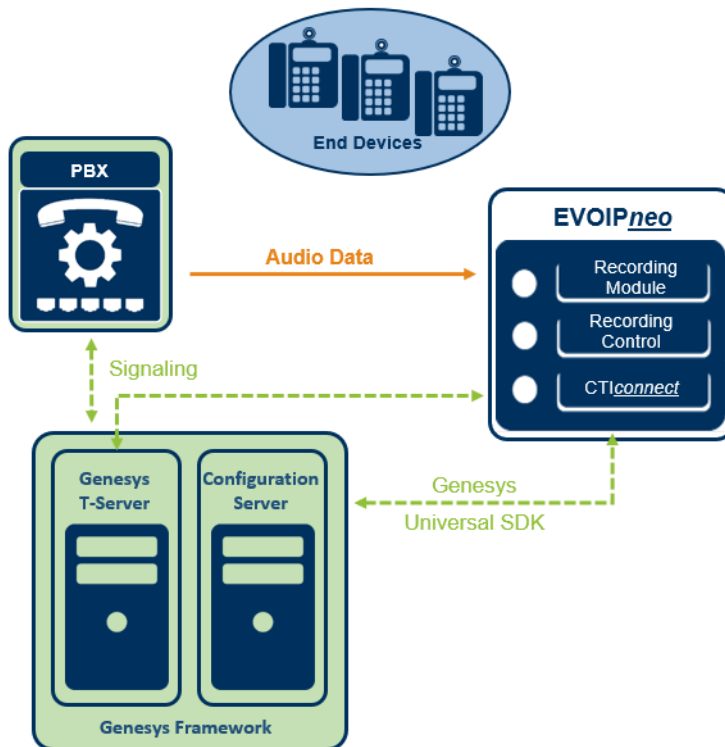


Fig. 297: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

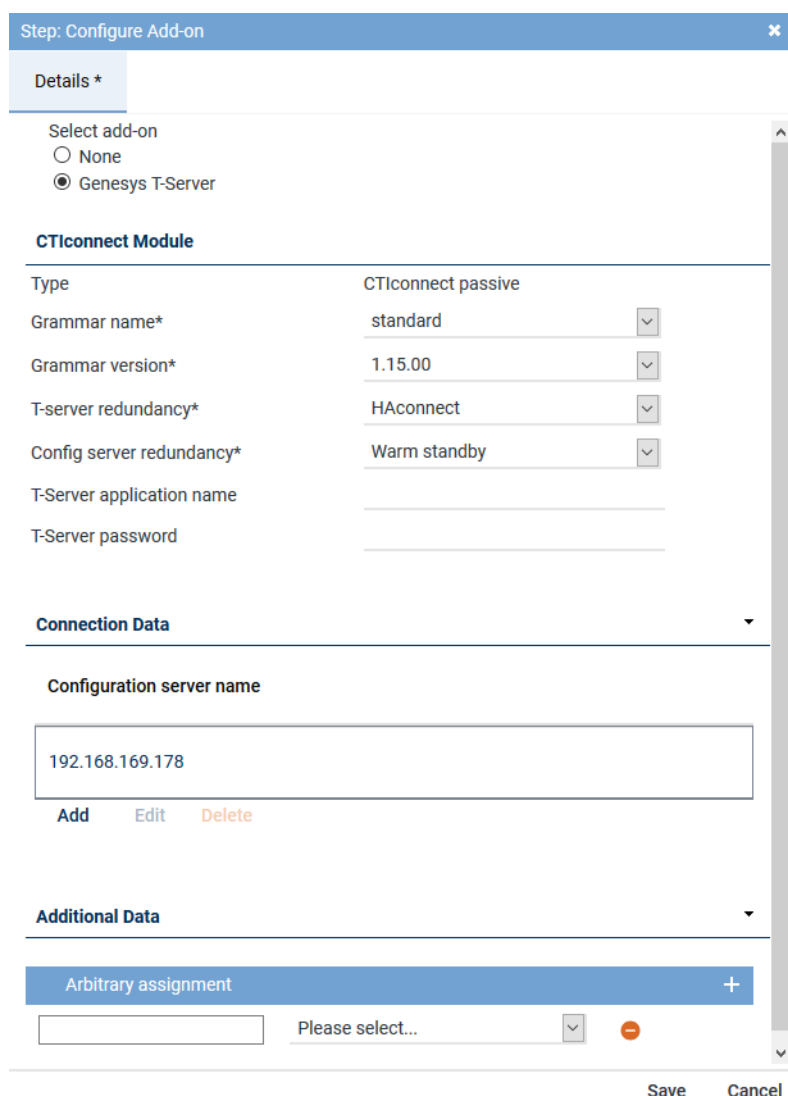
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name
192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment +

Please select...

Save Cancel

Fig. 298: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI <u>connect</u> 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.
<i>T-Server password</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI <u>connect</u> 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. 70: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 299: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 71: 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.

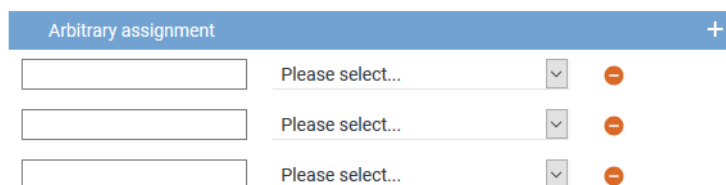



Fig. 300: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

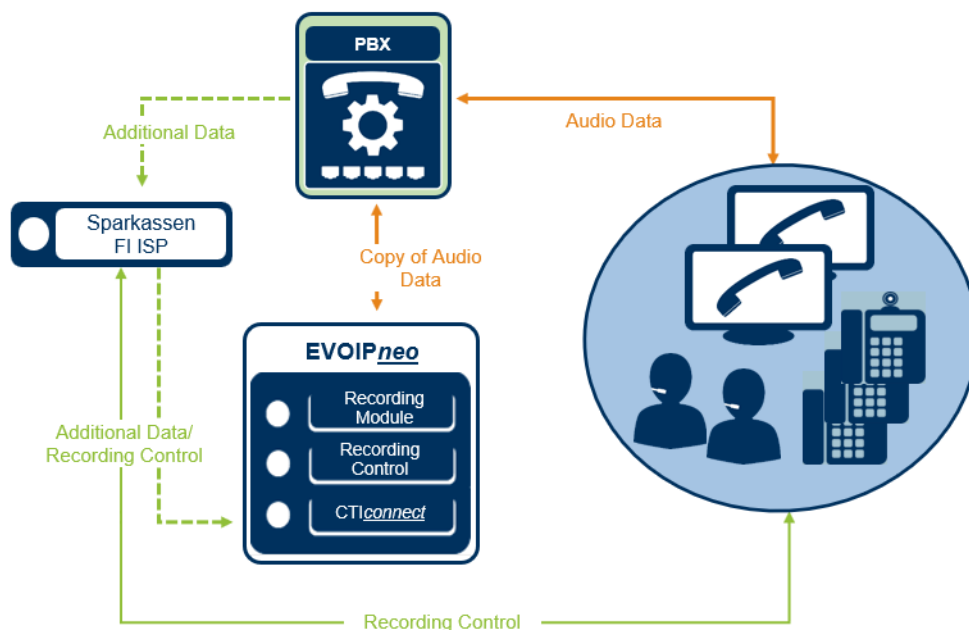



Fig. 301: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

<input style="width: 90%;" type="text"/>	Please select...	▼	⊖	
<input style="width: 90%;" type="text"/>	Please select...	▼	⊖	
<input style="width: 90%;" type="text"/>	Please select...	▼	⊖	

Save Cancel

Fig. 302: 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. 72: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 73: 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.

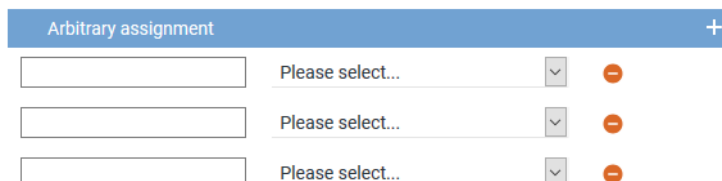



Fig. 303: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

Add Edit Delete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

Save Cancel

Fig. 304: Configure add-on for OSCC

Group field CTIconnect Module

- 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. 74: Configure CTIconnect module

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

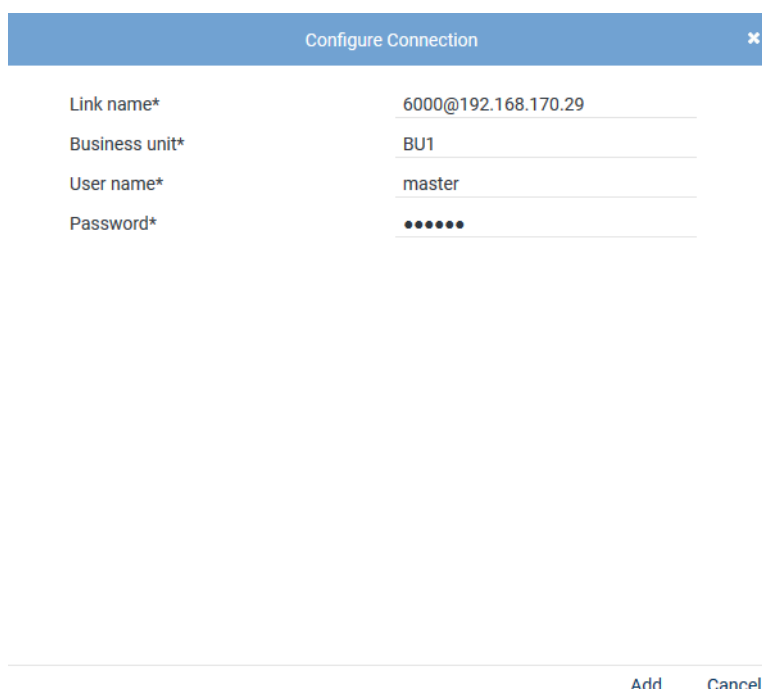


Fig. 305: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 75: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

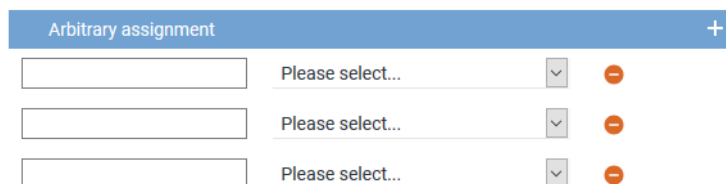





Fig. 306: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 307: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.













	SIP passive	SIP passive		
Step	Configuration			
Configure recording architecture	 			
Configure recording servers	 			
Configure add-on	 			
Configure miscellaneous settings	 			

Fig. 308: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✓	✓

Fig. 309: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ↕	Type ↕	Active ↕	Status ↕
⌵ SIP passive	SIP passive	✗	✓

Fig. 310: Deactivate integration

- 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.

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

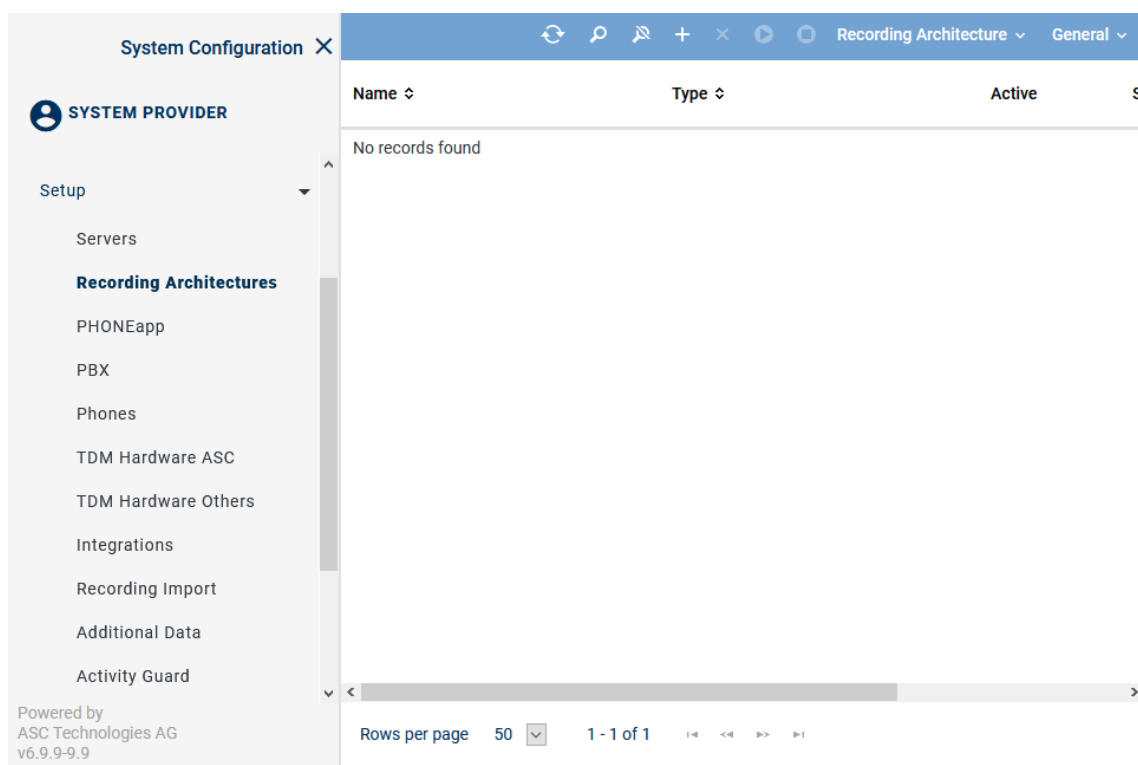




Fig. 311: Recording architectures - main view

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. 312: 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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	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.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	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.
<i>Recording Architecture</i>	<i>Standby Management</i>	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.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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 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*.

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

⇒ The window *New Recording Architecture* appears.

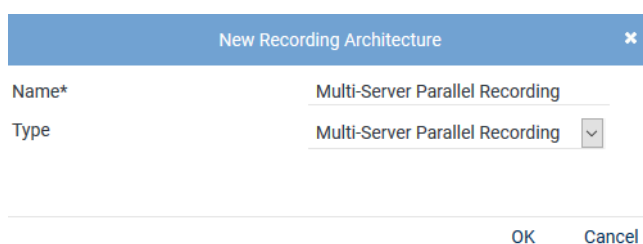


Fig. 313: Create recording architecture - Multi-Server Parallel Recording

- 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.

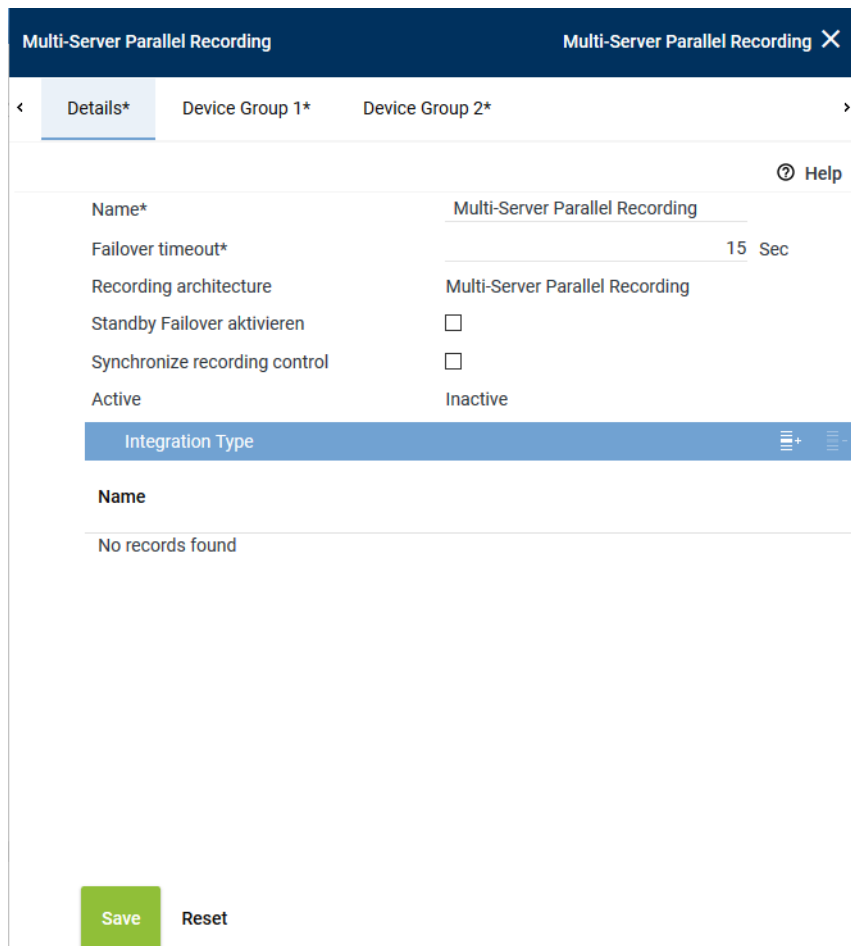


Fig. 314: Recording architecture - tab Details - Multi-Server Parallel Recording

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 Standby management for failover architectures.




