

EVOIPneo active for SIP



Administration manual for system providers

10/21/2021

Product line neo, version 6.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 © 2021 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.....	7
3.1	Hardware components	7
3.1.1	Recorder	7
3.2	Software components	7
3.3	External components	7
3.3.1	Supported PBXs and end devices	7
4	Installation requirements	9
4.1	Licenses	9
4.2	Information	9
5	Overview install and configure product.....	11
6	Installation	12
6.1	Install OpenScape Contact Center SDK-Runtime (optional).....	12
6.1.1	Basic setup.....	12
6.1.2	General patch.....	12
6.2	Install certificate for TLS encryption.....	12
6.2.1	Import certificate to recording server.....	12
6.2.1.1	Import customer-specific certificate to the recording server.....	13
6.2.1.2	Import PBX certificate to recording server	14
6.2.2	Import certificate to SIP client	15
6.2.2.1	Export TLS certificate from recording server.....	15
6.2.2.2	Import TLS certificate to SIP client.....	16
7	Configuration.....	17
7.1	System Configuration.....	17
7.1.1	Start application	17
7.1.2	Configure recording solution	18
7.1.2.1	Configure recording solution All-in-one Basic	18
7.1.2.2	Configure recording solution All-in-one Failover	74
7.1.2.3	Configure recording solution All-in-one Parallel Recording.....	132
7.1.2.4	Configure recording solution Multi-Server Recording	191
7.1.2.5	Configure recording solution Multi-Server Failover	249
7.1.2.6	Configure recording solution Multi-Server Parallel Recording	308
7.1.3	Synchronization options	366
7.1.3.1	Synchronization of recording control.....	366
7.1.3.2	Synchronization of system storage	368
7.1.4	Duplicates in parallel recording architectures	370
7.1.4.1	Configure duplicate detection.....	370
7.1.4.2	Additional data	372

7.1.4.3	Criteria to be ignored.....	373
7.1.5	Standby management for failover architectures.....	374
7.1.5.1	Standby management for All-in-one Failover.....	374
7.1.5.2	Standby management for Multi-Server Failover.....	376
7.1.6	Configure Recording Content Validation.....	377
7.1.7	Adjust neo configuration file.....	380
7.1.7.1	Adjust Recording Module for RTCP.....	380
7.1.7.2	Configure recording announcement.....	381
7.2	Configure CTIconnect add-on.....	384
7.2.1	Configure OpenScape Contact Center (optional).....	384
7.2.1.1	Create user for CTIconnect.....	384
7.2.2	Configure Genesys T-Server (optional).....	384
7.2.2.1	Configure IP address and port of the Genesys T-Server.....	384
7.2.2.2	Configure IP address and port of the Genesys Configuration Server.....	385
7.2.2.3	Configure switch instance in the Genesys Configuration Server.....	386
7.2.2.4	Create users for the Genesys Configuration Server.....	387
8	Troubleshooting.....	389
	List of figures.....	390
	List of tables.....	401
	Glossary.....	404

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} active for SIP provides the functionality which is necessary for an active IP recording of unencrypted and encrypted conversations in a SIP environment.

To record conversations, the recording server is added to the conference as participant. This can be done automatically if configured that way on the phone or on the PBX or initiated manually by another participant via the key control of the phone.



In this recording solution, the RX and TX audio data is saved as a mixed data stream in mono mode.

The additional data is extracted from the SIP signaling.

Since the recording is started by a conference call, the recording server does not receive the phone numbers of the other communication participants. To obtain this information nonetheless, different SIP headers can be configured as information source.

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} active for SIP

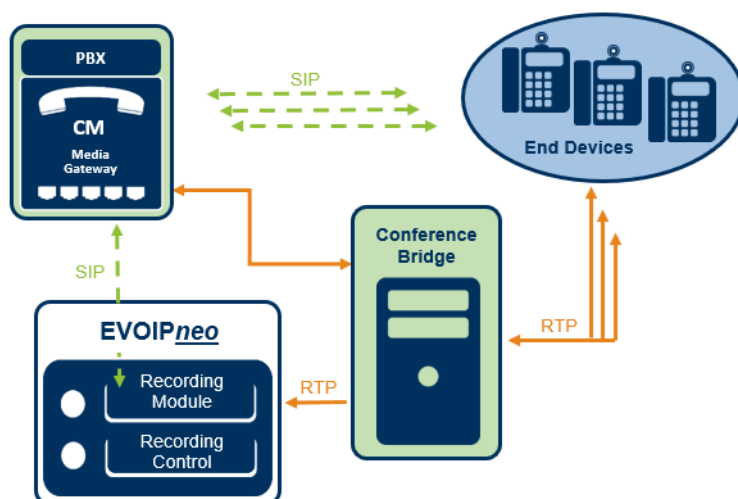


Fig. 1: Overview of the recording solution

3 System requirements



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



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



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

3.1 Hardware components



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



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

3.1.1 Recorder

For the recording solution you can use the following systems:

- EVOLUTION_{neo} eco
- EVOLUTION_{neo}
- EVOLUTION_{neo} XXL



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

3.2 Software components

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

3.3 External components



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

3.3.1 Supported PBXs and 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 3711 (SRTP)
- RFC 4566 (SDP Session Description Protocol)
- RFC 4568 (SDES)
- RFC 4733 (DTMF) optional

- RFC 6086 (DTMF via SIP INFO) optional

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

4 Installation requirements



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



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

4.1 Licenses

ASC

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

Tab. 1: Licenses of ASC



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

OpenScape Contact Center (optional)

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

Tab. 2: Licenses for OpenScape Contact Center optional

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

Genesys T-Server (optional)

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

Tab. 4: Licenses for Genesys

4.2 Information

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

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



In this recording solution, the [SIP](#) authentication methods *basic* and *auth* are supported.

5

Overview install and configure product

The following steps have to be carried out:

1. Install *neo* software
2. Configure PBX and conference bridge
 - 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.
 - Create, configure, and activate integration
 - Configure recording architecture
Link the integration to the previously created recording architecture.
 - Global recording settings
Configuration of port and transport protocol for SIP signaling
 - Configure recording servers
Configuration of the parameters of the recording server, e. g. IP address, incoming port for RTP, and extensions.
 - Configure add-on
The add-on is disabled by default.
Optionally, you can configure the following add-ons for this recording solution:
OpenScape Contact Center
Sparkassen FI ISP
Genesys T-Server
 - Configure miscellaneous settings
Optional configuration of participant information in an additional data field

6 Installation



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



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



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

6.1 Install OpenScape Contact Center SDK-Runtime (optional)

If you would like to use the software OpenScape Contact Center, you have to additionally install the following components.

Check which version of the OpenScape Contact Center is used, e. g. V8 R2 GP03.

Then install the *basic setup* for the release and subsequently the appropriate *general patch*, in the example GP03.

6.1.1 Basic setup

1. From the installation path, extract the ZIP file which corresponds to the version of your server, e. g. `\ASC\ASC Product Suite\thirdparty\OSCCRuntimeSDK\ SDK_Runtime_V8R2.zip`.
2. Execute the installation file `setup.exe` and follow the instructions of the installation wizard.

6.1.2 General patch

Start the Windows Installer Patch `OSCC80R2G03SDKRuntime.msp` under `\ASC\ASC Product Suite\thirdparty\OSCCRuntimeSDK\`.

6.2 Install certificate for TLS encryption

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

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

- [chapter "Import certificate to recording server"](#), p. 12
- [chapter "Import certificate to SIP client"](#), p. 15

6.2.1 Import certificate to recording server

To enable the recording server to confirm the certificate of the [SIP](#) client, the certificate must be available on the recording server.

There are 2 possibilities to import [TLS](#) certificates:

- *Installing a customer-specific certificate*, see [chapter "Import customer-specific certificate to the recording server"](#), p. 13
- *Installing PBX certificate already existing on the SIP client*, see [chapter "Import PBX certificate to recording server"](#), p. 14

6.2.1.1 Import customer-specific certificate to the recording server

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

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

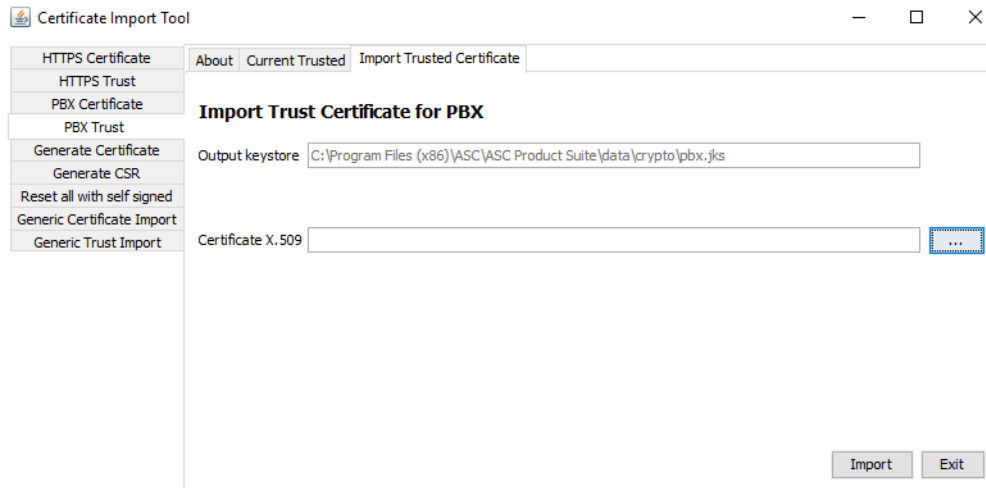


Fig. 2: Selection of the certificate

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

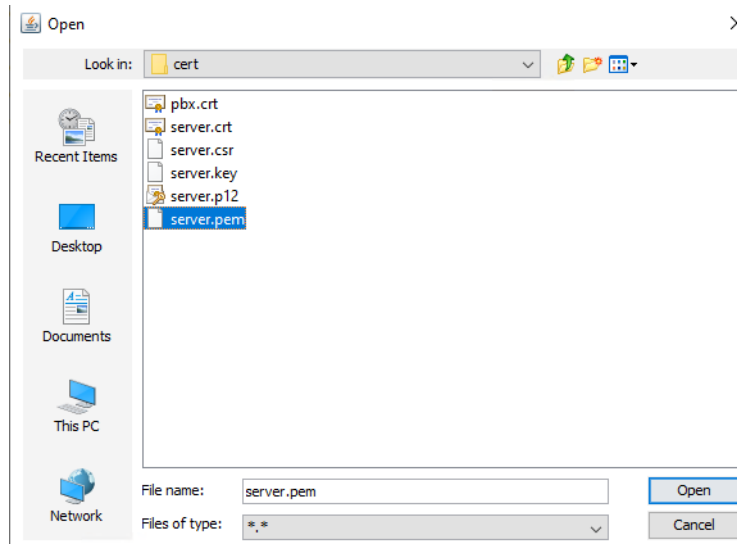


Fig. 3: Import certificate

6. Select the certificate file *server_certificate.pem* that you have copied from the [SIP](#) client.
7. Click on the button *Open*.
 ⇒ The window to enter the alias appears.

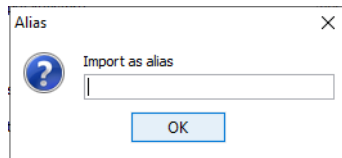


Fig. 4: Confirm alias

8. Enter the name of the [SIP](#) client.
9. Click on the button *OK* to confirm the alias.
 - ⇒ A message will inform you about the successful import.