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 Synchronization recording control.

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 method 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 Duplicates in parallel recording architectures.

Add integration type

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

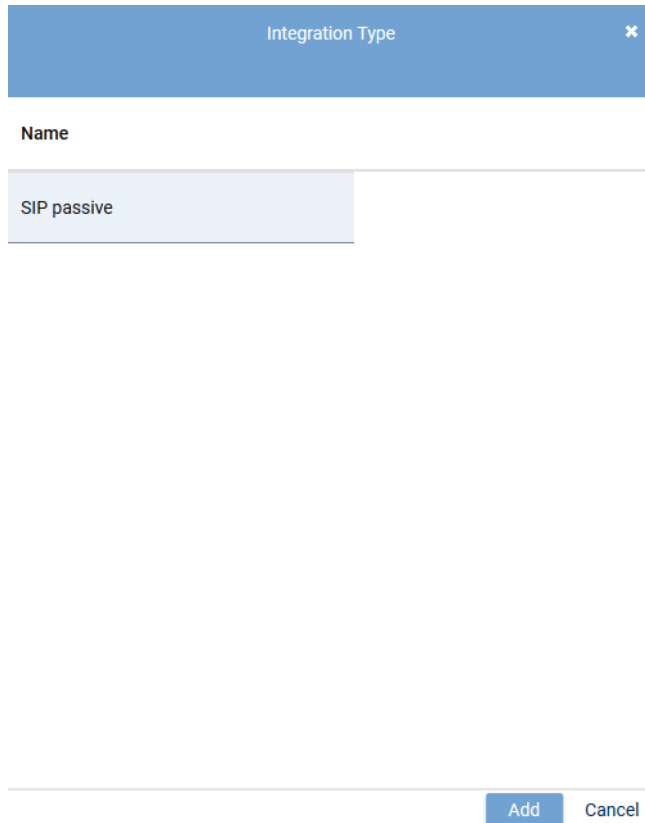


Fig. 315: Select integration type



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.

- Select *SIP passive* 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 view.

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

- 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 CTIconnect

In this group field, you can configure recording control. You can configure two different servers or the same server for this.

Multi-Server Parallel Recording

Multi-Server Parallel Recording

×

<

Details*

Device Group 1*

Device Group 2*

>

Recording Control and CTIconnect

▼

Recording Control device group 1*	RC-01	+	-
Used in activated architecture	No		
CTIconnect device group 1*	RC-01	+	-
Used in activated architecture	No		

Recording Server

▼

<

Recording Server

+

✎

⋮

Server ↕	Standby ↕
REC-01	REC-02

Save

Reset

Fig. 316: Recording architecture - server assignment device group 1

- Click on the button **+** next to the entry field *Recording Control* to assign a server.
⇒ The window *Servers* appears.

Servers			×
Name ↕	IP Address ↕	Path ↕	
RC-02	192.168.173.176	C:\	^
REC-01	192.168.173.171	C:\	
REC-04	192.168.173.174	C:\	
REC-02	192.168.173.172	C:\	
RC-01	192.168.173.175	C:\	
CTI-01	192.168.173.177	C:\	
CTI-02	192.168.173.178	C:\	▼

<

>

Rows per page

20

1 - 8 of 8

<<

<


>

>>

Add

Cancel

Fig. 317: 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 .




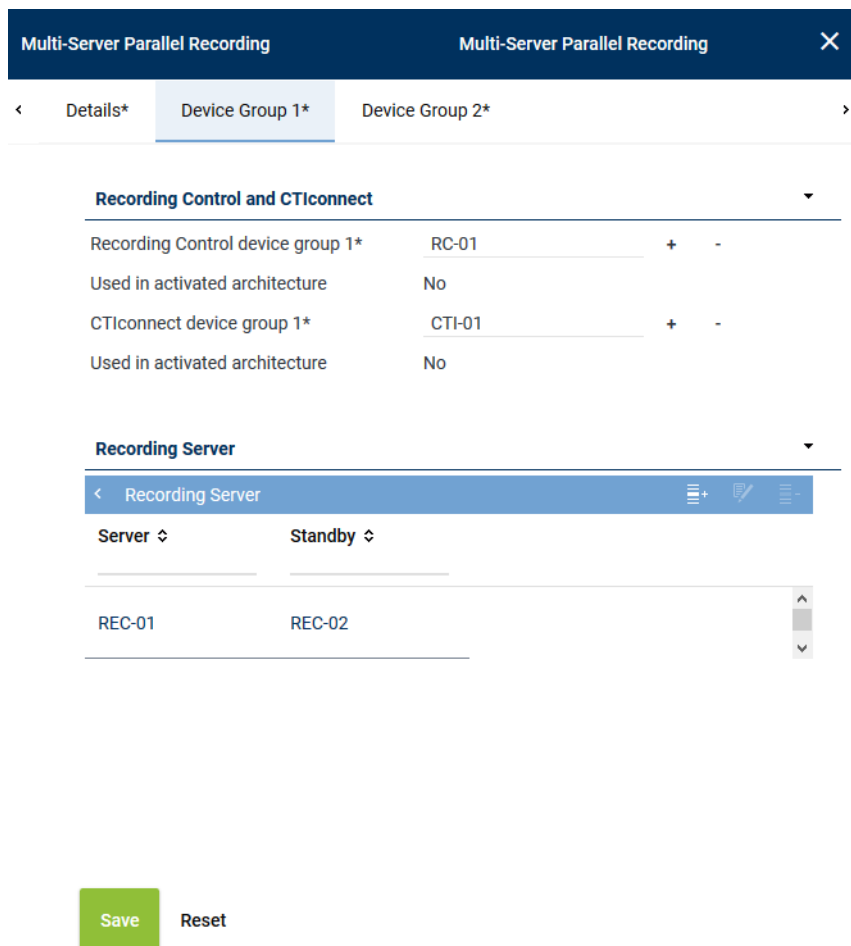
A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.

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 *CTIconnect module* in the entry field *CTIconnect*.

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:



Multi-Server Parallel Recording Multi-Server Parallel Recording X

< Details* Device Group 1* Device Group 2* >

Recording Control and CTIconnect



Recording Control device group 1*	RC-01	+	-
Used in activated architecture	No		
CTIconnect device group 1*	CTI-01	+	-
Used in activated architecture	No		



Recording Server

Server	Standby
REC-01	REC-02

Save Reset

Fig. 318: 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 tool-bar becomes active.
3. To activate the recording architecture, click on the icon  (*Activate*).
⇒ In the column *Active*, the icon  (*Active*) appears.










     Recording Architecture ▾ General ▾			
Name ▾	Type ▾	Active ▾	Standby active ▾
Multi-Server Parallel Recording	Multi-Server Parallel Recording		

Fig. 319: 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 [Configure duplicate detection](#).

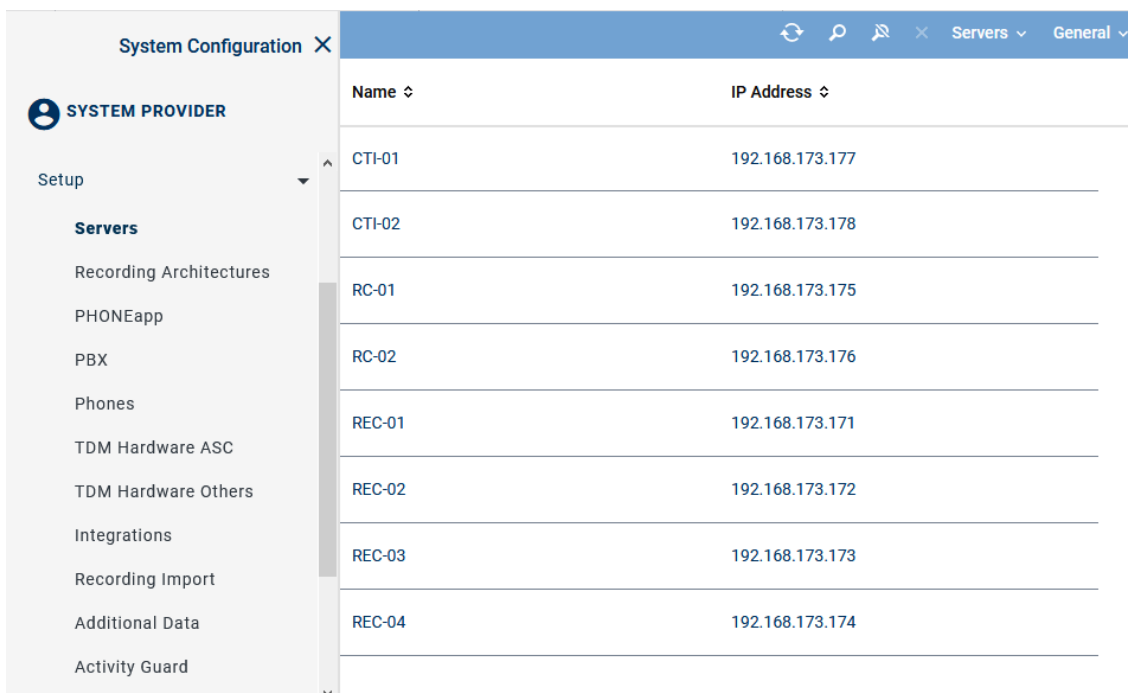


If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

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:



Name	IP Address
CTI-01	192.168.173.177
CTI-02	192.168.173.178
RC-01	192.168.173.175
RC-02	192.168.173.176
REC-01	192.168.173.171
REC-02	192.168.173.172
REC-03	192.168.173.173
REC-04	192.168.173.174

Fig. 320: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	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.

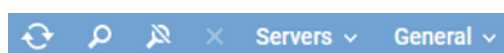







Fig. 321: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	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.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	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.

<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations" , p. 289.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

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

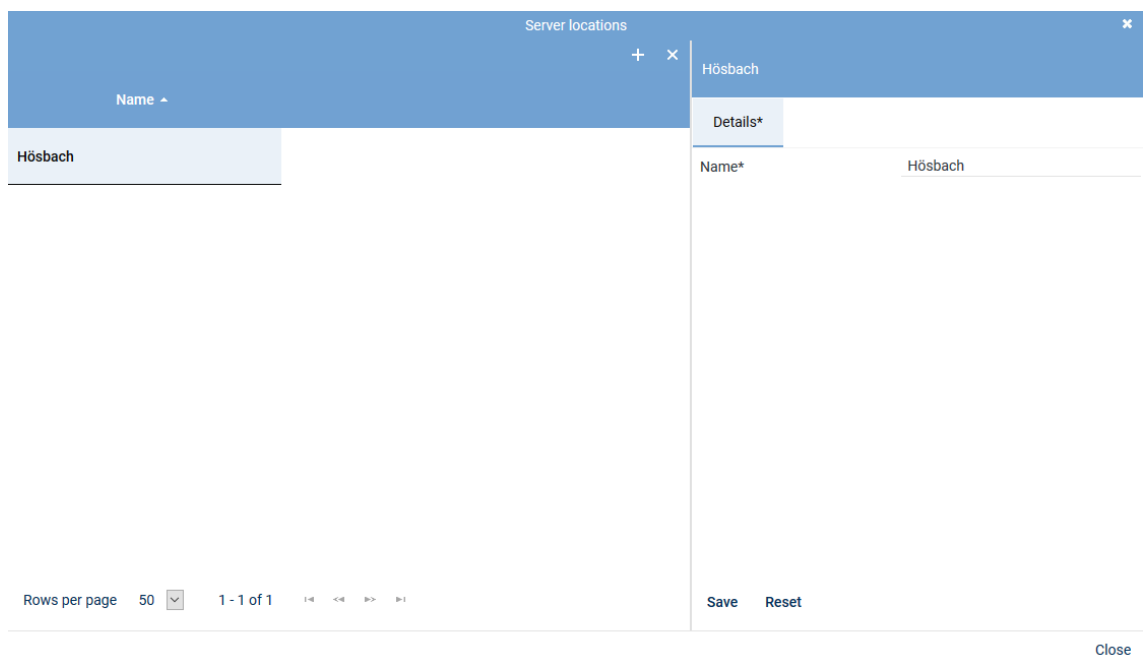



Fig. 322: Add server locations

- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.

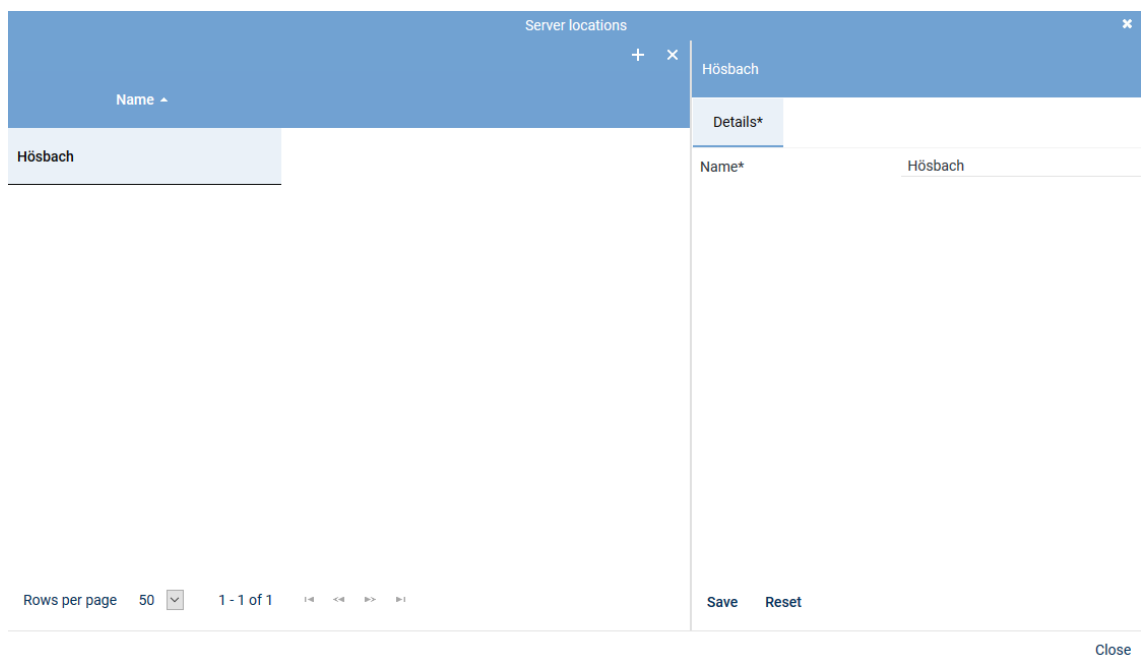
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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.



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a table with a header "Name" and a dropdown arrow. The table contains one row with the value "Hösbach". To the right of the table is a "Details*" tab. Below the table, there is a "Rows per page" dropdown set to "50" and a "1 - 1 of 1" indicator. At the bottom right of the window, there are "Save" and "Reset" buttons, and a "Close" button at the very bottom right.

Fig. 323: 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.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
Key Ma >

? Help

Name	REC-01
Configured IP address	192.168.173.171
IP address*	192.168.173.171 <input type="button" value="v"/>
Server location	Hörsbach <input type="button" value="v"/>

Fig. 324: Servers - tab Details

- From the drop-down list, select the IP address which is supposed to be used as default address of the server in the system.
- Select the *Server location* in the drop-down list. The drop-down list displays all locations which have been created in the location management.
- Click on the button **Save** if the entries are correct.

Tab Usage

- 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.

<
Details*
Usage*
Media Streamer*
Replay Server Address Mapping
Key M. >

API Server	▶
Audio Analysis	▶
Recording Control/Key Management	▶
Data Processing	▶
Replay	▶
Virtualization	▶

Fig. 325: Servers - tab usage

Group field API Server

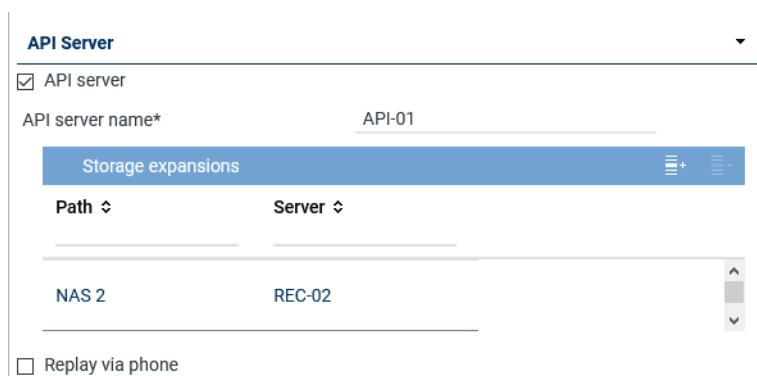




Fig. 326: Group field API Server

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
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>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 <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 302.</p>
<i>API server name</i>	<p>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.</p> <p>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.</p>
<i>List Storage expansions</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 293. By clicking on the icon  (<i>Remove</i>), 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.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, 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.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 300. To be able to do so, at least 1 PBX must have been configured in the system.</p>

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.