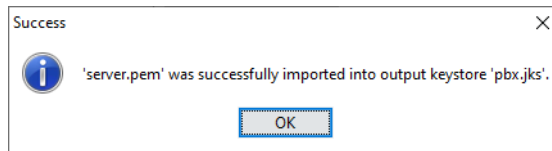


Fig. 5: Message - Successful import

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

6.2.1.2 Import PBX certificate to recording server

By means of this function you overwrite the delivered certificate on the recording server with the certificate of the [SIP](#) client or of the [PBX](#).

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

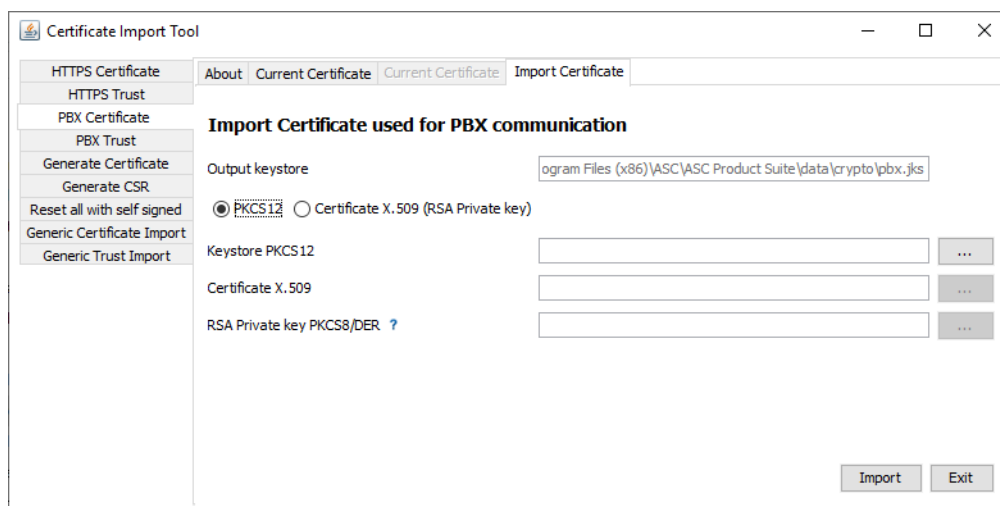


Fig. 6: Selection of the certificate

3. Select the menu item *PBX Certificate* in the navigation bar.
 - By means of this function you overwrite the delivered certificate on the recording server.
4. Select the tab *Import Certificate*.
5. Select the format of the certificate.
6. Click on the button *...* next to the respective entry field to select the certificate file.
7. Select the respective certificate file that you have copied from the [SIP](#) client.
8. Click on the button *Open*.
 - ⇒ The window to enter the alias appears.

9. Enter the alias of the **SIP** client.
10. Click on the button *OK* to confirm the alias.
 - ⇒ A message will inform you about the successful import.
11. Click on the button *OK* to confirm the success message.
12. Click on the button *Exit* to close the program *Certificate Import Tool*.

6.2.2 Import certificate to SIP client

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

6.2.2.1 Export TLS certificate from recording server

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

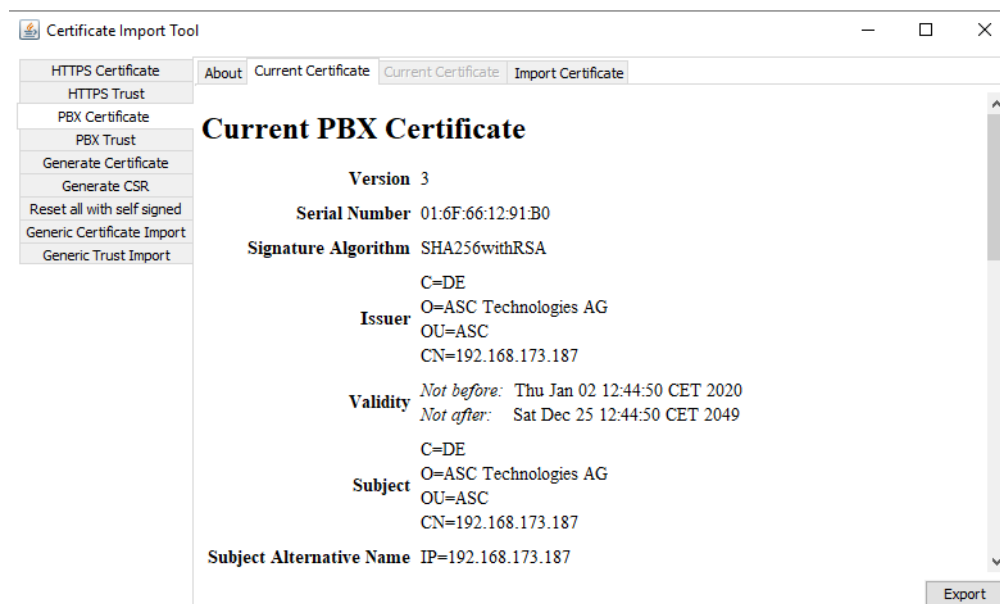
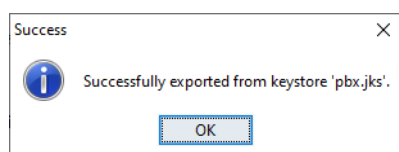


Fig. 7: Export PBX certificate from recording server

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



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

6.2.2.2 Import TLS certificate to SIP client

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

7 Configuration

7.1 System Configuration



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

7.1.1 Start application

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

1. To start the application directly on the server, double-click on the shortcut System Configuration.

To access the application from a computer via the web, enter the following URL in the address bar:

https://<System-IP>/SystemConfiguration.

If you have configured customer-specific ports, you have to include the port in the URL:

https://<System-IP>:<Port>/SystemConfiguration.

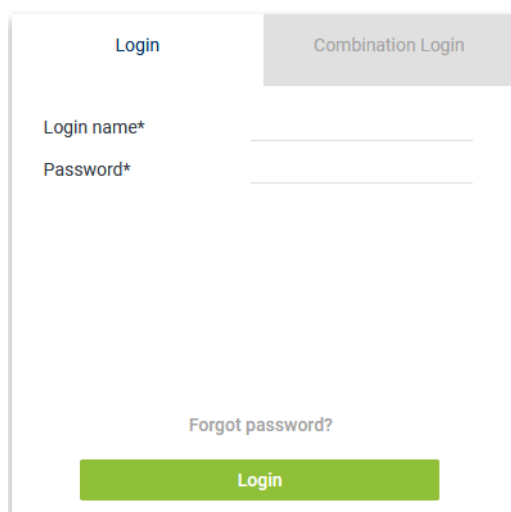


Fig. 8: System Configuration - web interface

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

Login data for the administrator of the system provider:

User name:	<i>system-admin</i>
<i>neo</i> 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 <i>neo</i> 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 <i>neo</i> version ≥ 6.3 , the changed password remains.
<i>neo</i> 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.

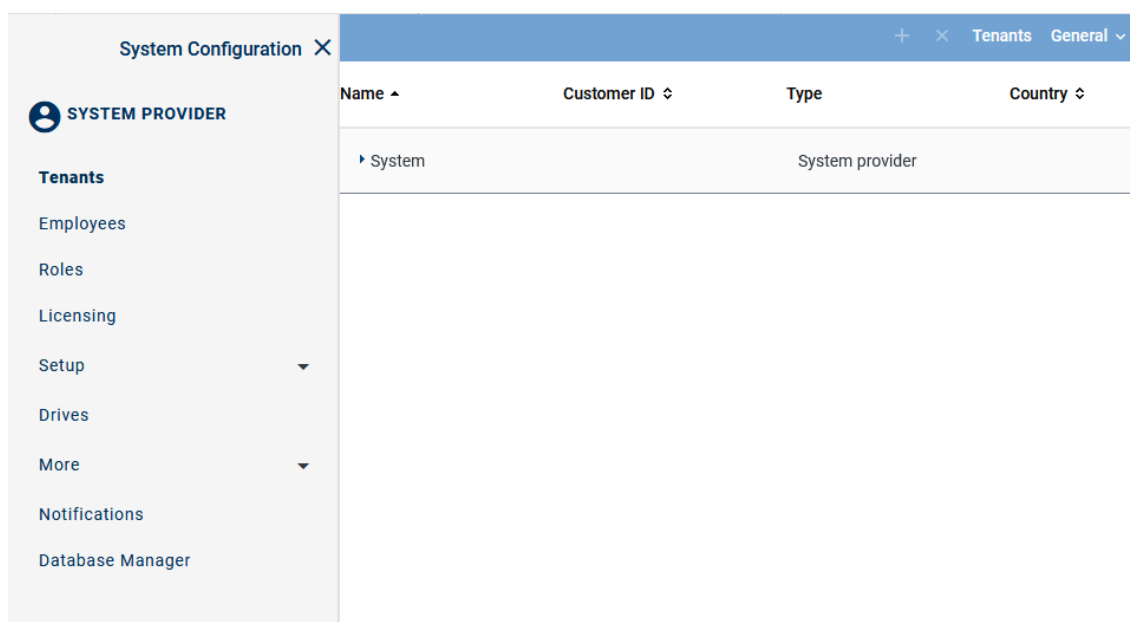


Fig. 9: System Configuration - main view:

7.1.2 Configure recording solution

Supported recording architectures

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

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

7.1.2.1 Configure recording solution All-in-one Basic

7.1.2.1.1 Create recording architecture

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

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

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

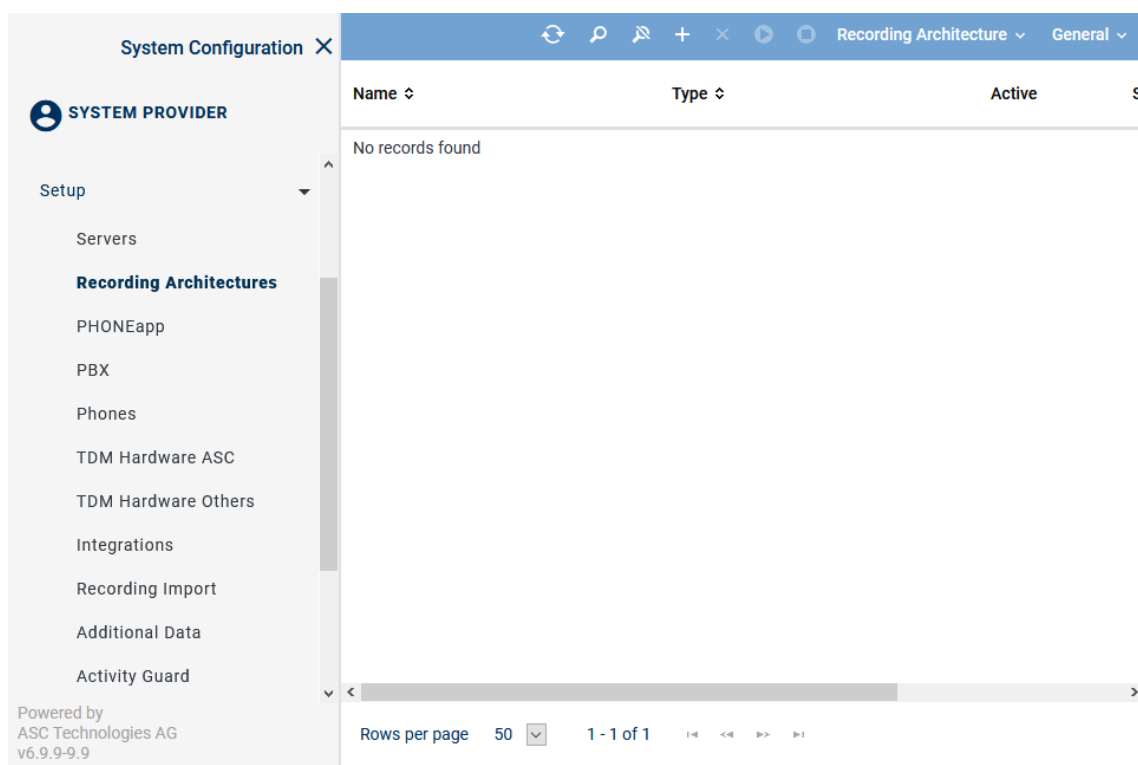




Fig. 10: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. <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. </div> <div> ✗ = 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. </div> <div> ✗ = 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. 11: Toolbar Recording Architectures module

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

		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<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*.

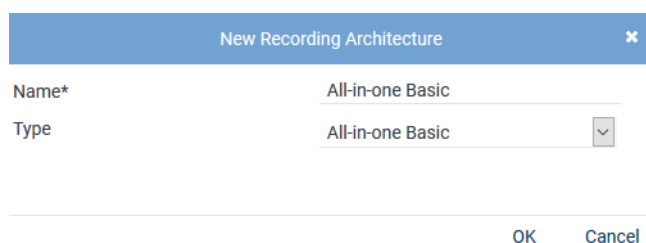
Create recording architecture All-in-one Basic

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



Depending on the selected recording architecture type, the following configuration steps vary. The following configuration steps are exemplary for the recording architecture *All-in-one Basic Recording*.

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



New Recording Architecture

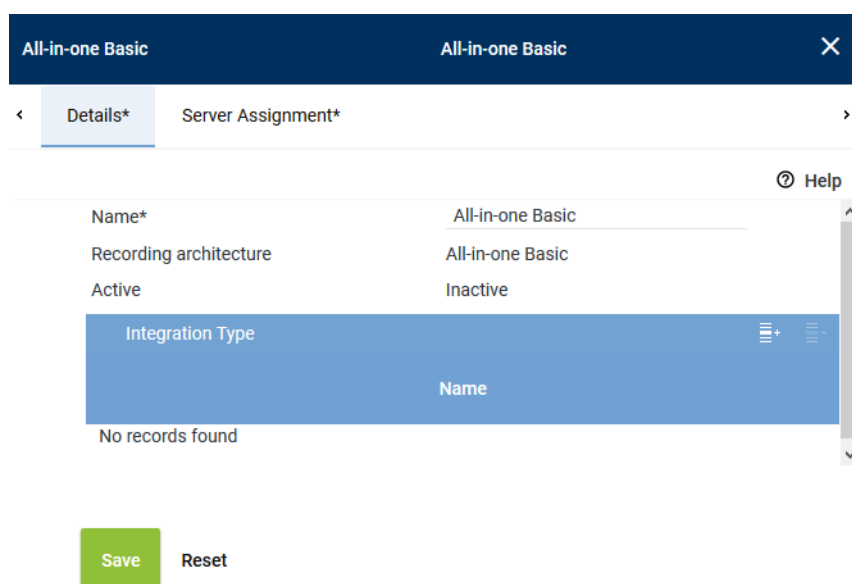
Name* All-in-one Basic

Type All-in-one Basic

OK Cancel

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



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

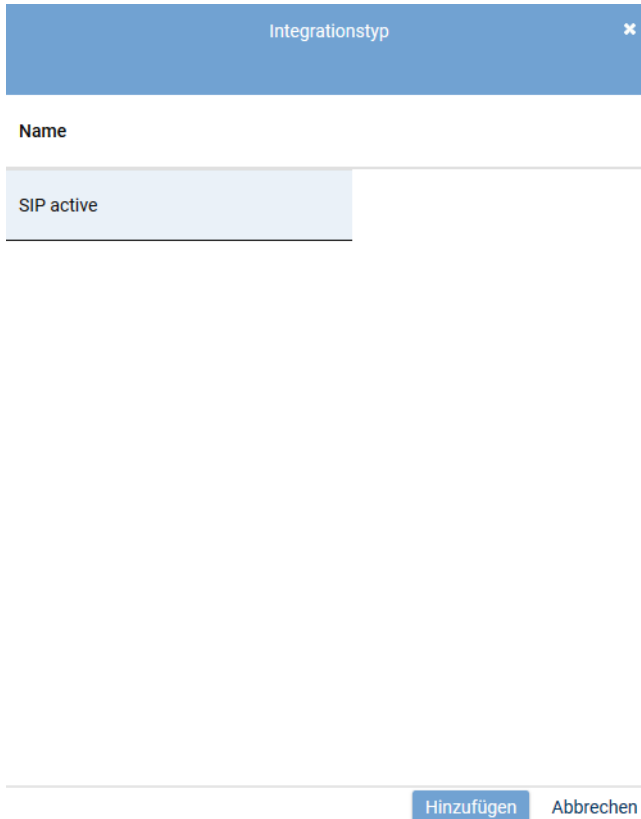
No records found

Save Reset

Fig. 13: Recording architecture - tab Details

Add integration type

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



Integrationstyp

Name

SIP active

Hinzufügen Abbrechen

Fig. 14: Select integration type



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

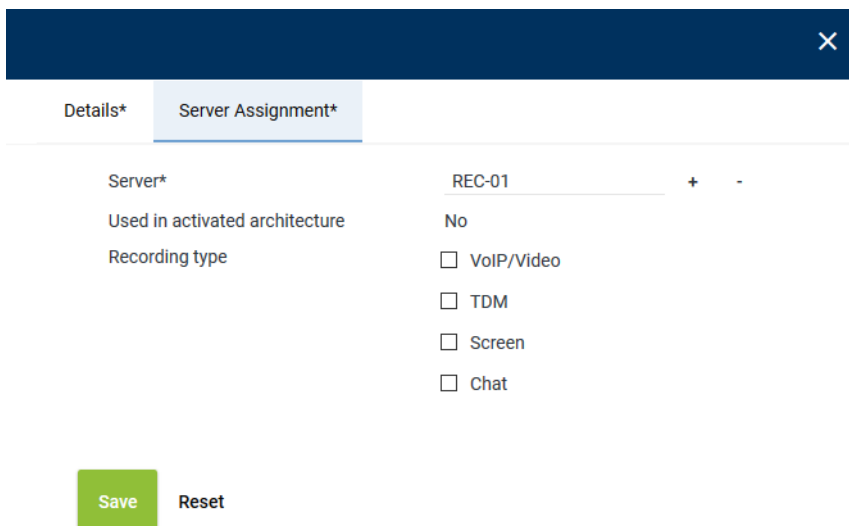


Any number of integration types can be assigned to a recording architecture.

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

Assign server for All-in-one Basic

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



Details* Server Assignment*

Server* REC-01 + -

Used in activated architecture No

Recording type

☐ VoIP/Video

☐ TDM

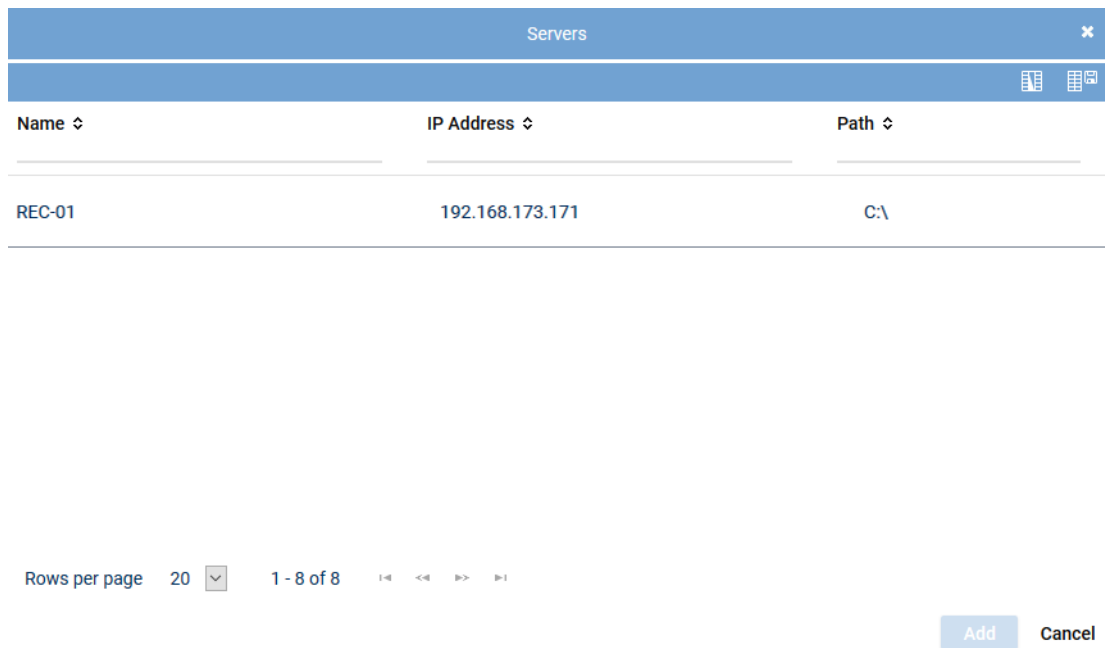
☐ Screen

☐ Chat

Save Reset

Fig. 15: Recording architecture - tab Server Assignment

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



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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 16: Recording architecture - assign server

3. Select the respective server.



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

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

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen

☐ Chat


Save Reset

Fig. 17: Recording architecture - activate recording variant



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

Activate recording architecture

1. Click on the button *Save*.
2. Select the recording architecture in the main view so that the icon  (*Activate*) in the 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. 18: Recording architecture - activate recording architecture

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



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



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

7.1.2.1.2 Configure server

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

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

System Configuration					
<div>SYSTEM PROVIDER</div> <div>Setup</div> <div>Servers</div> <div>Recording Architectures</div> <div>PHONEapp</div> <div>PBX</div> <div>Phones</div> <div>TDM Hardware ASC</div> <div>TDM Hardware Others</div> <div>Integrations</div> <div>Recording Import</div> <div>Additional Data</div> <div>Activity Guard</div>	<div>Servers</div> <div>General</div> <table> <tr> <th>Name</th><th>IP Address</th></tr> <tr> <td>REC-01</td><td>192.168.173.171</td></tr> </table>	Name	IP Address	REC-01	192.168.173.171
Name	IP Address				
REC-01	192.168.173.171				

Fig. 19: 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.

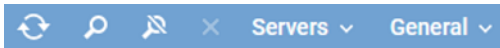







Fig. 20: Toolbar Servers module

	<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 <i>neo</i> 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. 25.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<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.