Storage Expansion for Replay				
Device Type	Name	Path	Free Disk Space	Server
NAS	NAS 2	NAS 2	<div></div>	REC-02

Rows per page: 20 1 - 1 of 1

Add Cancel

Fig. 327: Select storage expansion

- 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

Audio Analysis

☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 328: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> 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. 76: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

Rows per page 20 ▼ 1 - 8 of 8 ⏪ <⏪ ⏩ ⏭

Add Cancel

Fig. 329: Select server for emotion detection

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

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☐ Recording control/Live Streaming

Recording architecture Please choose... ▼

☐ neo key management

Fig. 330: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live streaming</i>	This recording solution does not support external recording control.
<i>Neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 77: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 331: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list</p>

Parameter	Value/Description
	<p><i>Target Server</i> 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.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 297. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 297. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>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.</p> <p>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.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p>

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*


(max. 5 characters)


API server*

+
 -

Name ↕	Connection Status
--------	-------------------

Fig. 333: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. 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.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>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 <i>Replay server</i>. 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.</p> <p>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.</p> <p>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 <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List API server</i>	<p>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.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 299.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (Remove), you can remove selected API servers from the list.

Tab. 79: 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.
- To assign an [API](#) server, click on the icon  (Add) in the toolbar of the list *API Server*.
 - Select the server from the list on which the [API](#) service is running.



Fig. 334: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 292](#).

- 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

Virtualization

☐ VM without Trusted License

Fig. 335: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> • <i>licensing.asc.de</i> If you enter this domain, there is no key management. • <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.

Tab. 80: Configure virtualization



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*.

[Details*](#)
[Usage*](#)
[Media Streamer*](#)
[Replay Server Address Mapping](#)
[Key M. >](#)

PBX
+

PBX	PBX ▼
Extension* <small>(max. 18 characters)</small>	123456
Media streamer IP address*	192.168.169.192 ▼
Minimum port	24000
Maximum port	24099
Transport protocol	UDP ▼
SIP signaling port	5062
User name	
Password	
PBX IP address	
PBX port	5060
Registration required	<input checked="" type="checkbox"/>
SIP registration expiration	3600 Second(s)

Save
Reset

Fig. 336: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>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. 306.</p>
Extension	<p>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.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>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.</p> <p>NOTICE! The port range must not have less than 64 ports.</p>

<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

<
Details*
Usage*
Media Streamer
Replay Server Address Mapping
>

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) : 4040

Internal download URL

External Address of the Replay Server (IP/Port or DNS) : 4040

External download URL


Save
Reset

Fig. 337: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server can be reached.
<i>Internal download URL</i>	Enter the URL under which the replay server can be reached internally, e. g.: <code>https://example.company.com/</code>
<i>External address of the replay server (IP/Port or DNS)</i>	Enter either the IP address and the port or the DNS name under which the replay server 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.
<i>External download URL</i>	Enter the URL under which the replay server can be reached via the browser from outside the local network, e. g.: <code>https://example.company.com/</code> 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 button  in the title bar of the group field.



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

< Usage* Media Streamer* Replay Server Address Mapping
Key Management >

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage

until

0 Day(s)

0 Hour(s)

☐ Key expiration date

after

0 Day(s)

☒ In case of an error switch to simple key management automatically

Save

Reset

Fig. 338: Servers module - tab Key Management

<i>Key creation interval</i>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> • <i>All</i> 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 • <i>Create key manually</i> Select that a key is supposed to be generated manually. <p>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.</p>
<i>Delay usage</i>	<p>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.</p> <p>Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = 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.</p>

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.

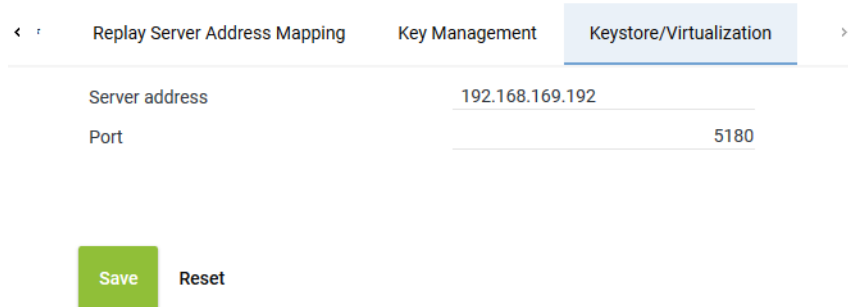


Fig. 339: Servers module - tab Keystore/Virtualization

<i>Server address</i>	<p>Enter the address of the server for the connection.</p> <ul style="list-style-type: none"> • If you use the hardware with neo key management: IP address of the server where the service <i>DongleMan</i> has been installed. • If you use the VM with dongle without neo key management: IP address of the server where the service <i>DongleMan</i> 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: <i>licensing.asc.de</i> • If you use the VM with <i>TRUSTED_VIRTUALIZATION</i> license and neo key management: IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	<p>Enter the port for the connection.</p> <p>5180 = Dongle Manager</p> <p>8181 = ASC License Management System</p>



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:

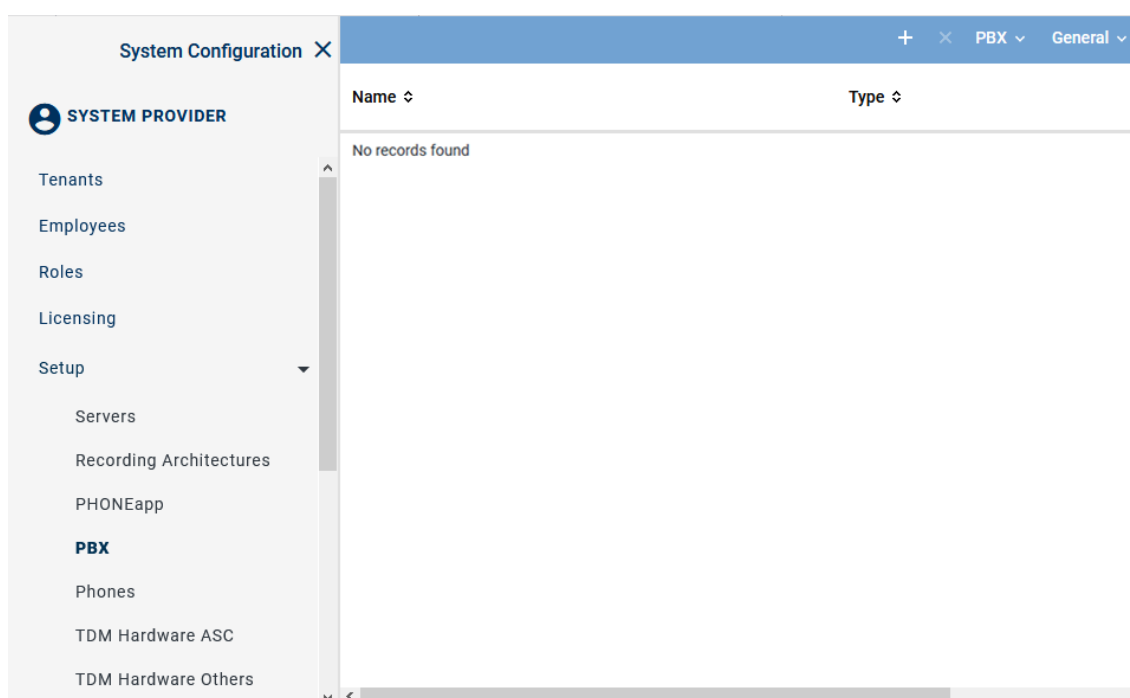




Fig. 340: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 341: Toolbar PBX module

	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administratre Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	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

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

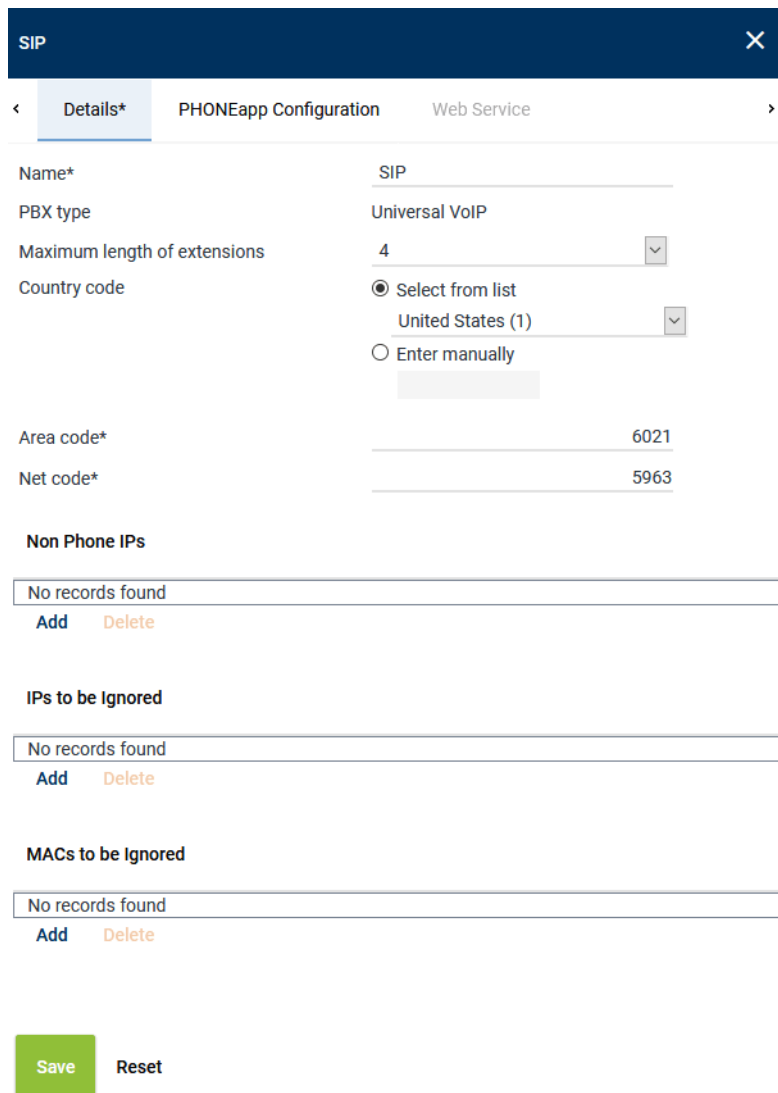


Fig. 342: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> 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.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.

Parameter	Value/Description
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 81: Create PBX

In the PBX module, there are advanced functions which cannot be configured in the Integrations module.

The following parameters are additionally available for passive recording and must be configured with the corresponding IP or MAC addresses of the customer's network for proper recording:

<i>Non Phone IPs</i>	<p>The <i>Non Phone IPs</i> entered here are treated as end device or participant which is not supposed to be recorded. Activities with this IPs are processed but the IPs are not considered independent phones. If you do not enter the Media Gateway here, for example, it is taken to be a phone and all parallel conversations are considered to be a conference when sniffed. In general, the Gateway is a <i>NonPhone</i> and the PBX a <i>Ignore IP</i>.</p> <p>Enter the gateway here, for example.</p>
<i>IPs to be ignored</i>	<p>The IP addresses entered here are ignored entirely. Enter the PBX here, for example, to ignore the music-on-hold data as otherwise a hold is interpreted as a connect with an unknown participant.</p> <p>Enter the IP addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p> <p>NOTICE! Do not enter an IP address as <i>Non Phone IP</i> and <i>IP to be ignored</i> at the same time as the communication with this IP address is then ignored entirely and not treated as <i>Non Phone IP</i> either anymore.</p>
<i>MACs to be ignored</i>	<p>The MAC addresses entered here are ignored entirely.</p> <p>If you work with a MAC address, enter the MAC addresses of all devices which are not supposed to be sniffed,</p> <p>e. g. PBXs, music-on-hold servers, phones that are not supposed to be sniffed.</p>

Passive recording will only work properly when all components of the customer's network that are not supposed to be recorded have been listed.



All components that are no phones but involved in the transmission of audio data such as gateways must be configured as *Non Phone IPs*.

All components of the customer's network that are not supposed to be recorded must be entered as *IPs to be ignored* with their respective IP or MAC addresses. These IP addresses are ignored entirely and not processed.

- 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.

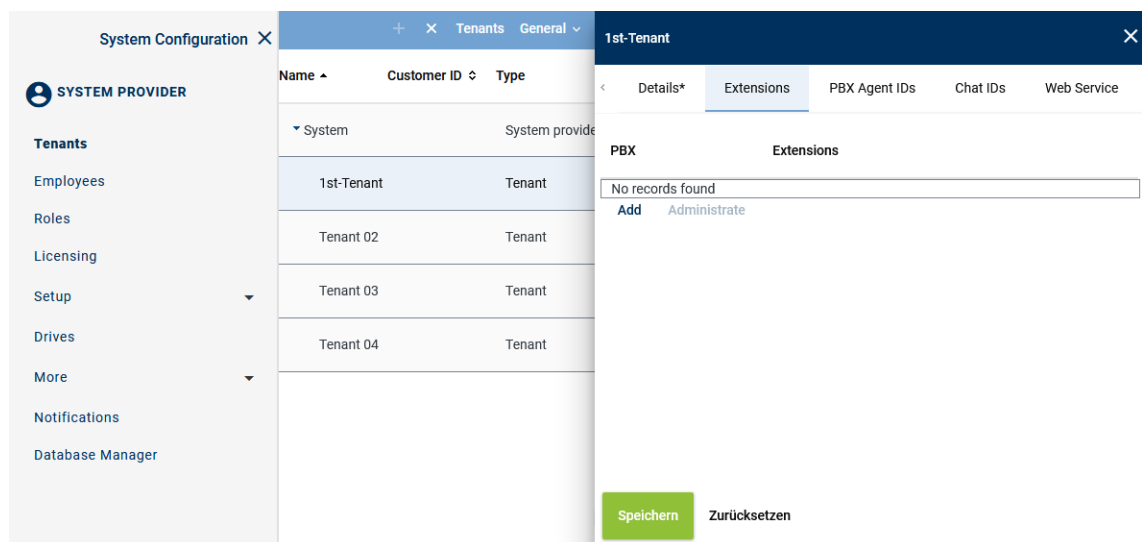


For information about the configuration refer to the administration manual for tenants *User management tenant*.

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.



The screenshot displays the 'System Configuration' window with the 'Tenants' module selected. The left sidebar contains a 'SYSTEM PROVIDER' section with a 'Tenants' menu item highlighted. The main area shows a table of tenants:

Name	Customer ID	Type
System		System provide
1st-Tenant		Tenant
Tenant 02		Tenant
Tenant 03		Tenant
Tenant 04		Tenant

On the right, the '1st-Tenant' details are shown, with the 'Extensions' tab selected. It displays a 'PBX' section with a table of extensions. The table is currently empty, showing 'No records found'. Below the table are buttons for 'Add' and 'Administrate'. At the bottom right, there are buttons for 'Speichern' (Save) and 'Zurücksetzen' (Reset).

Fig. 343: 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:

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

Extension or extension range separated by
", " or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 344: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> • ZIP • TXT • CSV <p>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.</p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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 detected, 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.

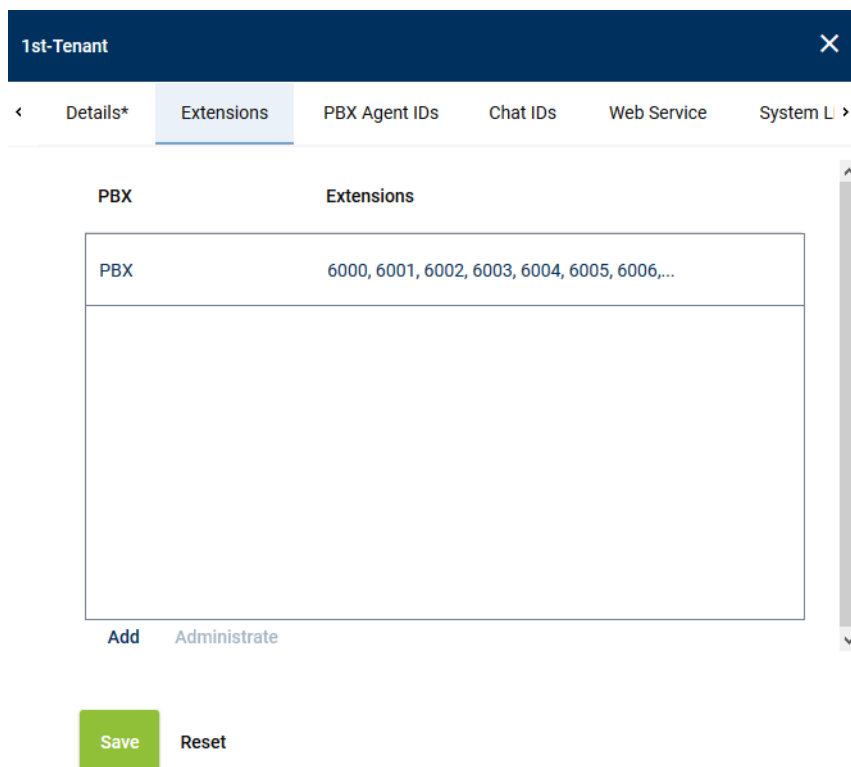


Fig. 345: Remove extensions

2. Click the button *Administrate*.

- 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. 346: Select extensions

- To remove the selected extensions, 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.