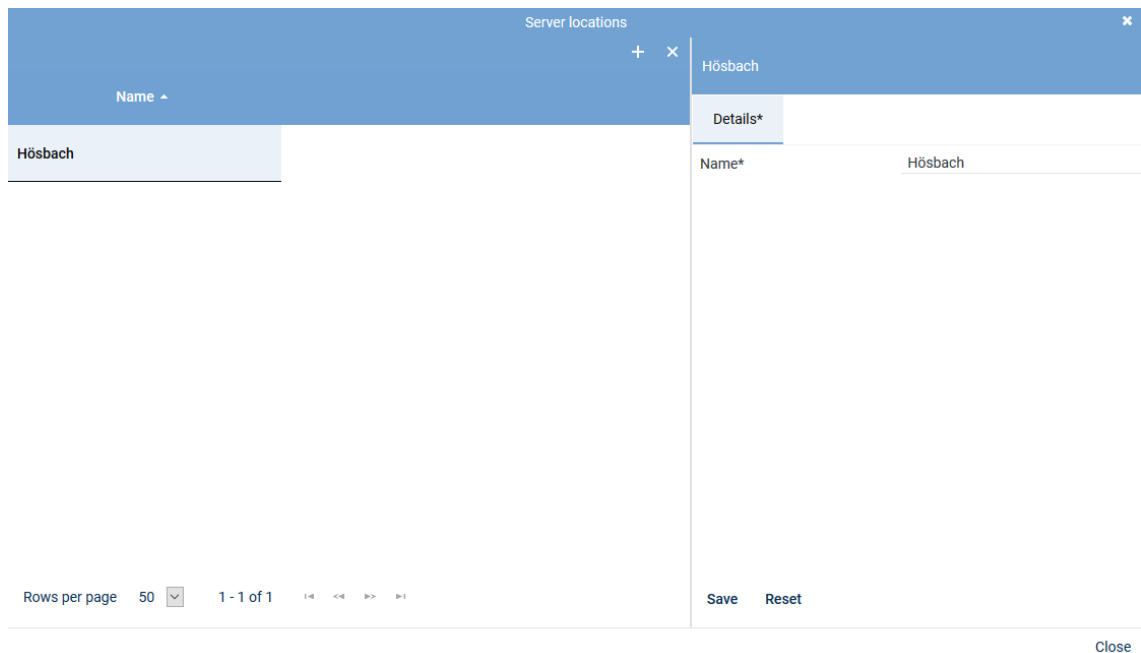



Fig. 21: Add server locations

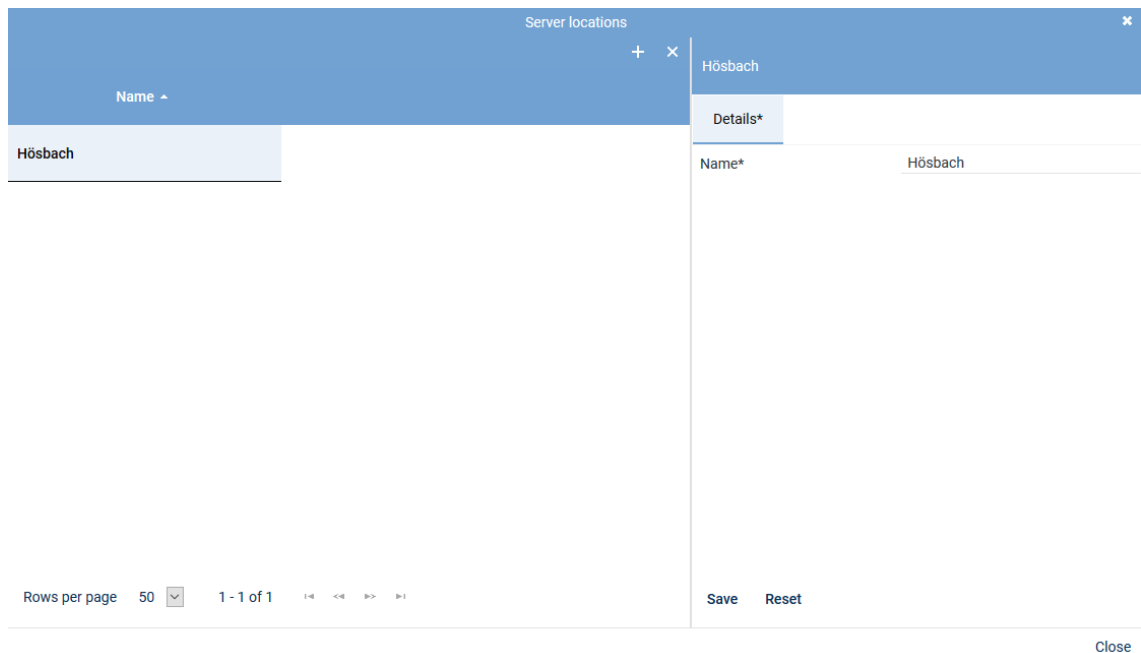
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

Delete server location



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

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



Server locations

Name
Hörsbach

Details*


Name* Hörsbach

Rows per page 50 1 - 1 of 1

Save Reset

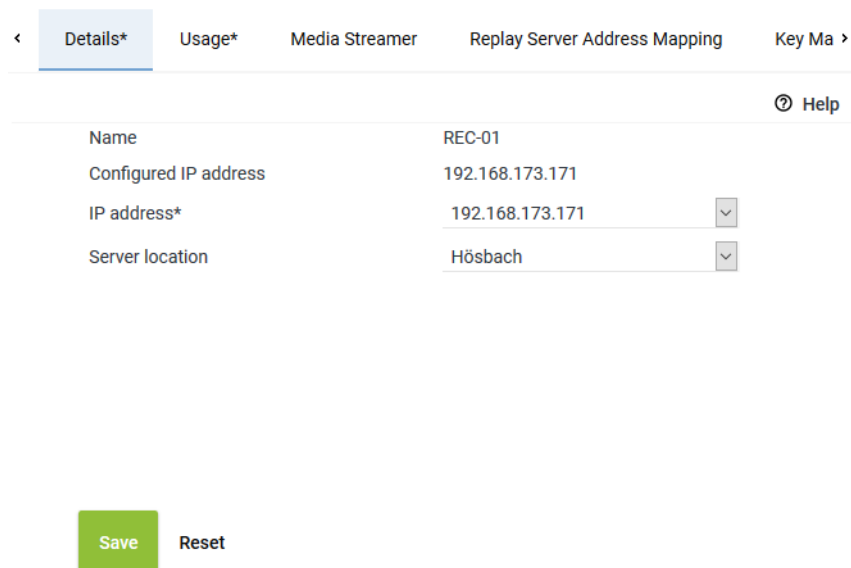
Close

Fig. 22: 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. 23: 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.

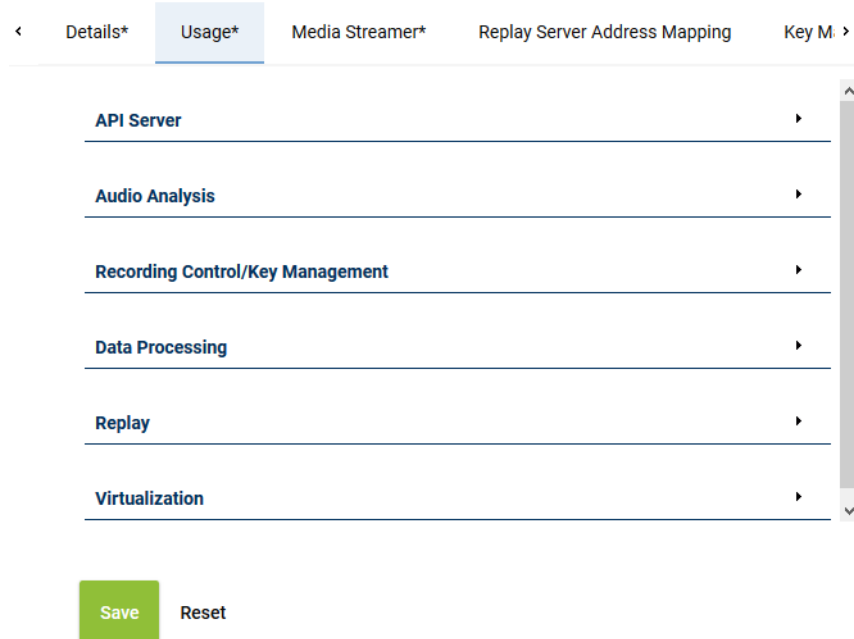


Fig. 24: Servers - tab usage

Group field API Server

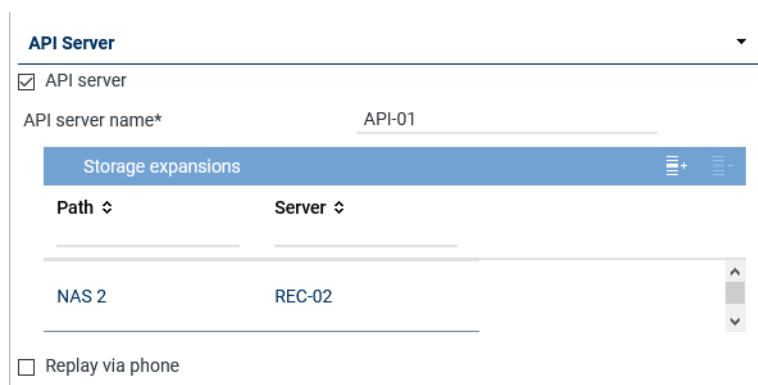




Fig. 25: Group field API Server

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


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

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

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

Parameter	Value/Description
	<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. 39.</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. 30. • 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 <i>neo</i> 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. 37. 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. 26: Select storage expansion

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


Group field Audio analysis

Audio Analysis

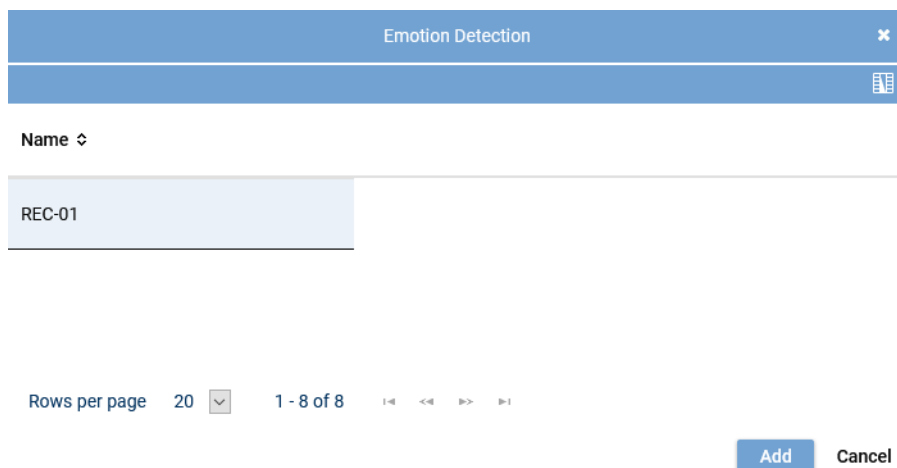
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 27: 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. 6: Configure audio analysis



Emotion Detection

Name ↕

REC-01

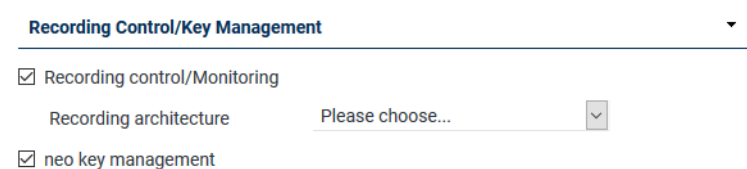
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 28: 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/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 29: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 30: 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. 34. 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. 34. 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 <i>neo</i> to <i>neo</i>, 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. 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.



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

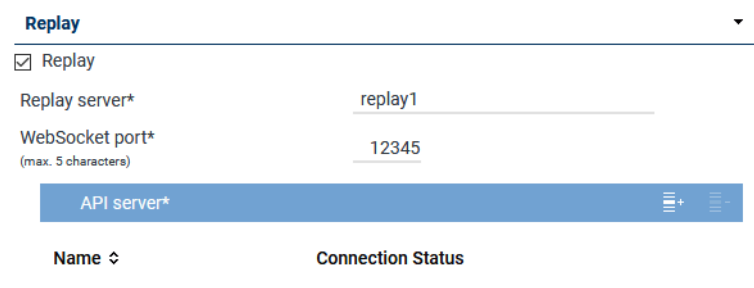
Fig. 31: Select server



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

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

Group field Replay





Replay

☒ Replay

Replay server*



WebSocket port*
(max. 5 characters)

API server*  

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

Fig. 32: 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 <i>POWERplay</i> 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. 35. • By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 9: Configure replay

Search and replay functions



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

Add API server to a list

The replay server required the services of an [API](#) server. The configuration must be as follows:

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


- If the replay server runs on a separate server, you must assign at least one **API** server that the replay server can address.
 - If several **API** servers are available in the network, you can assign further **API** servers in addition to the local **API** server. The assigned **API** servers are addressed in order. For this reason, the local **API** server should always be first in the list.
1. To assign an **API** server, click on the icon  (*Add*) in the toolbar of the list *API Server*.
 2. Select the server from the list on which the **API** service is running.



Fig. 33: Select server



Only those servers are available on which the **API** service has been installed and activated.
See [chapter "Group field API Server", p. 28](#).

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

Group field Virtualization



Fig. 34: Group field Virtualization

Parameter	Value/Description
<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. 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.

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

Save

Reset

Fig. 35: 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. 43.</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 <i>8000</i>.</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> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</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: <i>5062</i></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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<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 <i>5060</i>.</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. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.



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

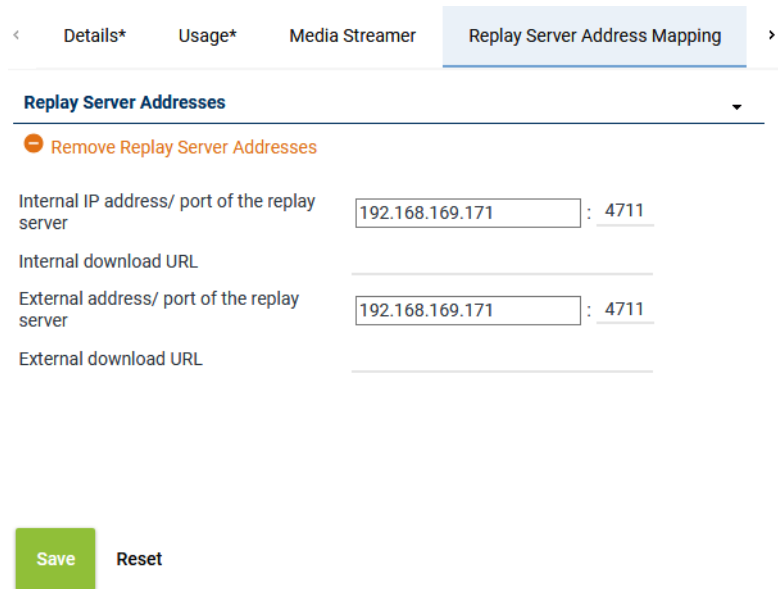


Fig. 36: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

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



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

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



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



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

Tab Key Management

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

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

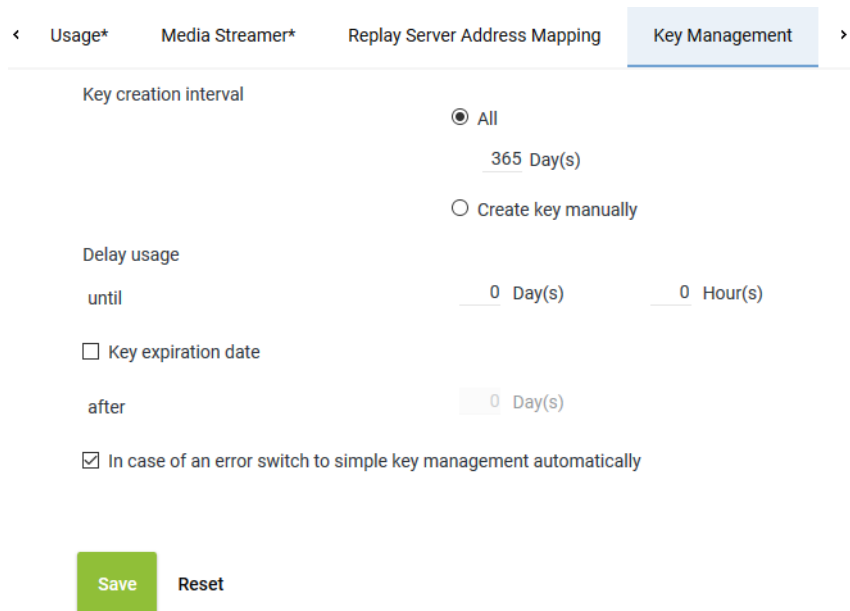


Fig. 37: Servers module - tab Key Management

Key creation interval

Select whether a key is supposed to be generated automatically or manually. Select one of the following options:

- *All*

Select the intervals in which a new key is supposed to be generated automatically.

Possible time interval: 1 to 365 days

Default value: 365 days

- *Create key manually*

Select that a key is supposed to be generated manually.

Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.

<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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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*

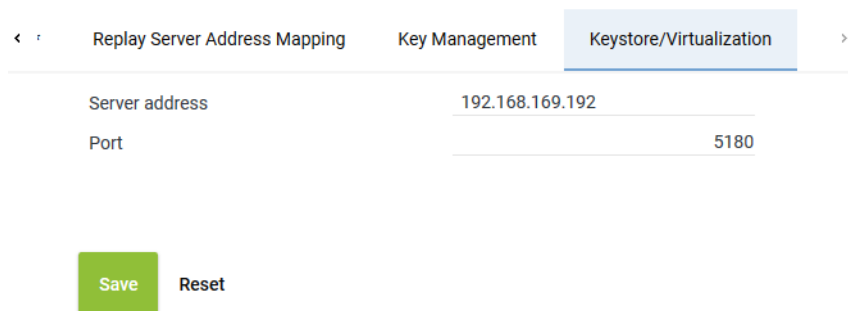
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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 currently 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 of the form, there are two buttons: a green 'Save' button and a grey 'Reset' button.

Fig. 38: 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*.

7.1.2.1.3 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.

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

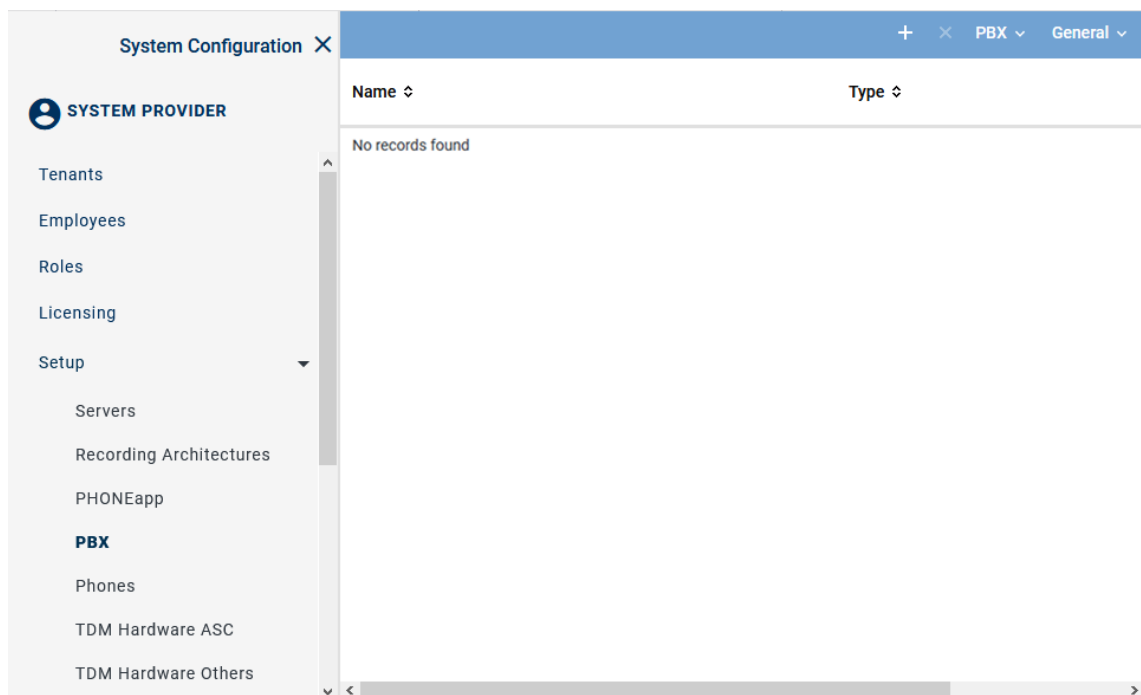


Fig. 39: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

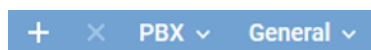




Fig. 40: Toolbar PBX module


	<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. 41: 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 <i>094</i>.
Area code	Enter the area code without the preceding 0, e. g. 6021.
Net code	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 11: Create PBX

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

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

Tab. 12: PBX parameters with complete phone number

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

7.1.2.1.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

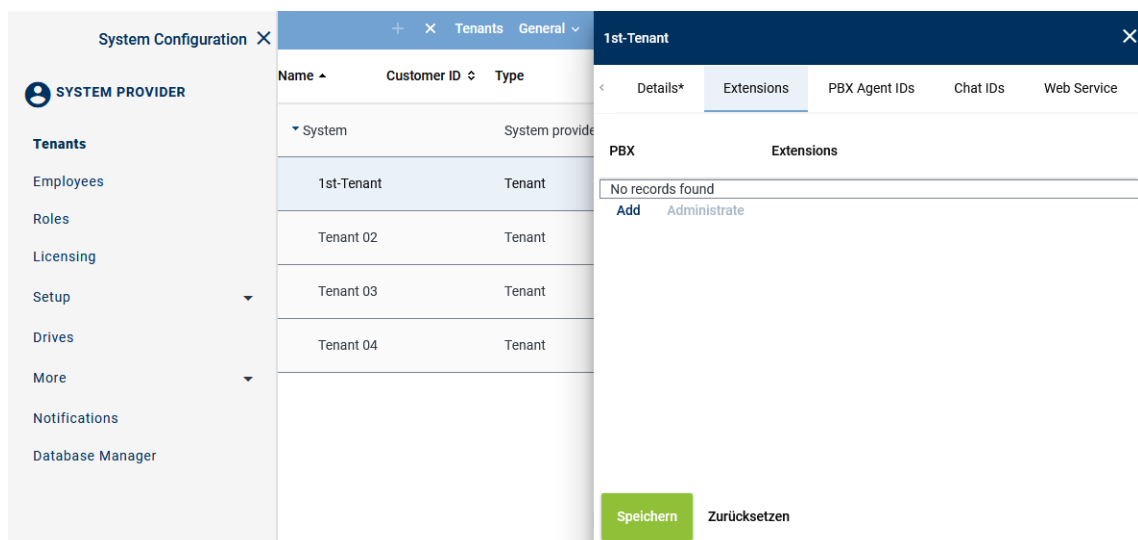
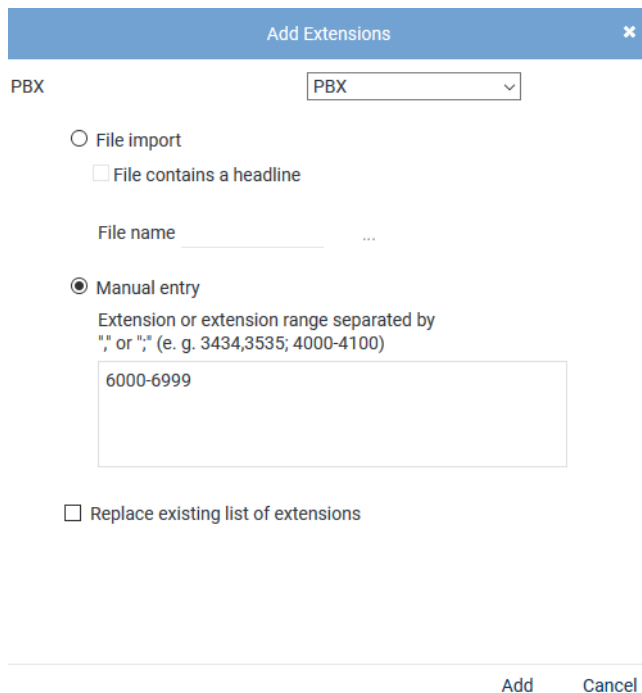