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

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

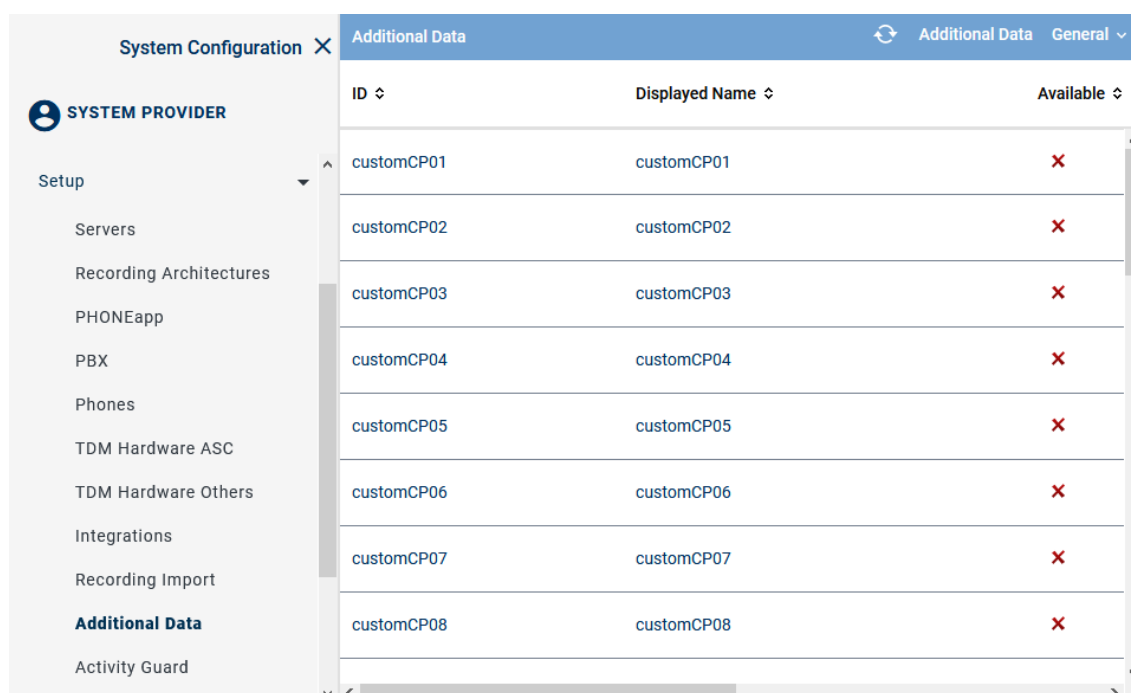


Fig. 347: Additional Data module main view

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

Change display name






Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	

Fig. 348: 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

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 349: 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 an 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:

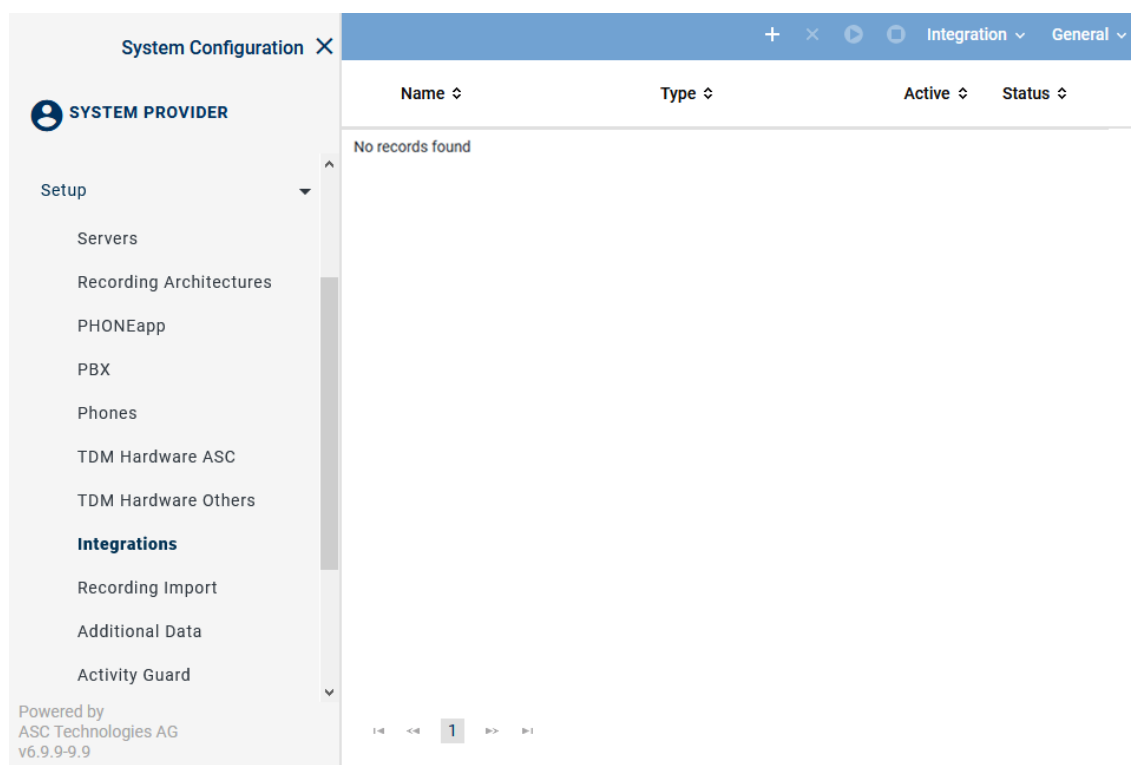




Fig. 350: Integrations - main view

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. <div> ✓ = Integration is active, can be deactivated in the toolbar via the icon . </div> <div> ✗ = Integration is not active, can be activated in the toolbar via the icon . </div>
Status	Shows whether the configuration has been carried out completely. <div> ✓ = Configuration is complete. </div> <div> ✗ = Configuration is incomplete. </div>

Toolbar of the Integrations module

The toolbar offers the following functions.

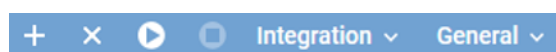







Fig. 351: Toolbar Integrations module

	<i>Create</i>	Opens the detail view so that you can create a new integration.
	<i>Delete</i>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	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.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Assign integration type

- 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.

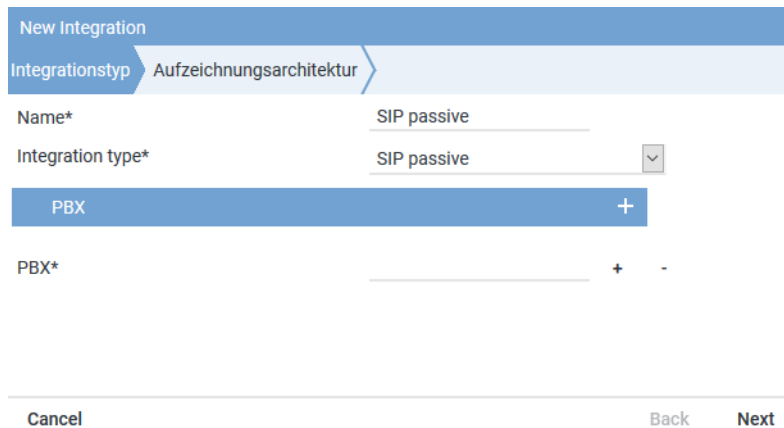



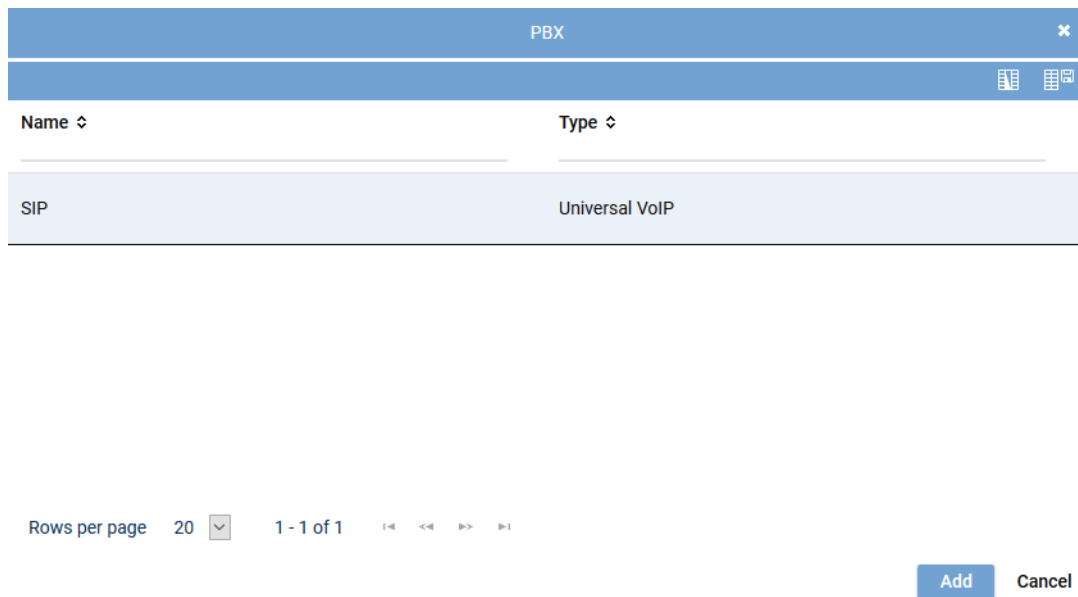
Fig. 352: Create integration type

- Enter the following parameters:

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

Tab. 82: Create integration type

- To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.



PBX	
Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

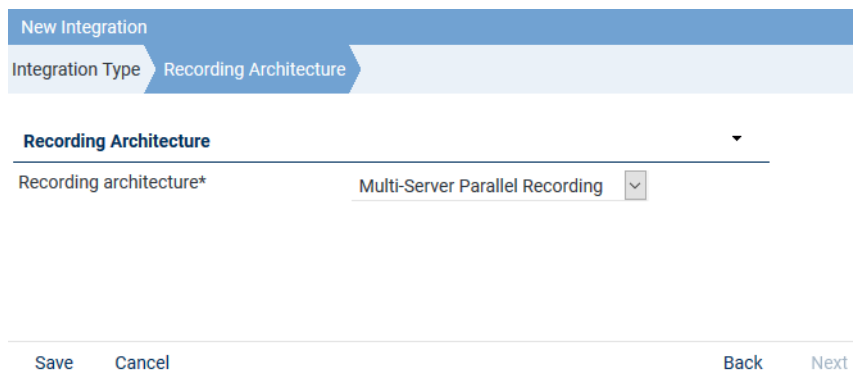
Add Cancel

Fig. 353: Integrations - 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.



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Parallel Recording

Save Cancel Back Next

Fig. 354: 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 Duplicates in parallel recording architectures.

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:

<div> <div></div> <div>SIP passive</div> <div>SIP passive</div> <div>×</div> <div>⚙️</div> </div>	
Step	Configuration
Configure recording architecture	<div>✓</div> <div>✎</div>
Configure recording servers	<div>×</div> <div>✎</div>
Configure add-on	<div>✓</div> <div>✎</div>
Configure miscellaneous settings	<div>✓</div> <div>✎</div>

Fig. 355: Configuration steps of the integration

Configure recording architecture

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

- 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.

Step: Configure Recording Architecture

Details *

Recording architecture*

Multi-Server Parallel Recording

▼


Save

Cancel

Fig. 356: Configuration step - Configure Recording Architecture

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

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Configure Recording Servers* appears.

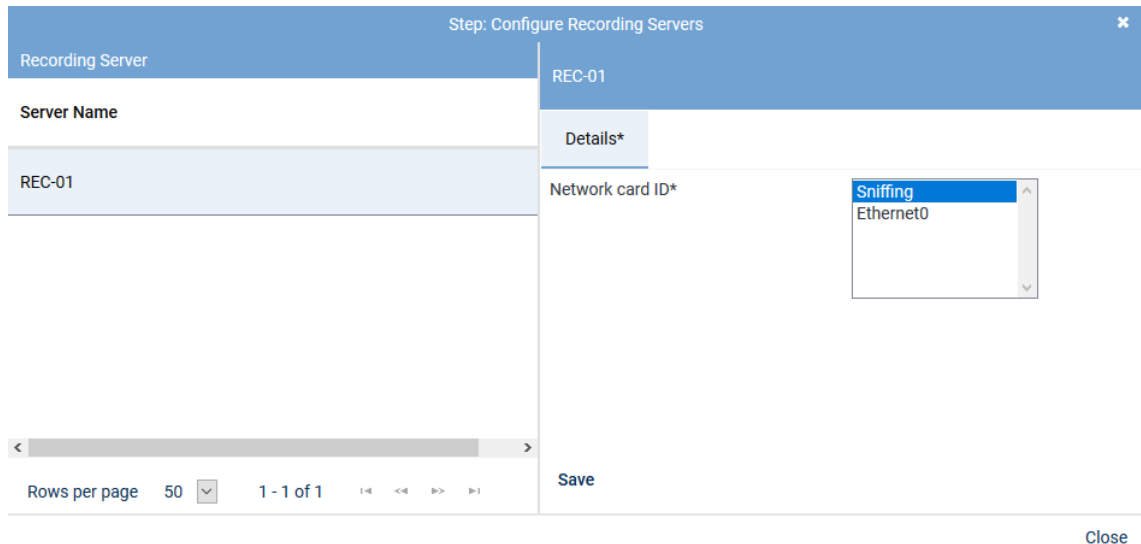


Fig. 357: Configuration step - Configure recording servers

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
<i>Network card ID</i>	From the list field, select the network card which is supposed to be used for sniffing the SIP and the RTP audio data.

Tab. 83: Configure recording servers



To ensure that only relevant data packages are considered in the recording, you must connect the respective network card with the correspondingly configured SPAN/mirror port of the network switch.

- Click on the button *Save*.
- Click on the button *Close* to finish this configuration step.



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.

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 CTIconnect module of the integration.



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

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 CTIconnect 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.

CTIconnect for Genesys T-Server

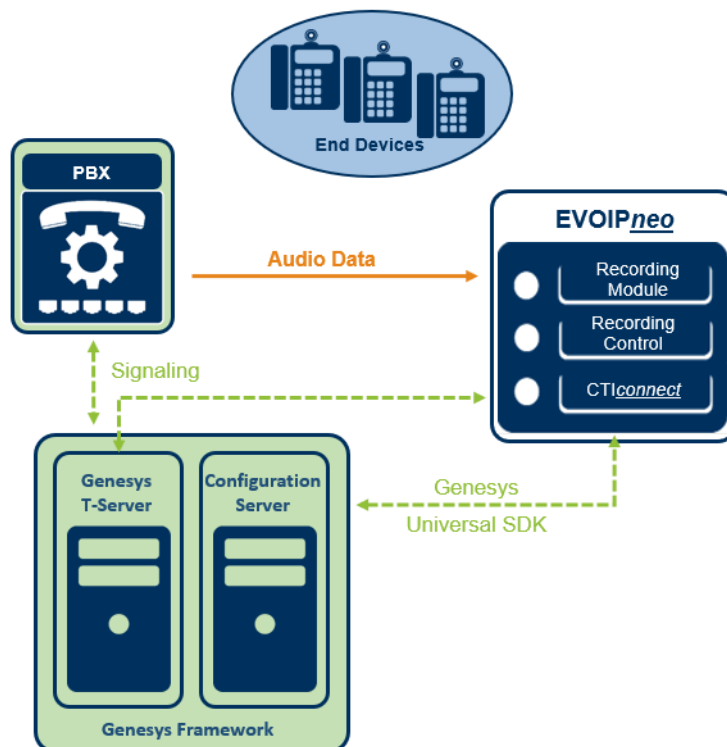


Fig. 358: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)"](#), p. 338.

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 CTIconnect module of the integration.

When using a CTIconnect 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*.