Fig. 42: Tenants - main view - tab Extensions

Add extensions

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



⇒ The following window appears:



The screenshot shows the 'Add Extensions' window. At the top is a blue header bar with the title 'Add Extensions' and a close button (X). Below the header, there is a label 'PBX' and a dropdown menu currently showing 'PBX'. Underneath, there are two radio button options: 'File import' and 'Manual entry'. The 'Manual entry' option is selected. Below 'File import' is a checkbox labeled 'File contains a headline'. Below 'Manual entry' is a text input field containing '6000-6999'. Below the input field is a checkbox labeled 'Replace existing list of extensions'. At the bottom right of the window are two buttons: 'Add' and 'Cancel'.

Fig. 43: Assign extensions to tenants

- 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"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <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.

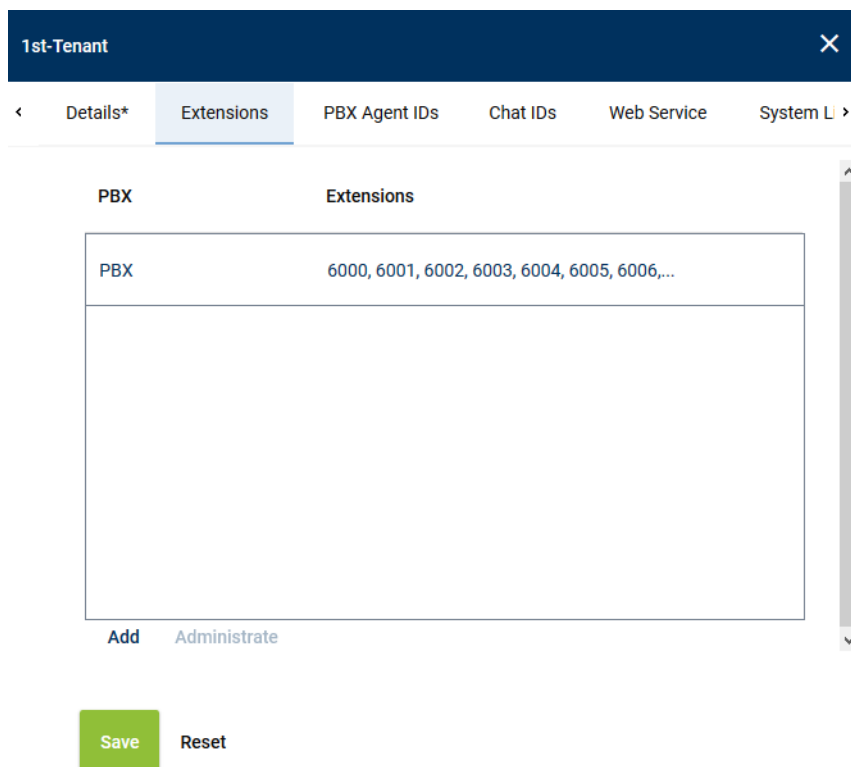
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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.



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. 44: 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. 45: 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.

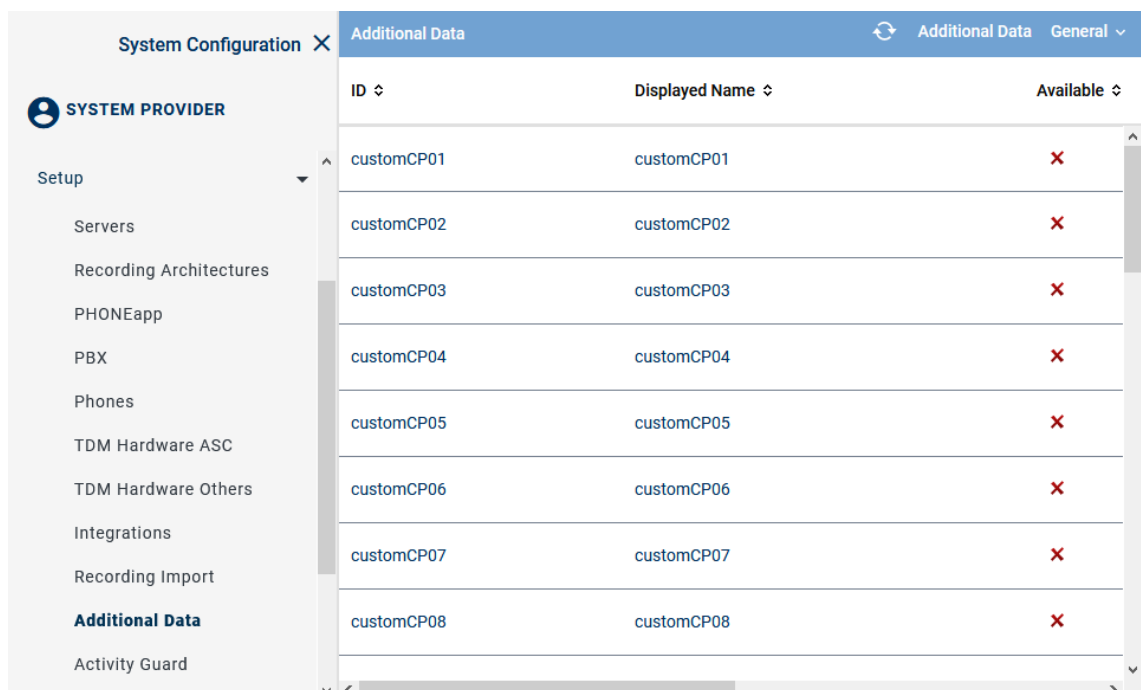


Fig. 46: Additional Data module main view

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. 47: 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. 48: 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:

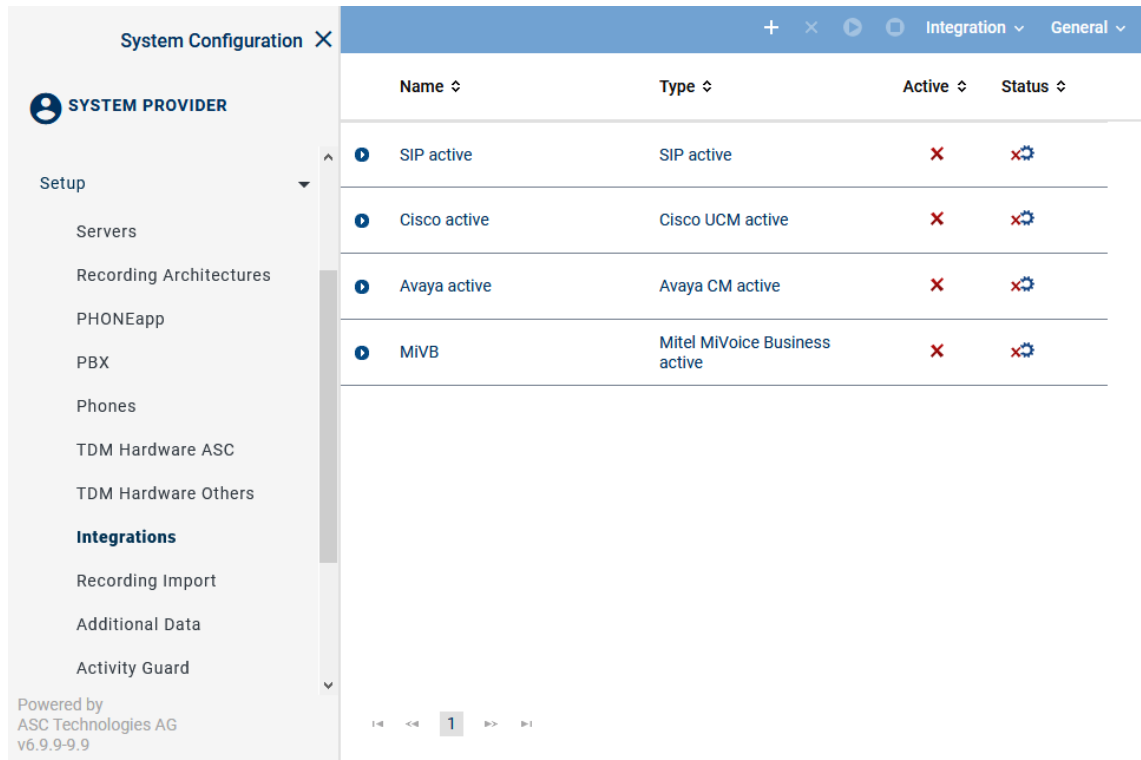




Fig. 49: Integrations - main view

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. 50: 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.

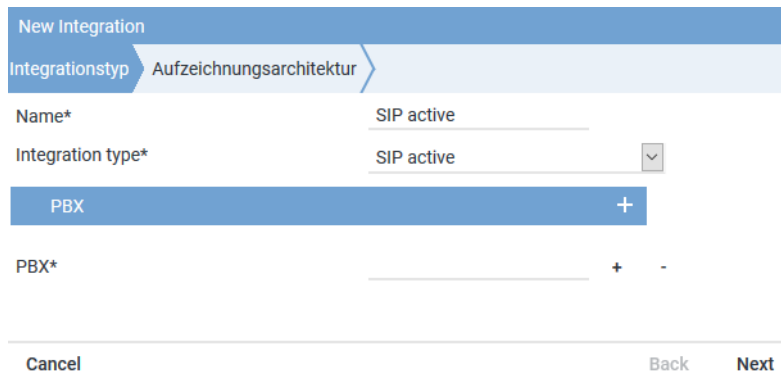



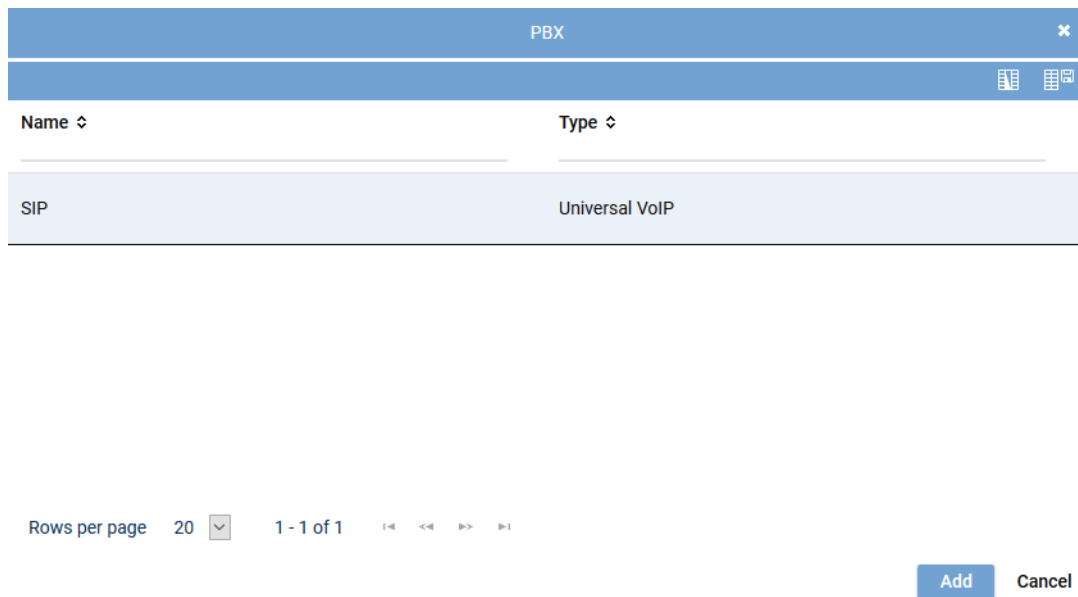
Fig. 51: Create integration type

- 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 13: 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. 52: 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. 53: 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:







SIP active		SIP active	X	⚙️
Step	Configuration			
Configure recording architecture	✓ 			
Global recording settings	✗ 			
Configure recording servers	✗ 			
Configure add-on	✓ 			
Configure miscellaneous settings	✓ 			

Fig. 54: 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. 55: 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.