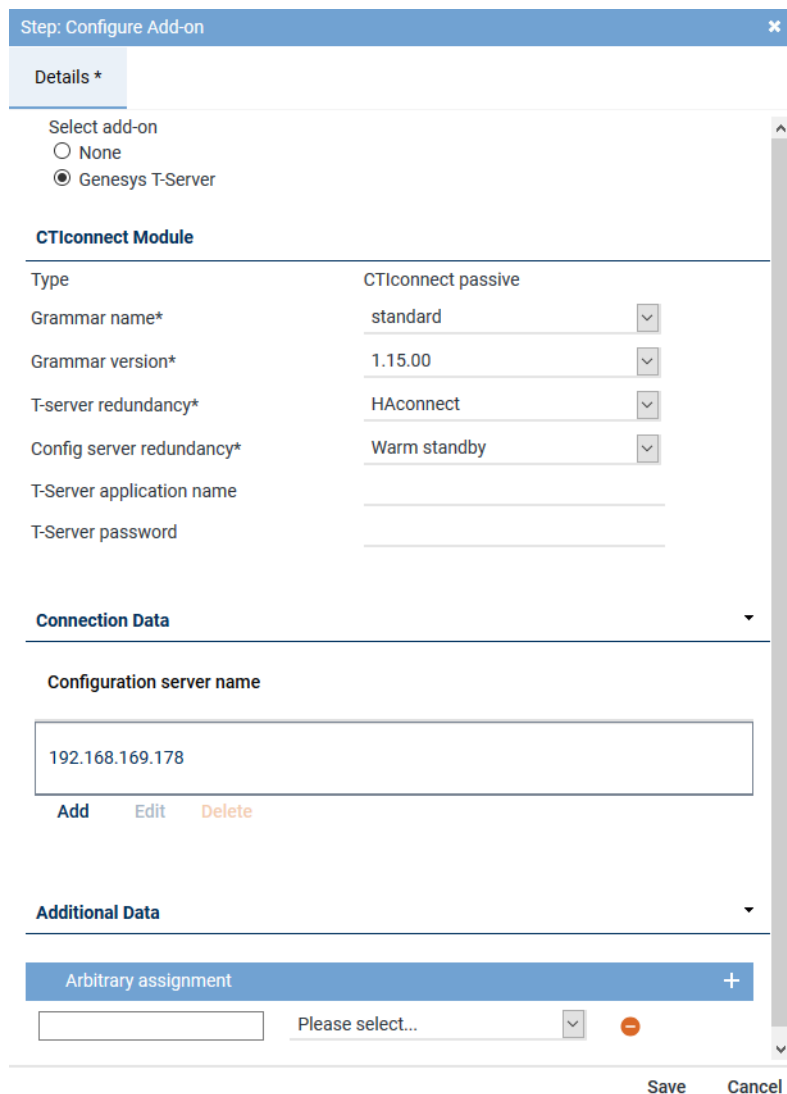
Adjust configuration file for Genesys add-on

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*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type	CTIconnect passive
Grammar name*	standard
Grammar version*	1.15.00
T-server redundancy*	HAconnect
Config server redundancy*	Warm standby
T-Server application name	
T-Server password	

Connection Data

Configuration server name

192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment +

Please select...

Save Cancel

Fig. 359: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the application name that the CTI <u>connect</u> 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.
<i>T-Server password</i>	This parameter must only be entered, if authentication on the Genesys T-Server is required. Enter the password that the CTI <u>connect</u> 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. 84: 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:

Configure Connection
✕

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add
Cancel

Fig. 360: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 85: 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.

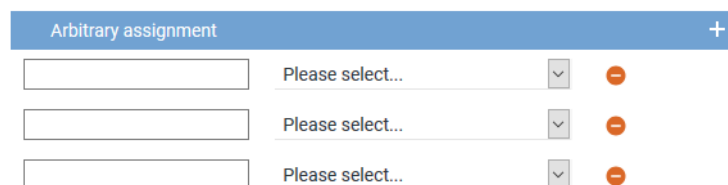



Fig. 361: Arbitrary assignment of the additional data

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 Sparkassen FI ISP (optional)

The add-on refers to the usage of CTIconnect 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 CTIconnect 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 CTIconnect for Sparkassen FI ISP and sent to the recording server.

Sparkassen FI Interaktive Service Plattform

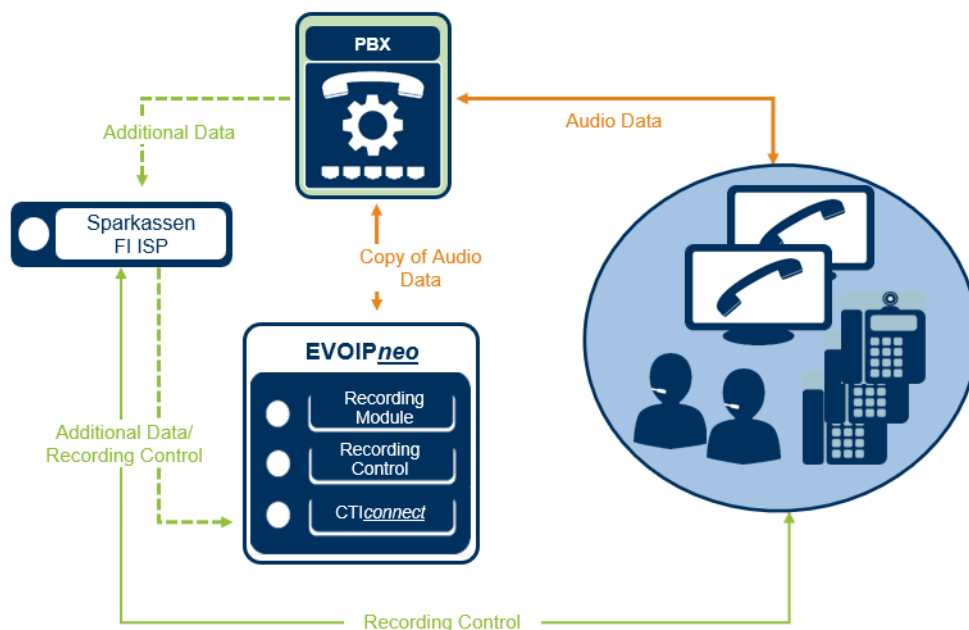



Fig. 362: Overview of Sparkassen FI ISP

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.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ Sparkassen FI ISP

CTIconnect Module

Type	CTIconnect passive	
Grammar name*	ISP Sparkassen FI	▼
Grammar version*	1.00.05	▼

Connection Data ▼

Listener port*	3468
----------------	------

Additional Data ▼

ID des Call Centers	Call Center ID	▼
ID des Calls aus Genesys	Universal Call ID	▼
Anmeldename des Kunden	User name	▼
Name des Kunden	Customer name	▼
Personennummer des Kunden	Customer ID	▼

Arbitrary assignment
+

	Please select...	▼	⊖
	Please select...	▼	⊖
	Please select...	▼	⊖

Save Cancel

Fig. 363: 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. 86: 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 Import grammars.

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
<i>Listener port</i>	Enter the port that the add-on connects to, e. g. 3468.

Tab. 87: 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 CTIconnect 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.

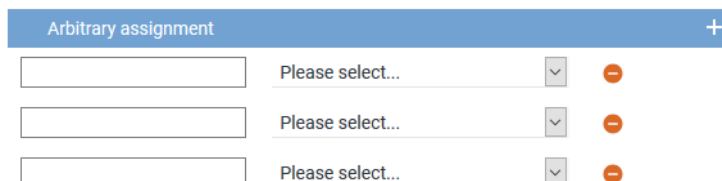



Fig. 364: Arbitrary assignment of the additional data

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 OpenScape Contact Center (optional)

The add-on refers to the usage of the OpenScape Contact Center and must only be configured if a OpenScape Contact Center is used.

The integration runs in combination with a Unify PBX which is responsible for recording. The CTI~~connect~~ Service receives the conversation events of the agents via a SDK link in the OpenScape Contact Center and sends the additional data to the EVOIP~~neo~~ Recording Service.

For information about the configuration of the OpenScape Contact Center, see Configure OpenScape Contact Center (optional).

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 OpenScape Contact Center in the detail view.

Step: Configure Add-on

Details

Select add-on
☐ None
☒ OpenScape Contact Center

CTIconnect Module

TypeCTIconnect passive
Grammar name*Unify OpenScape Contact Center
Grammar version*1.00.04

Connection Data

Connection data

6000@192.168.170.29

Add Edit Delete

Additional Data

Business UnitBusiness Unit
DepartmentDepartment
Department KeyDepartment Key
Call IDUniversal Call ID
To PartyTo Party
ACD Group NumberACD Group Number

Arbitrary assignment

Please select...

Please select...

Save Cancel

Fig. 365: Configure add-on for OSCC

Group field CTIconnect Module

- 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. 88: Configure CTIconnect module

Group field Connection Data

In the table Connection Data, you can enter one or several sets of connection data.

If you are configuring several connections, several connections to different business units are established simultaneously in the recording solution with OpenScape Contact Center.

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

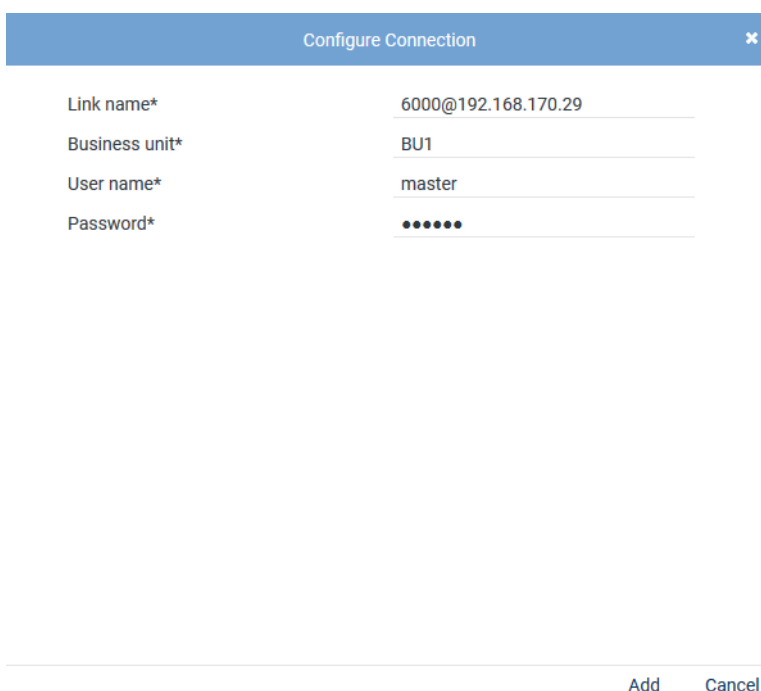


Fig. 366: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Link name</i>	Enter the link to the OSCC server in the format <i>osccport@ascserver</i> . The default value for the OSCC port is 6000 and the name of the OSCC server is usually spelled in minor letters. A valid link can look like this: 6000@osccv7r3. Ensure that the server name (e. g. osccv7r3) can be resolved to an IP address. Check whether the address can be reached via the ping command. Alternatively, you can also enter the IP address.
<i>Business unit</i>	The default name of a business unit is <i>default</i> . This is a predefined name for the business unit after a new OSCC server installation. Enter the business unit's actual name you would like to use in the future.
<i>User name</i>	Create a valid user for the business unit that you have created on the OSCC server, so the CTIconnect Service can establish the connection to the OSCC server. See Create user for CTIconnect.
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 89: Configure connection data

- Click on the button *Add* to save the entries and to close the window.
- To configure additional connections, repeat the configuration steps accordingly.

Group field Additional Data

When using **CTIconnect** for Unify OpenScope Contact Center, the following additional data is delivered with the protocol by default:

- *Business unit*
- *Department*
- *Department Key*
- *Call ID*

- *To Party*
- *ACD Group Number*

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 have been configured and made available in the Additional Data module previously.

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

Here, you can map the database fields for the additional data which is delivered by the [OSCC](#). The contact data of the processed contacts of the OpenScape Contact Center provides a list of key pairs/value pairs. The keyword of this key pair/value pair can be chosen arbitrarily and adjusted customer-specifically. If you would like to use more than one word, avoid spaces. Use underscores instead of spaces, e. g. *ACD_group*.

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.

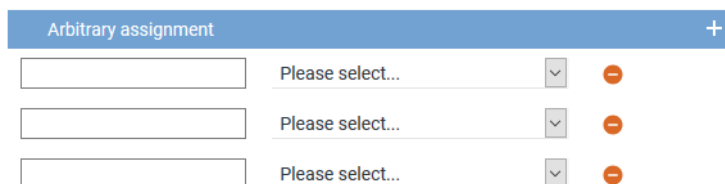





Fig. 367: Arbitrary assignment of the additional data

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 a configured display name of the additional data type which is supposed to appear as column headline in the players. Here, you can only select the display names for the additional data that you have configured and made available 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. To delete an assignment, click on the icon  in the respective row.
6. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

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.

Step: Miscellaneous Settings

Details

Dispatcher
Please select...

Save Cancel

Fig. 368: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	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*.












	SIP passive	SIP passive		
Step		Configuration		
Configure recording architecture				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 369: Activate integration

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

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
⌵ SIP passive	SIP passive	✓	✓

Fig. 370: 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.

- 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.

+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
⌵ SIP passive	SIP passive	✗	✓

Fig. 371: Deactivate integration

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

7.1.3 Adjust neo configuration file

Some parameters cannot be configured via the graphic interface but have to be adjusted in the configuration files.

To map additional data from the protocol, you have to adjust the configuration file of the Recording module.

7.1.3.1 Adjust Recording module

The configuration files for the Recording module are located in the following path:

C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingModule

For each configured integration, a separate configuration file is created upon the first start. Customer-specific adjustments of the parameters must be made in the corresponding integration configuration file. Upon the start, the basic file *basic.recorder.properties* is read out first. Then, the integration configuration file is read out. The values in the integration configuration file are prioritized and will eventually be used.

If you have configured several integrations of the same integration type, you must make your adjustments for each integration separately. To determine which file belongs to which integration, you can open the configuration file and check the range of assigned extensions, for instance. Do not change the original file name! Otherwise, it will not be possible to start the integration again.

Integrations which have been configured but not activated are marked with *inactive* in front of the file name. The file will not be deleted even if the integration is deleted in the application System Configuration. If a deactivated integration is activated again, the information inactive is removed and the file is used again.

1. Change to the installation directory *C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingModule*.

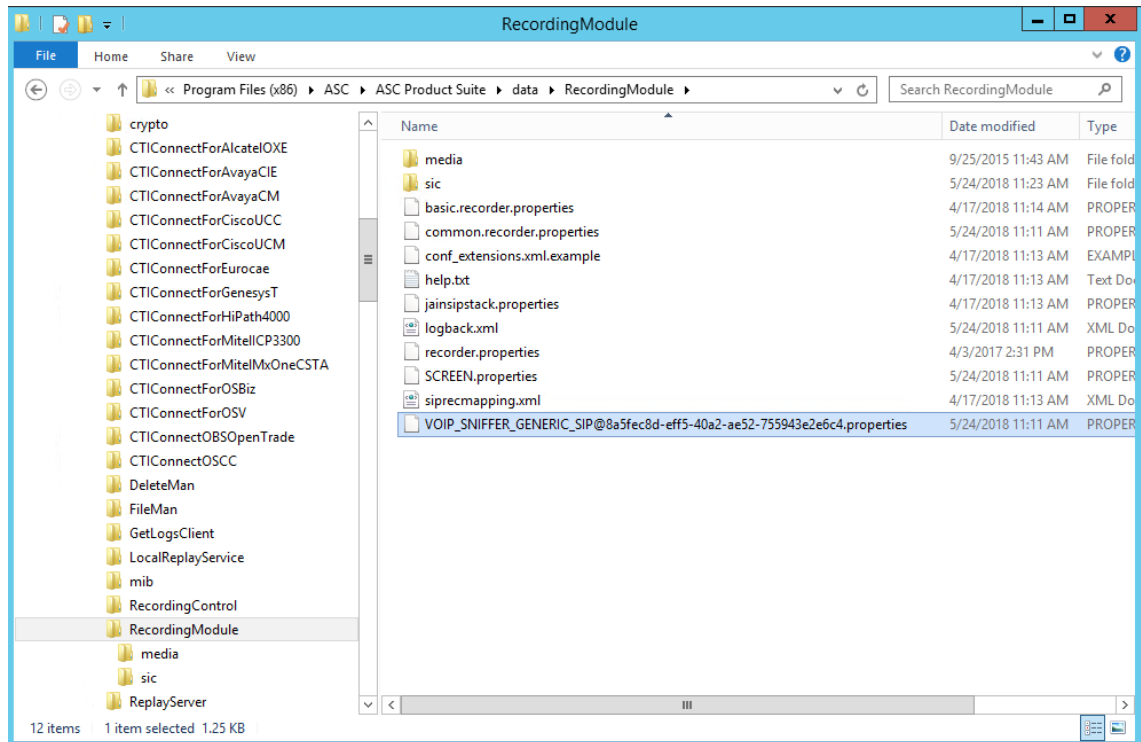
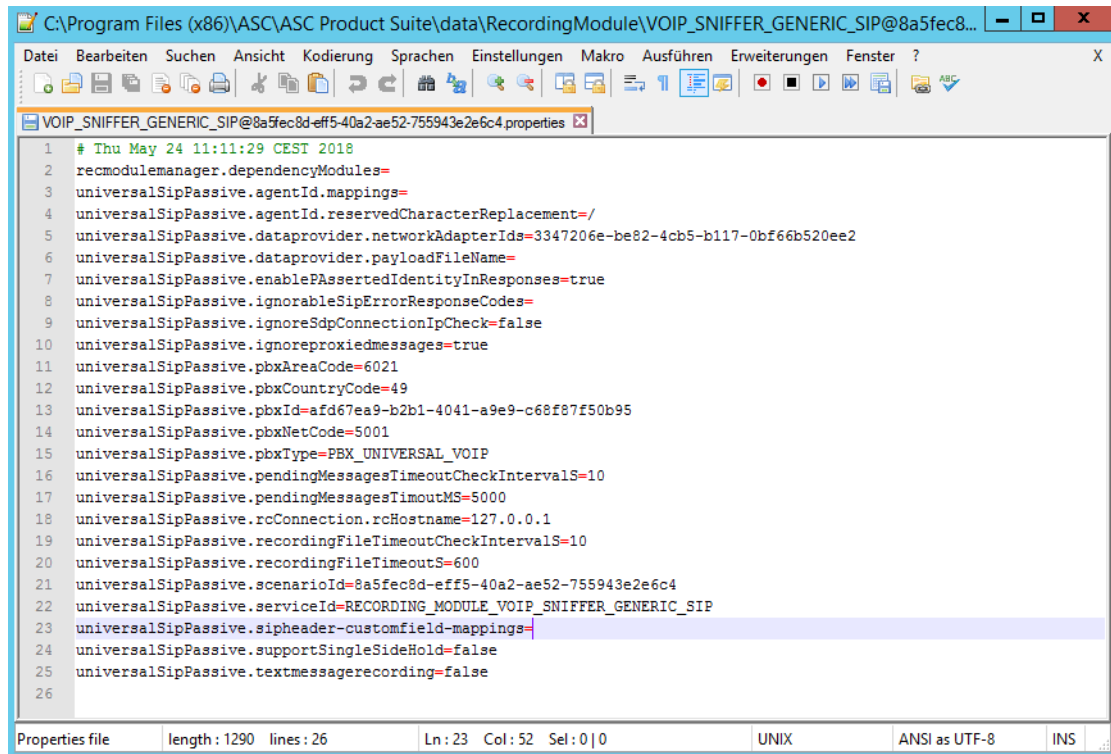