Global recording settings for All-in-one Basic

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

Step: Global Recording Settings
✕

Details *

SIP Header Tagging*

Transport protocol
UDP ▼

Port SIP signaling*
5060

Activate SIP authentication
☒

User name for the SIP registration
123456

Password for the SIP registration
••••••

Activate PBX connection
☒

SIP registration expiration*
3600

PBX IP address*
192.168.170.178

PBX port*
5060

Activate SMS recording
☒

Save Cancel

Fig. 56: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
<i>Port SIP signaling</i>	<p>Enter the port for the SIP signaling, where the recording server is expecting the signaling.</p> <p>Default value for UDP and TCP is 5060.</p> <p>Default value with TLS encryption is 5061.</p> <p>NOTICE! If you would like to use several integrations, you have to configure a separate SIP port for each integration.</p> <p>NOTICE! If you would like to use a media streamer for replay, configure another SIP port for it, too. In case of communication issues with the media streamer, this could otherwise affect the recording.</p>
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password of the SIP registration</i>	Enter the password, if an authentication for the SIP registration is used.
<i>Activate PBX connection</i>	Activate this check box if the recording server is supposed to register itself on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration runs out, e. g. 3600.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port on which the SIP signaling is sent to the PBX . The default value is 5060.

Parameter	Value/Description
<i>Activate SMS recording</i>	Activate the check box if you would like to use SMS recording.

Tab. 14: Global recording settings

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

Tab SIP Header Tagging

- If you would like to configure the SIP header tagging, click on the tab *SIP Header Tagging*.

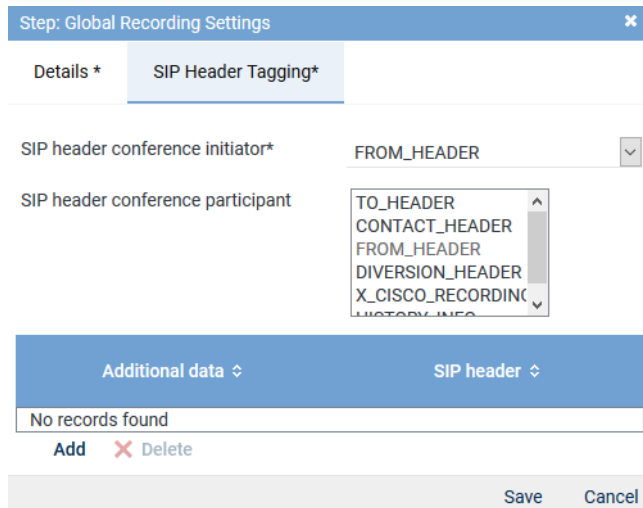


Fig. 57: Tab SIP Header Tagging Configure sources

- Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

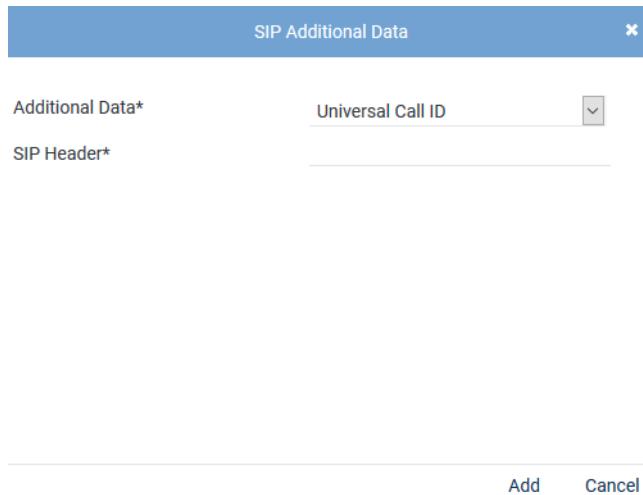
Tab. 15: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down.
To deselect an entry, click on it again without releasing the [Ctrl] key.

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



SIP Additional Data

Additional Data* Universal Call ID

SIP Header*

Add Cancel

Fig. 58: SIP Additional Data



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


- Enter the following parameters:

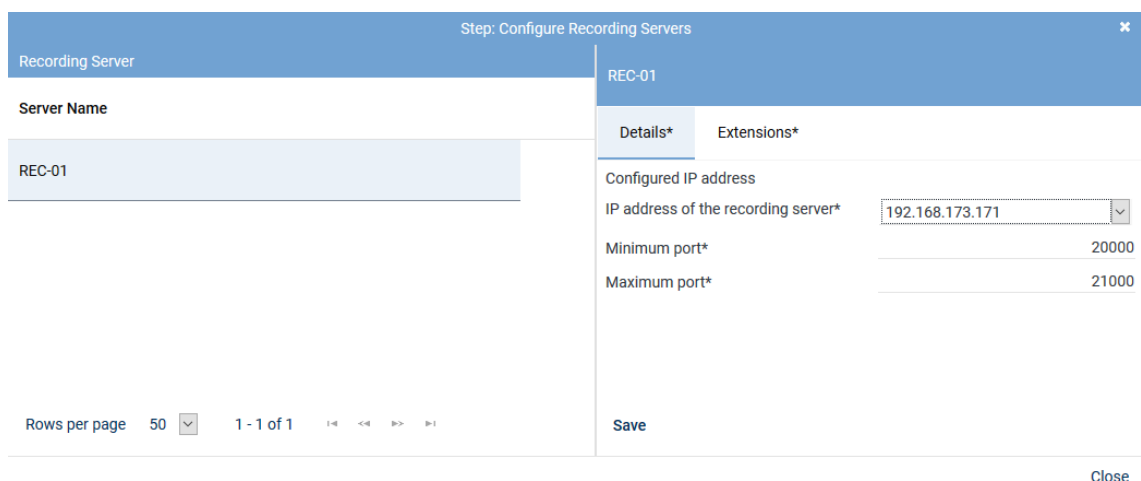
Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.

Tab. 16: Configure SIP conversation parameters

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

Configure recording server for All-in-one Basic

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



Step: Configure Recording Servers

Recording Server

Server Name

REC-01

REC-01

Details* Extensions*

Configured IP address

IP address of the recording server* 192.168.173.171

Minimum port* 20000

Maximum port* 21000

Save

Rows per page 50 1 - 1 of 1

Close

Fig. 59: Configuration step - Configure recording servers

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

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

Tab. 17: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**. In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

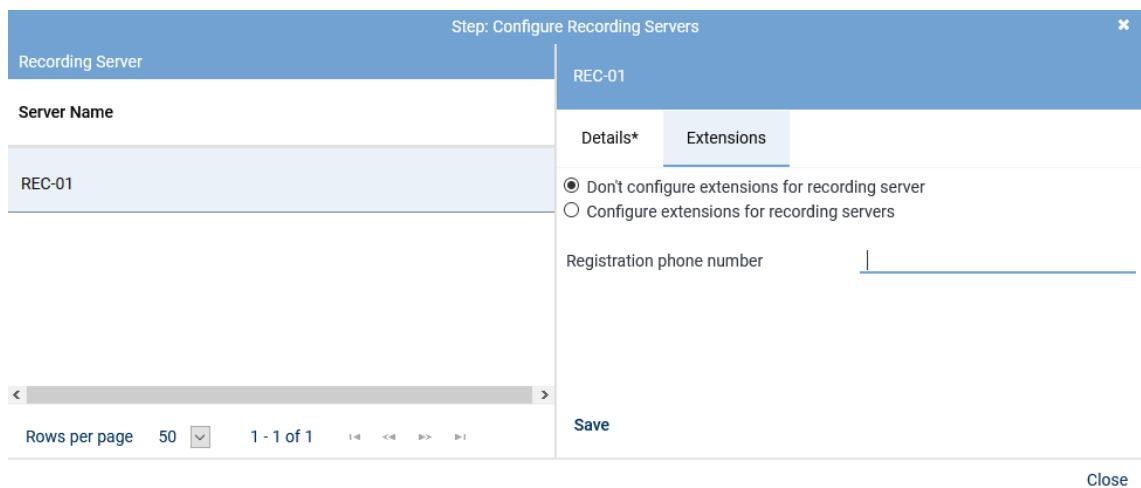


Fig. 60: Recording server - Configure extension for SIP trunk

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a **SIP** trunk phone number instead.



If you do not define a phone number for the **SIP** trunk of the recording server, all incoming **SIP** connections are accepted without being examined.

Registration phone number Enter a registration phone number for the **SIP** trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the **SIP** trunk, see chapter "Global recording settings for All-in-one Basic", p. 54.