Fig. 372: Path to the configuration file

2. Open the file *VOIP_SNIFFER_GENERIC_SIP@<UUID>.properties* in the Editor.



```

1 # Thu May 24 11:11:29 CEST 2018
2 recmodulemanager.dependencyModules=
3 universalSipPassive.agentId.mappings=
4 universalSipPassive.agentId.reservedCharacterReplacement=/
5 universalSipPassive.dataprovider.networkAdapterIds=3347206e-be82-4cb5-b117-0bf66b520ee2
6 universalSipPassive.dataprovider.payloadFileName=
7 universalSipPassive.enablePassertedIdentityInResponses=true
8 universalSipPassive.ignoreableSipErrorResponseCodes=
9 universalSipPassive.ignoreSdpConnectionIpCheck=false
10 universalSipPassive.ignoreproxiedmessages=true
11 universalSipPassive.pbxAreaCode=6021
12 universalSipPassive.pbxCountryCode=49
13 universalSipPassive.pbxId=afd67ea9-b2b1-4041-a9e9-c68f87f50b95
14 universalSipPassive.pbxNetCode=5001
15 universalSipPassive.pbxType=PBX_UNIVERSAL_VOIP
16 universalSipPassive.pendingMessagesTimeoutCheckIntervals=10
17 universalSipPassive.pendingMessagesTimeoutMS=5000
18 universalSipPassive.rcConnection.rcHostname=127.0.0.1
19 universalSipPassive.recordingFileTimeoutCheckIntervals=10
20 universalSipPassive.recordingFileTimeoutS=600
21 universalSipPassive.scenarioId=8a5fec8d-ef5-40a2-ae52-755943e2e6c4
22 universalSipPassive.serviceId=RECORDING_MODULE_VOIP_SNIFFER_GENERIC_SIP
23 universalSipPassive.sipheader-customfield-mappings=
24 universalSipPassive.supportSingleSideHold=false
25 universalSipPassive.textmessagerecording=false
26

```

Fig. 373: Configure parameters

3. Search for the entry `universalSipPassive.sipheader-customfield-mappings=`.
4. Enter a regular expression here.
5. For the information from the SIP header to be issued in the additional data fields in the replay applications, you have to go to the Additional Data module to map the fields from the SIP header to the customCP fields, see [chapter "Configure additional data", p. 47](#).

Example:

```

# sipheader-customfield-mappings= <custom field definition>['<custom field definition>']*
# <custom field definition> ::= <tag definition>|'<source definition>|'<reg ex pattern>
# <tag definition> ::= <RC tag name definition> | <pattern group names use indicator>
# <RC tag name definition> ::= 'customCP'[0-9]*
# <pattern group names use indicator> ::= 'group-names'
# <source definition> ::= (<SIP header name> | 'content')[':'<source SIP message type list>]
# <SIP header name> ::= any valid SIP header name
# <source SIP message type list> ::= <SIP message type>['<SIP message type>']*
# <SIP message type> ::= <SIP request method> | <SIP response code>
# <SIP request method> ::= any valid SIP request method like INVITE, ACK, INFO...
# <SIP response code> ::= any numeric SIP response code like 100, 180, 183, 200 ...
# <reg ex pattern> ::= Java regular expression, may contain group names as tag names when
'group-names' is set as <tag definition>

```

1. Example 1:
To have the Lync Conference ID issued in the field *customCP02*, enter the following regular expression:
 - `universalSipPassive.sipheader-customfileld-mappings=customCP02|To|audio-video:id:(.*)`
2. Example 2:
To have the SIP Call ID issued in the field *customCP01*, enter the following regular expression:

- `universalSipPassive.sipheader-customfileld-mappings=customCP01|Call-ID|(.*)`
- 3. Example 3:
To have the connection IP and the media port from the content of INVITE, 200 OK, and ACK Messages issued in different fields, enter the following regular expression:
 - `universalSipPassive.sipheader-customfileld-mappings=group-names|content:INVITE 200 ACK|c=IN IP4 (?<customCP1>[^\r]*).*m=audio (?<customCP2>[^\h]*)`
- 4. Once you have finished the configuration , save the changes in the configuration file.
- 5. Restart the service *ASC RecordingModule* so that the changes are applied.

7.1.4 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*.

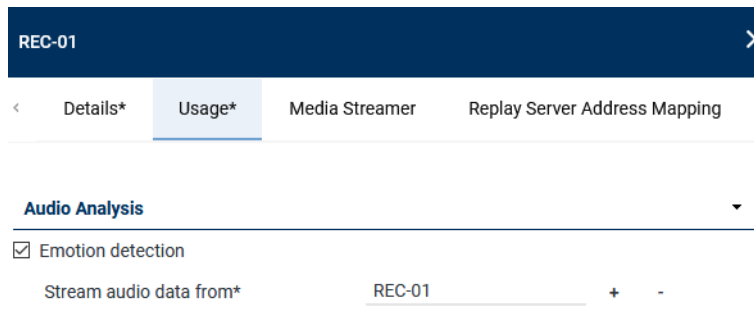


Fig. 374: Servers module - Activate emotion detection

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 the correct functionality of the recording system and the validity of recording content:

- *Packet loss detection*
- *Silence detection*

×

< Details*
Recording Content Validation
>

Activate packet loss detection	<input checked="" type="checkbox"/>
Activate decryption error detection	<input type="checkbox"/>
<input checked="" type="checkbox"/> Activate silence detection	
Minimum duration*	30000 ms
Threshold value*	-60 dB
Silence percentage*	90 %
Weighting*	10
Emotion detection*	+ -


Save

Reset

Fig. 375: Create integration - tab Recording Content Validation

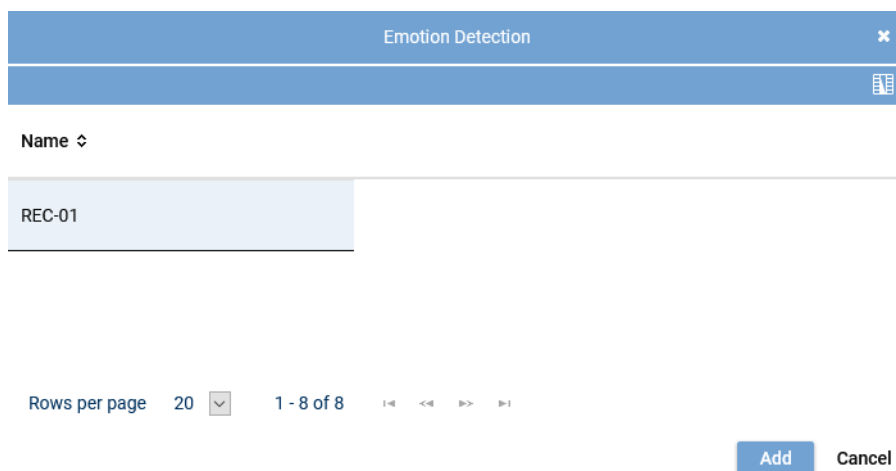
Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost. NOTICE! Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	NOTICE! This check is not required in this recording solution.
Activate silence detection	<input checked="" type="checkbox"/> Activate the check box to check whether the recording contain sections of silence and under which conditions sections are recognized as silence. NOTICE! A high percentage of silence sections can indicate a technical problem such as a connection interruption.
<i>Minimum duration</i>	Enter the minimum duration of silence after which a notification is supposed to be issued. Default value is 30000 ms (30 seconds).
<i>Threshold value</i>	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.
<i>Silence percentage</i>	Enter the percentage of silence in a recording which is supposed to trigger a notification. Default value is 90 %.
<i>Weighting</i>	Enter the extent to which the audio curve (samples) is supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 1-10000 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.



Emotion Detection

Name ▾

REC-01

Rows per page 20 ▾ 1 - 8 of 8 << < > >>

Add Cancel

Fig. 376: 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.

7.1.5 Configure CTIconnect add-on

7.1.5.1 Configure Genesys T-Server (optional)

7.1.5.1.1 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.

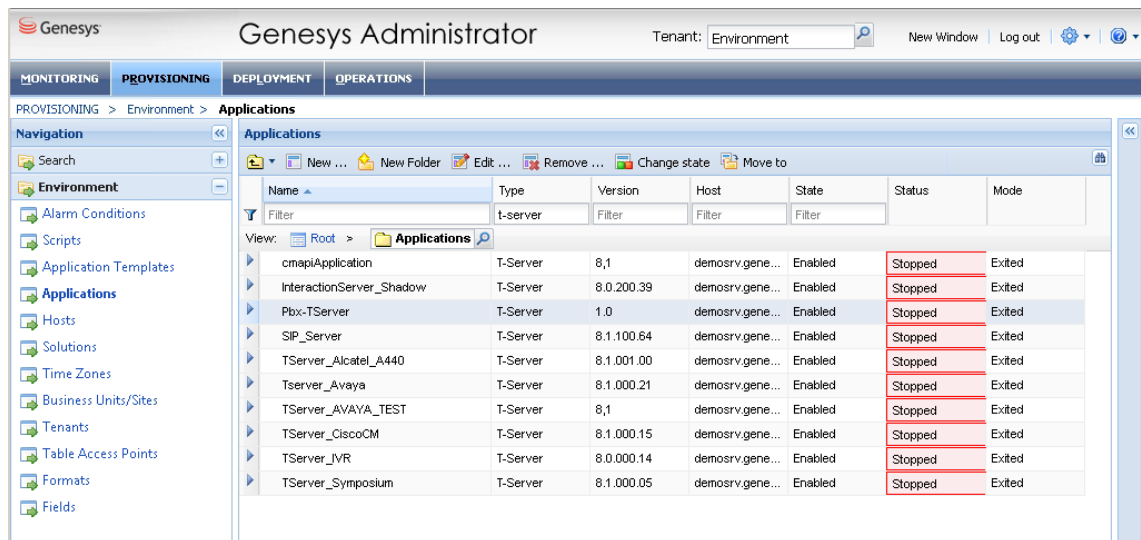


Fig. 377: Genesys Administrator - select T-Server

- Double-click on the entry T-Server which has been connected to the switch instance to be monitored.
⇒ The window *Configuration* appears.
- Expand the area *Server Info*.

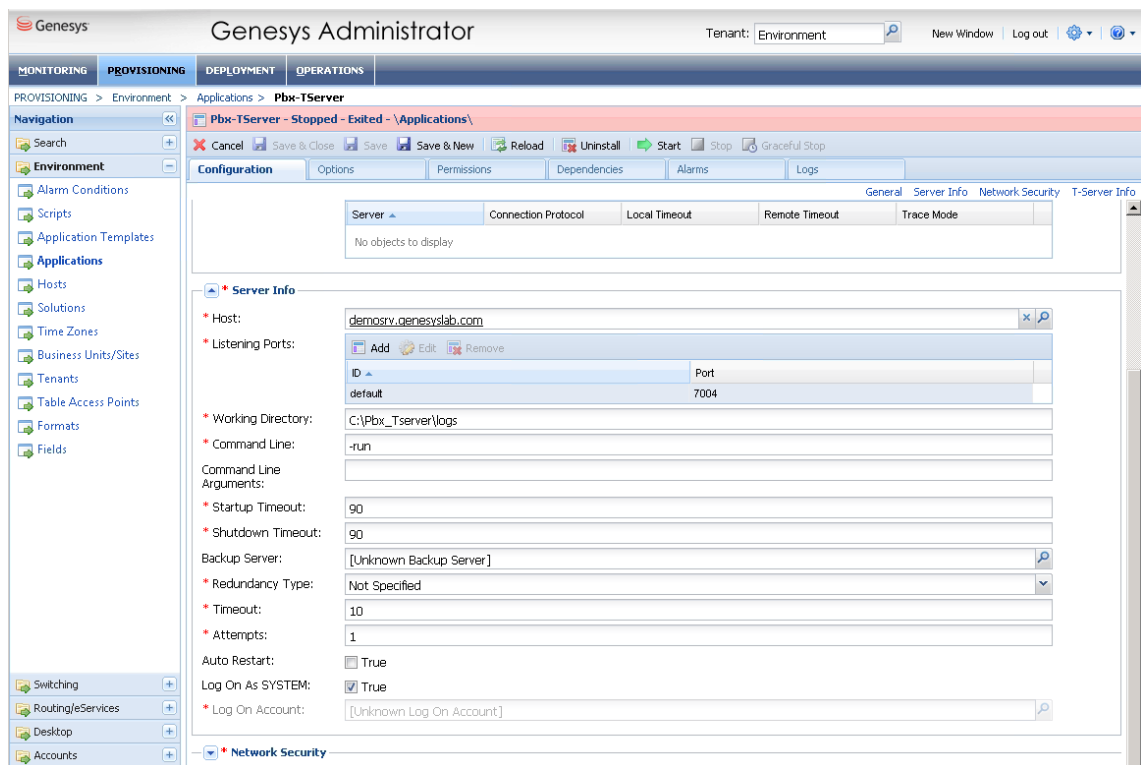


Fig. 378: Genesys Administrator - configure T-Server

- In the field *Host*, enter the IP address or the computer name of the T-Server, e. g. *demosrv8.genesyslab.com*.
- In the field *Listening Port*, enter the port of the T-Server, e. g.

7.1.5.1.2 Configure IP address and port of the Genesys Configuration Server

- Click on the menu item *Environment > Applications* in the navigation bar.

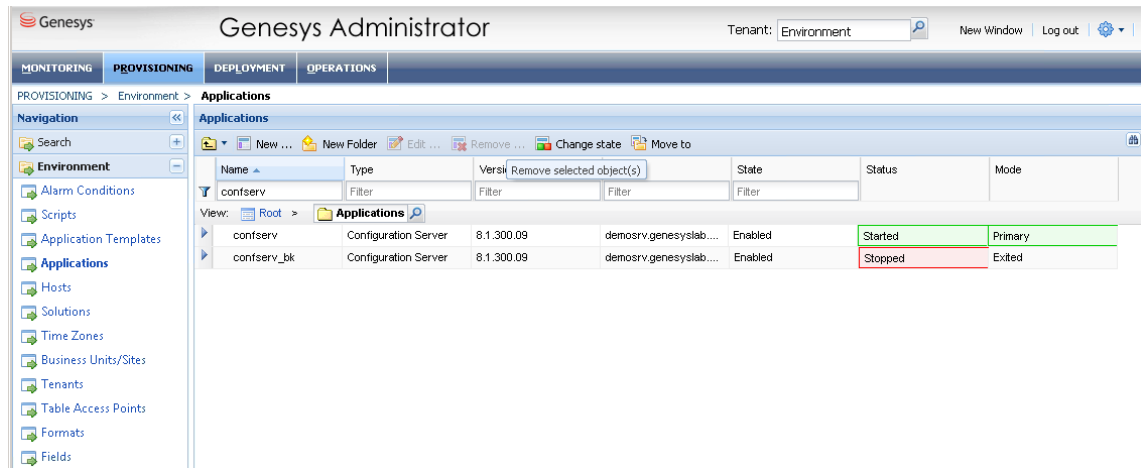


Fig. 379: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.
⇒ The window *Configuration* appears.
3. Expand the area *Server Info*.

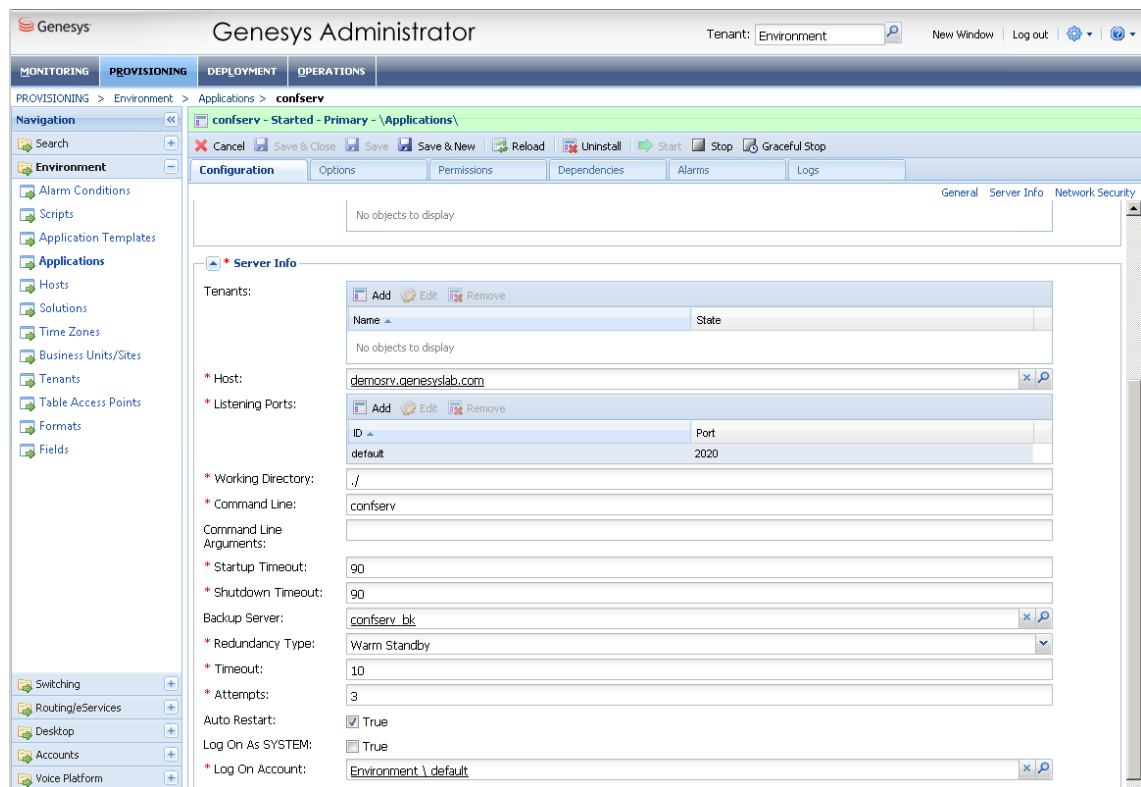


Fig. 380: Genesys Administrator - configure configuration server

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*.

7.1.5.1.3 Configure switch instance in the Genesys Configuration Server

1. Click on the menu item *Switching > Switches* in the navigation bar.

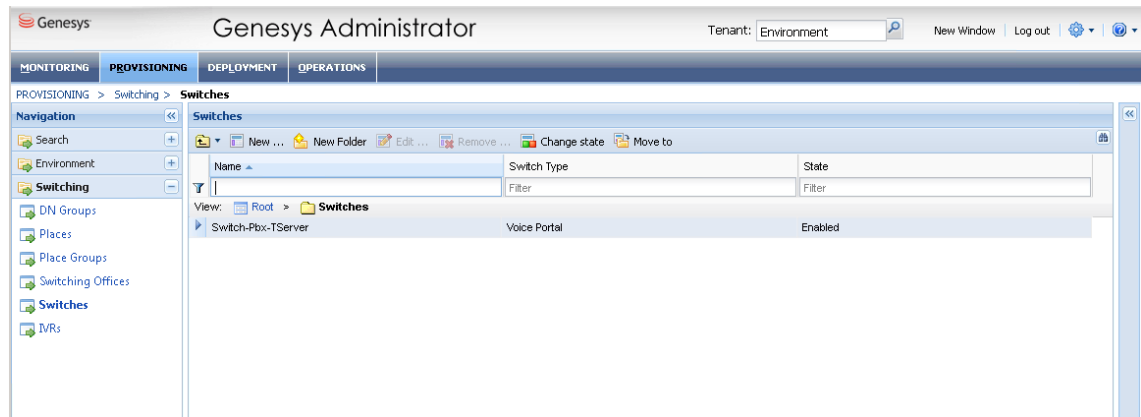


Fig. 381: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.
⇒ The window *Configuration > General* appears.

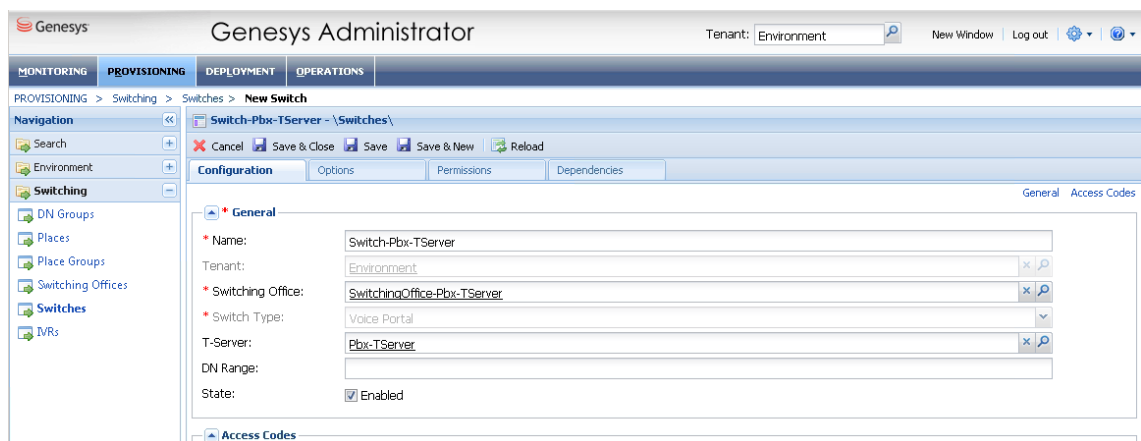


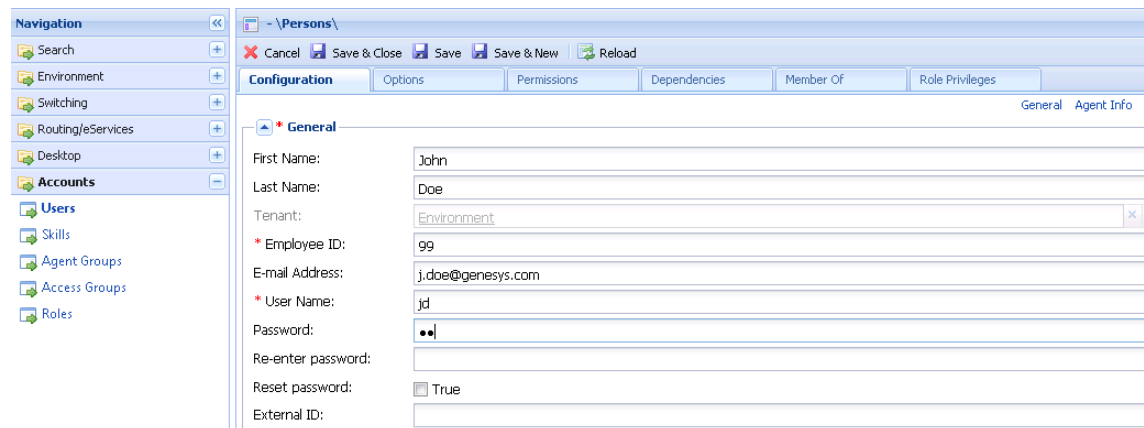
Fig. 382: Genesys Administrator - configure switch instance

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.

7.1.5.1.4 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.



Navigation: Search, Environment, Switching, Routing/Services, Desktop, Accounts, Users, Skills, Agent Groups, Access Groups, Roles

Configuration: Options, Permissions, Dependencies, Member Of, Role Privileges

General Agent Info

* General

First Name: John

Last Name: Doe

Tenant: Environment

* Employee ID: 99

E-mail Address: j.doe@genesys.com

* User Name: jd

Password: [masked]

Re-enter password: [empty]

Reset password: ☐ True

External ID: [empty]

Fig. 383: 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.

8 Troubleshooting



Before initiating any troubleshooting measures, verify that the recording solution has been configured according to the description in the manual and check whether an up-to-date hotfix version with bug fixes is available.

If no calls or additional data have been recorded check:

- whether the correct network device has been selected in System Configuration, see [chapter "Configure server", p. 21](#)
- the correct configuration of the SPAN port

When opening a ticket, include the following information:

- Log files with test calls
NOTICE! Before creating any log files, adjust the settings of the log levels in the Log Level module in System Monitoring as described below, see user manual *System Monitoring*.
- detailed description of the issue and of the scenarios of the test calls which have been made
- extension, MAC IP address of the affected device
- manufacturer, type, and software version of the PBX
- Wireshark traces of the recording network interface

Log level settings

Module	Log level
RECORDING_CONTROL	DEBUG
RECORDING_MODULE_MANAGER	DEBUG
API_SERVER	DEBUG
FILE_MANAGER	DEBUG

List of figures

Fig. 1	Overview of the recording solution.....	6
Fig. 2	SIP trunk recording with gateway or SBC	7
Fig. 3	Configuration Manager - Select recording profile as default	14
Fig. 4	System Configuration - web interface	15
Fig. 5	System Configuration - main view:.....	16
Fig. 6	Recording architectures - main view	17
Fig. 7	Toolbar Recording Architectures module.....	17
Fig. 8	Create recording architecture - All-in-one Basic Recording	18
Fig. 9	Recording architecture - tab Details.....	19
Fig. 10	Select integration type.....	19
Fig. 11	Recording architecture - tab Server Assignment	20
Fig. 12	Recording architecture - assign server	20
Fig. 13	Recording architecture - activate recording variant.....	21
Fig. 14	Recording architecture - activate recording architecture.....	21
Fig. 15	Servers - main view.....	22
Fig. 16	Toolbar Servers module.....	22
Fig. 17	Add server locations.....	23
Fig. 18	Delete server location	24
Fig. 19	Servers - tab Details.....	25
Fig. 20	Servers - tab usage	25
Fig. 21	Group field API Server	26
Fig. 22	Select storage expansion.....	27
Fig. 23	Group field Audio Analysis	28
Fig. 24	Select server for emotion detection.....	28
Fig. 25	Group field Recording Control/Key Management	28
Fig. 26	Group field Data Processing	29
Fig. 27	Select server	31
Fig. 28	Group field Replay	32
Fig. 29	Select server	33
Fig. 30	Group field Virtualization	34
Fig. 31	Servers module - tab Media Streamer	35
Fig. 32	Servers module - tab Replay Server Address Mapping	36
Fig. 33	Servers module - tab Key Management.....	38
Fig. 34	Servers module - tab Keystore/Virtualization	40
Fig. 35	PBX module - main view	41
Fig. 36	Toolbar PBX module	41
Fig. 37	Create new PBX - tab Details	42
Fig. 38	Tenants - main view - tab Extensions	44
Fig. 39	Assign extensions to tenants	45
Fig. 40	Remove extensions.....	46
Fig. 41	Select extensions	47

Fig. 42	Additional Data module main view	47
Fig. 43	Configure additional data	48
Fig. 44	Additional data - configure availability	48
Fig. 45	Integrations - main view	49
Fig. 46	Toolbar Integrations module	49
Fig. 47	Create integration type	50
Fig. 48	Integrations - select PBX.....	51
Fig. 49	Assign recording architecture - All-in-one Basic	51
Fig. 50	Configuration steps of the integration	52
Fig. 51	Configuration step - Configure Recording Architecture.....	52
Fig. 52	Configuration step - Configure recording servers	53
Fig. 53	Overview of the add on of Genesys T-Server	54
Fig. 54	Configure add-on for Genesys T-Server	55
Fig. 55	Configure connection data	57
Fig. 56	Arbitrary assignment of the additional data.....	58
Fig. 57	Overview of Sparkassen FI ISP	59
Fig. 58	Configure add-on for Sparkassen FI ISP	60
Fig. 59	Arbitrary assignment of the additional data.....	61
Fig. 60	Configure add-on for OSCC.....	63
Fig. 61	Configure connection data	64
Fig. 62	Arbitrary assignment of the additional data.....	65
Fig. 63	Configure miscellaneous settings	66
Fig. 64	Activate integration.....	66
Fig. 65	Activated integration.....	67
Fig. 66	Deactivate integration	67
Fig. 67	Recording architectures - main view	68
Fig. 68	Toolbar Recording Architectures module.....	68
Fig. 69	Create recording architecture - All-in-one Failover	69
Fig. 70	Recording architecture - tab Details - All-in-one Failover.....	70
Fig. 71	Select integration type.....	71
Fig. 72	Recording Architecture - tab Server Assignment	72
Fig. 73	Recording Architecture - assign server - example	72
Fig. 74	Recording Architecture - activate recording type	73
Fig. 75	Recording architecture - activate recording architecture.....	73
Fig. 76	Servers - main view.....	74
Fig. 77	Toolbar Servers module.....	74
Fig. 78	Add server locations.....	76
Fig. 79	Delete server location	77
Fig. 80	Servers - tab Details.....	77
Fig. 81	Servers - tab usage.....	78
Fig. 82	Group field API Server	78
Fig. 83	Select storage expansion.....	80

Fig. 84	Group field Audio Analysis	80
Fig. 85	Select server for emotion detection.....	81
Fig. 86	Group field Recording Control/Key Management	81
Fig. 87	Group field Data Processing	82
Fig. 88	Select server	84
Fig. 89	Group field Replay	84
Fig. 90	Select server	86
Fig. 91	Group field Virtualization	86
Fig. 92	Servers module - tab Media Streamer	87
Fig. 93	Servers module - tab Replay Server Address Mapping	89
Fig. 94	Servers module - tab Key Management.....	90
Fig. 95	Servers module - tab Keystore/Virtualization	92
Fig. 96	PBX module - main view	93
Fig. 97	Toolbar PBX module	93
Fig. 98	Create new PBX - tab Details	95
Fig. 99	Tenants - main view - tab Extensions	97
Fig. 100	Assign extensions to tenants	98
Fig. 101	Remove extensions.....	99
Fig. 102	Select extensions	100
Fig. 103	Additional Data module main view	100
Fig. 104	Configure additional data	101
Fig. 105	Additional data - configure availability	101
Fig. 106	Integrations - main view	102
Fig. 107	Toolbar Integrations module	102
Fig. 108	Create integration type	103
Fig. 109	Integrations - select PBX.....	104
Fig. 110	Assign recording architecture - All-in-one Failover	104
Fig. 111	Configuration steps of the integration	105
Fig. 112	Configuration step - Configure Recording Architecture.....	105
Fig. 113	Configuration step - Configure recording servers	106
Fig. 114	Overview of the add on of Genesys T-Server	107
Fig. 115	Configure add-on for Genesys T-Server	108
Fig. 116	Configure connection data	110
Fig. 117	Arbitrary assignment of the additional data.....	111
Fig. 118	Overview of Sparkassen FI ISP	112
Fig. 119	Configure add-on for Sparkassen FI ISP	113
Fig. 120	Arbitrary assignment of the additional data.....	114
Fig. 121	Configure add-on for OSCC.....	116
Fig. 122	Configure connection data	117
Fig. 123	Arbitrary assignment of the additional data.....	118
Fig. 124	Configure miscellaneous settings	119
Fig. 125	Activate integration.....	119

Fig. 126	Activated integration.....	120
Fig. 127	Deactivate integration	120
Fig. 128	Recording architectures - main view	121
Fig. 129	Toolbar Recording Architectures module.....	121
Fig. 130	Create recording architecture - All-in-one Parallel Recording.....	122
Fig. 131	Recording architecture - tab Details - All-in-one Parallel Recording	123
Fig. 132	Select integration type.....	124
Fig. 133	Recording Architecture - tab Server Assignment	125
Fig. 134	Recording Architecture - assign server - example	125
Fig. 135	Recording Architecture - activate recording type	126
Fig. 136	Activate recording architecture.....	126
Fig. 137	Servers - main view.....	127
Fig. 138	Toolbar Servers module.....	127
Fig. 139	Add server locations.....	129
Fig. 140	Delete server location	130
Fig. 141	Servers - tab Details.....	130
Fig. 142	Servers - tab usage.....	131
Fig. 143	Group field API Server	131
Fig. 144	Select storage expansion.....	133
Fig. 145	Group field Audio Analysis	133
Fig. 146	Select server for emotion detection.....	134
Fig. 147	Group field Recording Control/Key Management	134
Fig. 148	Group field Data Processing	135
Fig. 149	Select server	137
Fig. 150	Group field Replay	137
Fig. 151	Select server	139
Fig. 152	Group field Virtualization	139
Fig. 153	Servers module - tab Media Streamer	140
Fig. 154	Servers module - tab Replay Server Address Mapping	142
Fig. 155	Servers module - tab Key Management.....	143
Fig. 156	Servers module - tab Keystore/Virtualization	145
Fig. 157	PBX module - main view	146
Fig. 158	Toolbar PBX module	146
Fig. 159	Create new PBX - tab Details	148
Fig. 160	Tenants - main view - tab Extensions	150
Fig. 161	Assign extensions to tenants	151
Fig. 162	Remove extensions.....	152
Fig. 163	Select extensions	153
Fig. 164	Additional Data module main view	153
Fig. 165	Configure additional data	154
Fig. 166	Additional data - configure availability.....	154
Fig. 167	Integrations - main view	155

Fig. 168	Toolbar Integrations module	155
Fig. 169	Create integration type	156
Fig. 170	Integrations - select PBX.....	157
Fig. 171	Assign recording architecture - All-in-one Parallel	157
Fig. 172	Configuration steps of the integration	158
Fig. 173	Configuration step - Configure Recording Architecture.....	158
Fig. 174	Configuration step - Configure recording servers	159
Fig. 175	Overview of the add on of Genesys T-Server	160
Fig. 176	Configure add-on for Genesys T-Server	161
Fig. 177	Configure connection data	163
Fig. 178	Arbitrary assignment of the additional data.....	164
Fig. 179	Overview of Sparkassen FI ISP	165
Fig. 180	Configure add-on for Sparkassen FI ISP	166
Fig. 181	Arbitrary assignment of the additional data.....	167
Fig. 182	Configure add-on for OSCC.....	169
Fig. 183	Configure connection data	170
Fig. 184	Arbitrary assignment of the additional data.....	171
Fig. 185	Configure miscellaneous settings	172
Fig. 186	Activate integration.....	172
Fig. 187	Activated integration.....	173
Fig. 188	Deactivate integration	173
Fig. 189	Recording architectures - main view	174
Fig. 190	Toolbar Recording Architectures module.....	174
Fig. 191	Create recording architecture - Multi-Server Recording.....	175
Fig. 192	Recording architecture - tab Details - Multi-Server Recording.....	176
Fig. 193	Select integration type.....	177
Fig. 194	Recording architecture - tab Server Assignment	178
Fig. 195	Recording architecture - assign server - example.....	178
Fig. 196	Add recording server	179
Fig. 197	Recording architecture - activate recording architecture.....	180
Fig. 198	Servers - main view.....	181
Fig. 199	Toolbar Servers module.....	181
Fig. 200	Add server locations.....	182
Fig. 201	Delete server location	183
Fig. 202	Servers - tab Details.....	184
Fig. 203	Servers - tab usage	184
Fig. 204	Group field API Server	185
Fig. 205	Select storage expansion.....	186
Fig. 206	Group field Audio Analysis	187
Fig. 207	Select server for emotion detection.....	187
Fig. 208	Group field Recording Control/Key Management	187
Fig. 209	Group field Data Processing	188

Fig. 210	Select server	190
Fig. 211	Group field Replay	191
Fig. 212	Select server	192
Fig. 213	Group field Virtualization	193
Fig. 214	Servers module - tab Media Streamer	194
Fig. 215	Servers module - tab Replay Server Address Mapping	195
Fig. 216	Servers module - tab Key Management.....	197
Fig. 217	Servers module - tab Keystore/Virtualization	199
Fig. 218	PBX module - main view	200
Fig. 219	Toolbar PBX module	200
Fig. 220	Create new PBX - tab Details	201
Fig. 221	Tenants - main view - tab Extensions	203
Fig. 222	Assign extensions to tenants	204
Fig. 223	Remove extensions.....	205
Fig. 224	Select extensions	206
Fig. 225	Additional Data module main view	206
Fig. 226	Configure additional data	207
Fig. 227	Additional data - configure availability	207
Fig. 228	Integrations - main view	208
Fig. 229	Toolbar Integrations module	208
Fig. 230	Create integration type	209
Fig. 231	Integrations - select PBX.....	210
Fig. 232	Assign recording architecture - Multi-Server Recording.....	210
Fig. 233	Configuration steps of the integration	211
Fig. 234	Configuration step - Configure Recording Architecture.....	211
Fig. 235	Configuration step - Configure recording servers	212
Fig. 236	Overview of the add on of Genesys T-Server	213
Fig. 237	Configure add-on for Genesys T-Server	214
Fig. 238	Configure connection data	216
Fig. 239	Arbitrary assignment of the additional data	217
Fig. 240	Overview of Sparkassen FI ISP	218
Fig. 241	Configure add-on for Sparkassen FI ISP	219
Fig. 242	Arbitrary assignment of the additional data	220
Fig. 243	Configure add-on for OSCC	222
Fig. 244	Configure connection data	223
Fig. 245	Arbitrary assignment of the additional data	224
Fig. 246	Configure miscellaneous settings	225
Fig. 247	Activate integration.....	225
Fig. 248	Activated integration.....	226
Fig. 249	Deactivate integration	226
Fig. 250	Recording architectures - main view	227
Fig. 251	Toolbar Recording Architectures module	227

Fig. 252	Create recording architecture - Multi-Server Failover	228
Fig. 253	Recording architecture - tab Details - Multi-Server Failover	229
Fig. 254	Select integration type.....	230
Fig. 255	Recording Architecture - tab Server Assignment	231
Fig. 256	Recording Architecture - assign server - example	232
Fig. 257	Add Recording Server	233
Fig. 258	Recording architecture - activate recording architecture.....	234
Fig. 259	Servers - main view.....	234
Fig. 260	Toolbar Servers module.....	235
Fig. 261	Add server locations.....	236
Fig. 262	Delete server location	237
Fig. 263	Servers - tab Details.....	237
Fig. 264	Servers - tab usage	238
Fig. 265	Group field API Server	238
Fig. 266	Select storage expansion.....	240
Fig. 267	Group field Audio Analysis	240
Fig. 268	Select server for emotion detection.....	241
Fig. 269	Group field Recording Control/Key Management	241
Fig. 270	Group field Data Processing	242
Fig. 271	Select server	244
Fig. 272	Group field Replay	244
Fig. 273	Select server	246
Fig. 274	Group field Virtualization	246
Fig. 275	Servers module - tab Media Streamer	247
Fig. 276	Servers module - tab Replay Server Address Mapping.....	249
Fig. 277	Servers module - tab Key Management.....	250
Fig. 278	Servers module - tab Keystore/Virtualization	252
Fig. 279	PBX module - main view	253
Fig. 280	Toolbar PBX module	253
Fig. 281	Create new PBX - tab Details	255
Fig. 282	Tenants - main view - tab Extensions	257
Fig. 283	Assign extensions to tenants	258
Fig. 284	Remove extensions.....	259
Fig. 285	Select extensions	260
Fig. 286	Additional Data module main view	260
Fig. 287	Configure additional data	261
Fig. 288	Additional data - configure availability	261
Fig. 289	Integrations - main view	262
Fig. 290	Toolbar Integrations module	262
Fig. 291	Create integration type.....	263
Fig. 292	Integrations - select PBX.....	264
Fig. 293	Assign recording architecture - Multi-Server Failover	264

Fig. 294	Configuration steps of the integration	265
Fig. 295	Configuration step - Configure Recording Architecture.....	265
Fig. 296	Configuration step - Configure recording servers	266
Fig. 297	Overview of the add on of Genesys T-Server	267
Fig. 298	Configure add-on for Genesys T-Server	268
Fig. 299	Configure connection data	270
Fig. 300	Arbitrary assignment of the additional data	271
Fig. 301	Overview of Sparkassen FI ISP	272
Fig. 302	Configure add-on for Sparkassen FI ISP	273
Fig. 303	Arbitrary assignment of the additional data.....	274
Fig. 304	Configure add-on for OSCC.....	276
Fig. 305	Configure connection data	277
Fig. 306	Arbitrary assignment of the additional data.....	278
Fig. 307	Configure miscellaneous settings	279
Fig. 308	Activate integration.....	279
Fig. 309	Activated integration.....	280
Fig. 310	Deactivate integration	280
Fig. 311	Recording architectures - main view	281
Fig. 312	Toolbar Recording Architectures module.....	281
Fig. 313	Create recording architecture - Multi-Server Parallel Recording.....	282
Fig. 314	Recording architecture - tab Details - Multi-Server Parallel Recording.....	283
Fig. 315	Select integration type.....	284
Fig. 316	Recording architecture - server assignment device group 1	285
Fig. 317	Recording architecture - assign server - example.....	285
Fig. 318	Add recording server	286
Fig. 319	Recording architecture - activate recording architecture - example.....	287
Fig. 320	Servers - main view.....	288
Fig. 321	Toolbar Servers module.....	288
Fig. 322	Add server locations.....	289
Fig. 323	Delete server location	290
Fig. 324	Servers - tab Details.....	291
Fig. 325	Servers - tab usage	291
Fig. 326	Group field API Server	292
Fig. 327	Select storage expansion.....	293
Fig. 328	Group field Audio Analysis	294
Fig. 329	Select server for emotion detection.....	294
Fig. 330	Group field Recording Control/Key Management	294
Fig. 331	Group field Data Processing	295
Fig. 332	Select server	297
Fig. 333	Group field Replay	298
Fig. 334	Select server	299
Fig. 335	Group field Virtualization	300

Fig. 336 Servers module - tab Media Streamer	301
Fig. 337 Servers module - tab Replay Server Address Mapping	302
Fig. 338 Servers module - tab Key Management.....	304
Fig. 339 Servers module - tab Keystore/Virtualization	306
Fig. 340 PBX module - main view	307
Fig. 341 Toolbar PBX module	307
Fig. 342 Create new PBX - tab Details	308
Fig. 343 Tenants - main view - tab Extensions	310
Fig. 344 Assign extensions to tenants	311
Fig. 345 Remove extensions.....	312
Fig. 346 Select extensions	313
Fig. 347 Additional Data module main view	313
Fig. 348 Configure additional data	314
Fig. 349 Additional data - configure availability.....	314
Fig. 350 Integrations - main view	315
Fig. 351 Toolbar Integrations module	315
Fig. 352 Create integration type.....	316
Fig. 353 Integrations - select PBX.....	317
Fig. 354 Assign recording architecture - Multi-Server Parallel	317
Fig. 355 Configuration steps of the integration	318
Fig. 356 Configuration step - Configure Recording Architecture.....	318
Fig. 357 Configuration step - Configure recording servers	319
Fig. 358 Overview of the add on of Genesys T-Server	320
Fig. 359 Configure add-on for Genesys T-Server	321
Fig. 360 Configure connection data	323
Fig. 361 Arbitrary assignment of the additional data.....	324
Fig. 362 Overview of Sparkassen FI ISP	325
Fig. 363 Configure add-on for Sparkassen FI ISP	326
Fig. 364 Arbitrary assignment of the additional data.....	327
Fig. 365 Configure add-on for OSCC.....	329
Fig. 366 Configure connection data	330
Fig. 367 Arbitrary assignment of the additional data.....	331
Fig. 368 Configure miscellaneous settings	332
Fig. 369 Activate integration.....	332
Fig. 370 Activated integration.....	333
Fig. 371 Deactivate integration	333
Fig. 372 Path to the configuration file.....	334
Fig. 373 Configure parameters	335
Fig. 374 Servers module - Activate emotion detection.....	336
Fig. 375 Create integration - tab Recording Content Validation.....	337
Fig. 376 Select server for emotion detection.....	338
Fig. 377 Genesys Administrator - select T-Server	339

Fig. 378 Genesys Administrator - configure T-Server.....	339
Fig. 379 Genesys Administrator - select configuration server.....	340
Fig. 380 Genesys Administrator - configure configuration server	340
Fig. 381 Genesys Administrator - switch instances	341
Fig. 382 Genesys Administrator - configure switch instance	341
Fig. 383 Genesys administrator - create user	342

List of tables

Tab. 1	Licenses of ASC.....	10
Tab. 2	Licenses for Genesys.....	10
Tab. 3	Licenses for Sparkassen FI ISP optional	10
Tab. 4	Licenses for OpenScape Contact Center Campaign Director optional	10
Tab. 5	Login data - system provider	15
Tab. 6	Configure audio analysis.....	28
Tab. 7	Configure recording control/key management	29
Tab. 8	Data storage.....	29
Tab. 9	Configure replay.....	32
Tab. 10	Configure virtualization.....	34
Tab. 11	Create PBX	42
Tab. 12	Create integration type.....	50
Tab. 13	Configure recording servers.....	53
Tab. 14	Configure add-on for Genesys T-Server	56
Tab. 15	Configure connection data	57
Tab. 16	Configure CTIconnect module	60
Tab. 17	Configure connection data	61
Tab. 18	Configure CTIconnect module	63
Tab. 19	Configure connection data	64
Tab. 20	Configure audio analysis.....	80
Tab. 21	Configure recording control/key management	81
Tab. 22	Data storage.....	82
Tab. 23	Configure replay.....	84
Tab. 24	Configure virtualization.....	86
Tab. 25	Create PBX	95
Tab. 26	Create integration type.....	103
Tab. 27	Configure recording servers.....	106
Tab. 28	Configure add-on for Genesys T-Server	109
Tab. 29	Configure connection data	110
Tab. 30	Configure CTIconnect module	113
Tab. 31	Configure connection data	114
Tab. 32	Configure CTIconnect module	116
Tab. 33	Configure connection data	117
Tab. 34	Configure audio analysis.....	133
Tab. 35	Configure recording control/key management	134
Tab. 36	Data storage.....	135
Tab. 37	Configure replay.....	137
Tab. 38	Configure virtualization.....	139
Tab. 39	Create PBX	148
Tab. 40	Create integration type.....	156
Tab. 41	Configure recording servers.....	159

Tab. 42	Configure add-on for Genesys T-Server	162
Tab. 43	Configure connection data	163
Tab. 44	Configure CTIconnect module	166
Tab. 45	Configure connection data	167
Tab. 46	Configure CTIconnect module	169
Tab. 47	Configure connection data	170
Tab. 48	Configure audio analysis.....	187
Tab. 49	Configure recording control/key management	188
Tab. 50	Data storage.....	188
Tab. 51	Configure replay.....	191
Tab. 52	Configure virtualization.....	193
Tab. 53	Create PBX	201
Tab. 54	Create integration type.....	209
Tab. 55	Configure recording servers.....	212
Tab. 56	Configure add-on for Genesys T-Server	215
Tab. 57	Configure connection data	216
Tab. 58	Configure CTIconnect module	219
Tab. 59	Configure connection data	220
Tab. 60	Configure CTIconnect module	222
Tab. 61	Configure connection data	223
Tab. 62	Configure audio analysis.....	240
Tab. 63	Configure recording control/key management	241
Tab. 64	Data storage.....	242
Tab. 65	Configure replay.....	244
Tab. 66	Configure virtualization.....	246
Tab. 67	Create PBX	255
Tab. 68	Create integration type.....	263
Tab. 69	Configure recording servers.....	266
Tab. 70	Configure add-on for Genesys T-Server	269
Tab. 71	Configure connection data	270
Tab. 72	Configure CTIconnect module	273
Tab. 73	Configure connection data	274
Tab. 74	Configure CTIconnect module	276
Tab. 75	Configure connection data	277
Tab. 76	Configure audio analysis.....	294
Tab. 77	Configure recording control/key management	295
Tab. 78	Data storage.....	295
Tab. 79	Configure replay.....	298
Tab. 80	Configure virtualization.....	300
Tab. 81	Create PBX	308
Tab. 82	Create integration type.....	316
Tab. 83	Configure recording servers.....	319

Tab. 84	Configure add-on for Genesys T-Server	322
Tab. 85	Configure connection data	323
Tab. 86	Configure CTIconnect module	326
Tab. 87	Configure connection data	327
Tab. 88	Configure CTIconnect module	329
Tab. 89	Configure connection data	330

Glossary

API

Application Programming Interface

API server

Server on which the API service runs. (API=Application Programming Interface)

DNS

Domain Name System is a worldwide directory service which administrates the name domain of the Internet. Its 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

Monitor/Mirror/SPAN Port

Port mirroring is used to copy a network package, which passes a switch port, to another switch port.

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.

SBC

Session Border Controller

SDP

The Session Description Protocol describes properties of multimedia data streams. It serves to manage communication sessions and is used together with SIP and H.323 for instance within the IP telephony to deal codecs, transport protocols and addresses as well as for the transmission of meta data. (Source: Wikipedia 4th May 2017)

SIP

Session Initiation Protocol

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