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

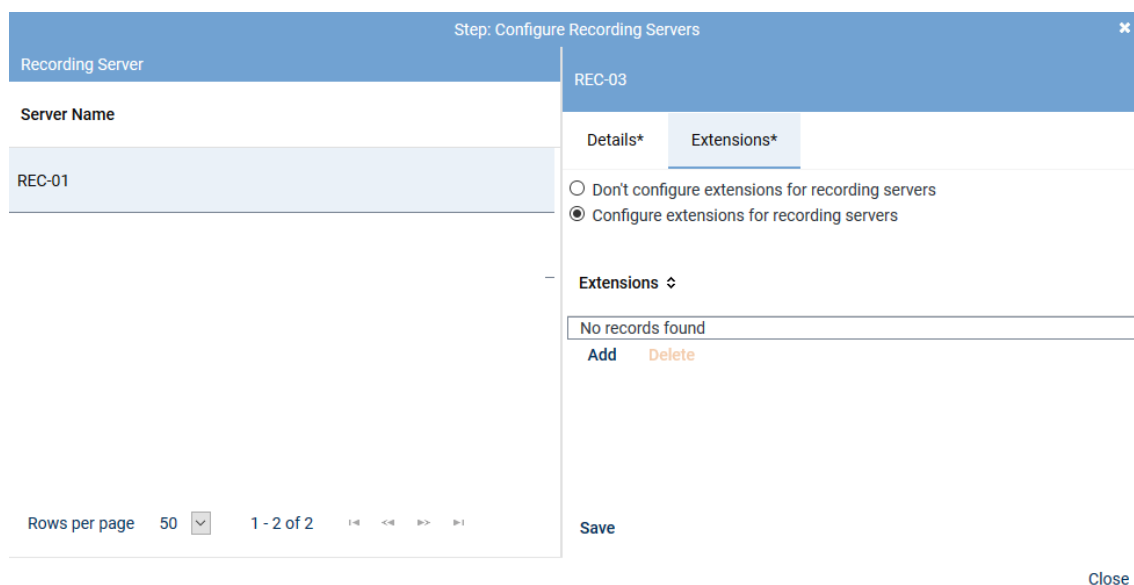


Fig. 61: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

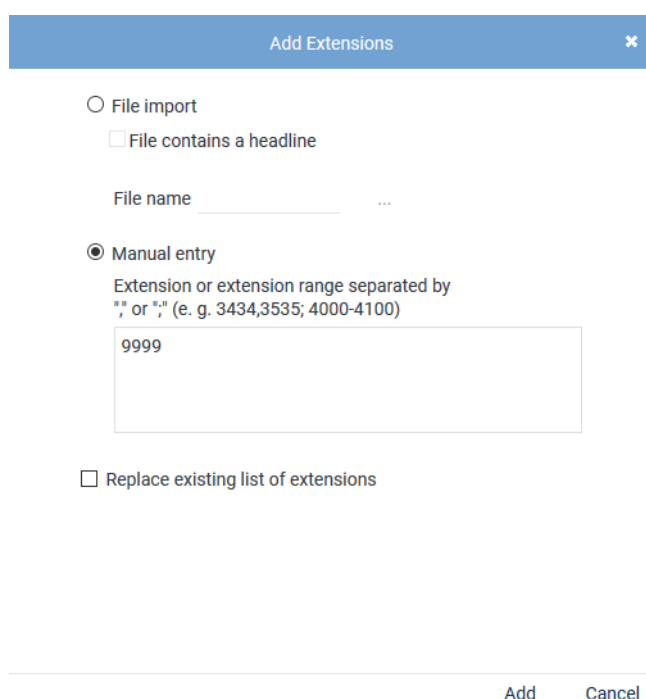


Fig. 62: Add extensions

3. In the window *Add Extensions*, enter either the individual extensions or an extension range that the recording server is supposed to use to register at the PBX.
4. Click on the button *Add*.
 - ⇒ The extensions are added in the table of extensions.
5. 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*.
6. The configured extensions now appear in the detail view.

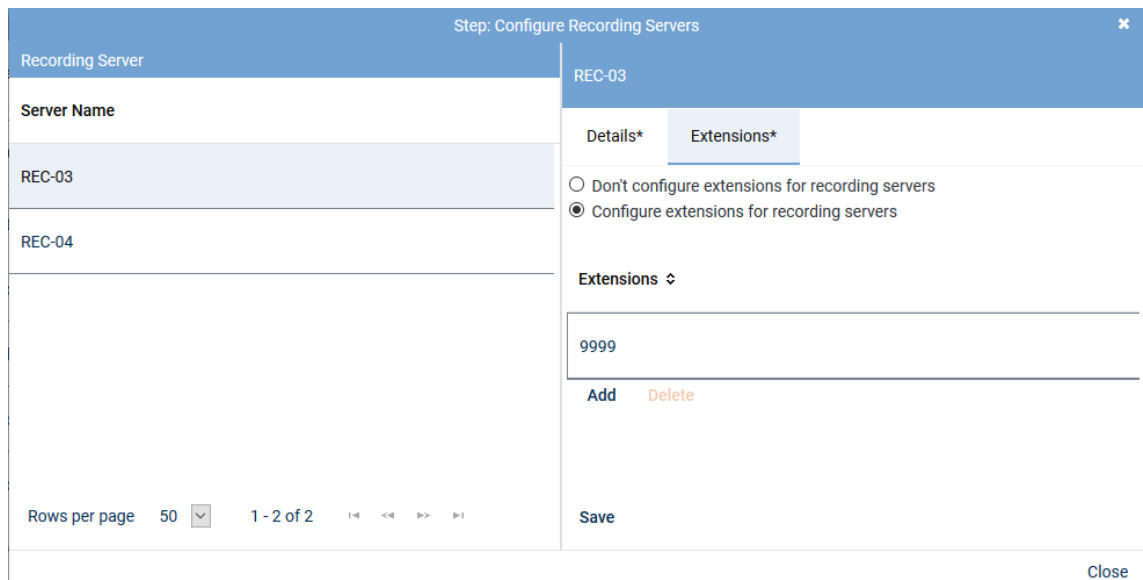


Fig. 63: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the [SIP](#) registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the [SIP](#) end-points again.

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

Configure add-on



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

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



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



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

Configure add-on for Sparkassen FI ISP (optional)

The add-on refers to the usage of 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

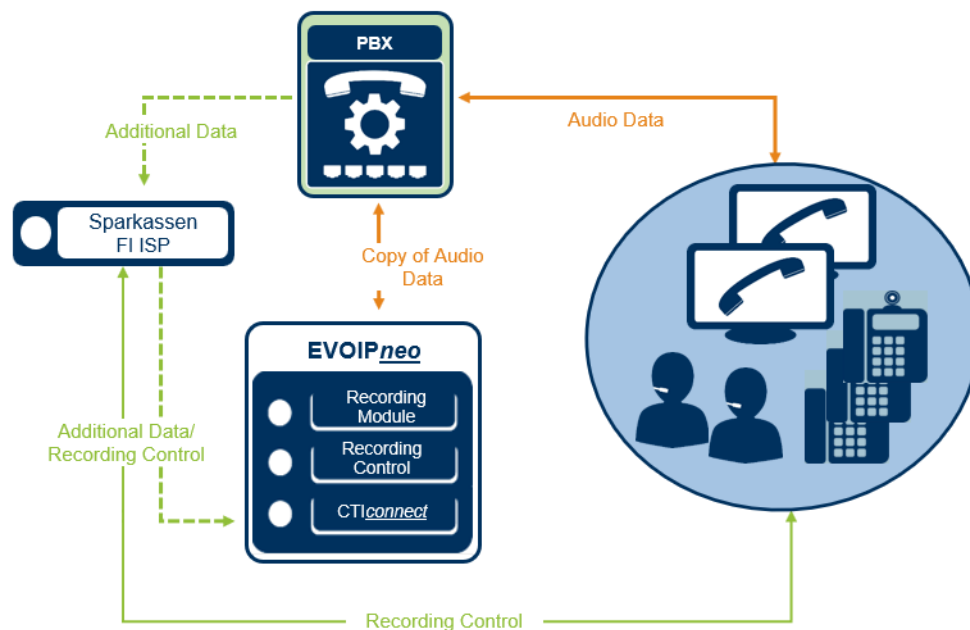



Fig. 64: Overview of Sparkassen FI ISP

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. 65: 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. 18: Configure CTIconnect module



For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

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

Tab. 19: 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.

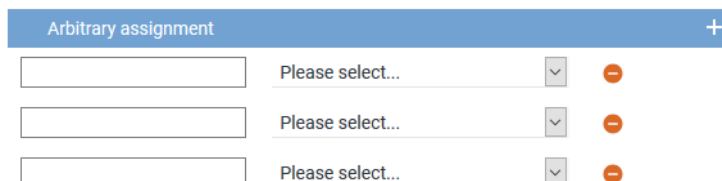



Fig. 66: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)"](#), p. 384.

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. 67: 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. 20: 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:

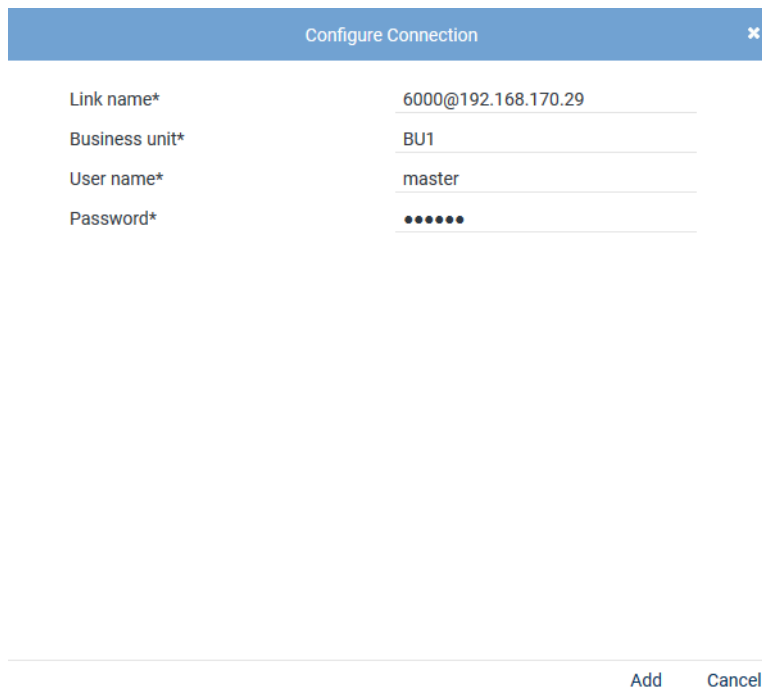


Fig. 68: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 21: 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.

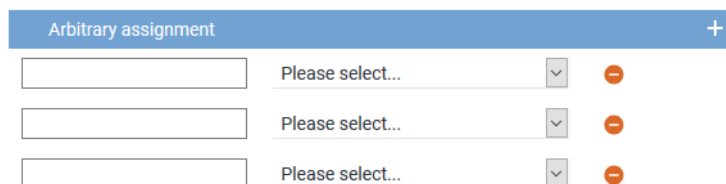




Fig. 69: Arbitrary assignment of the additional data

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 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

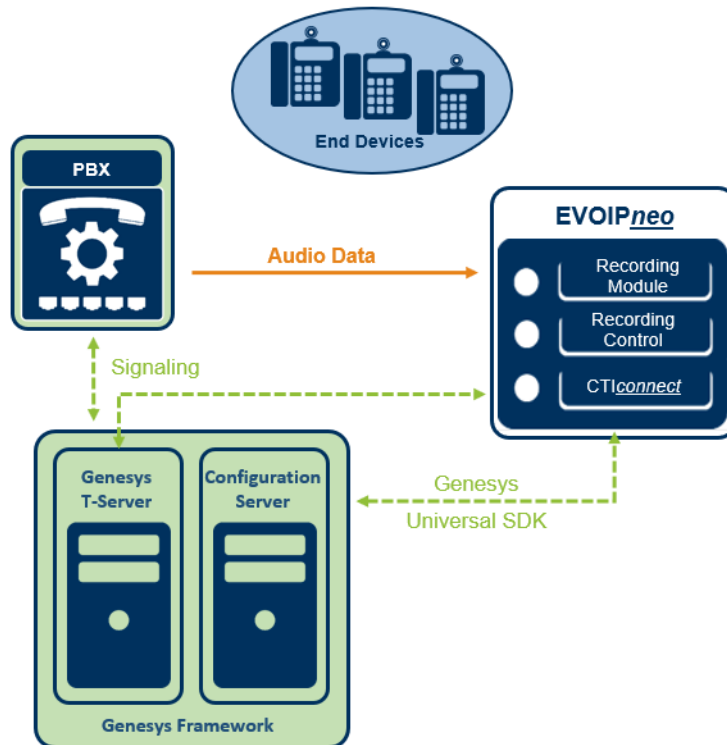


Fig. 70: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

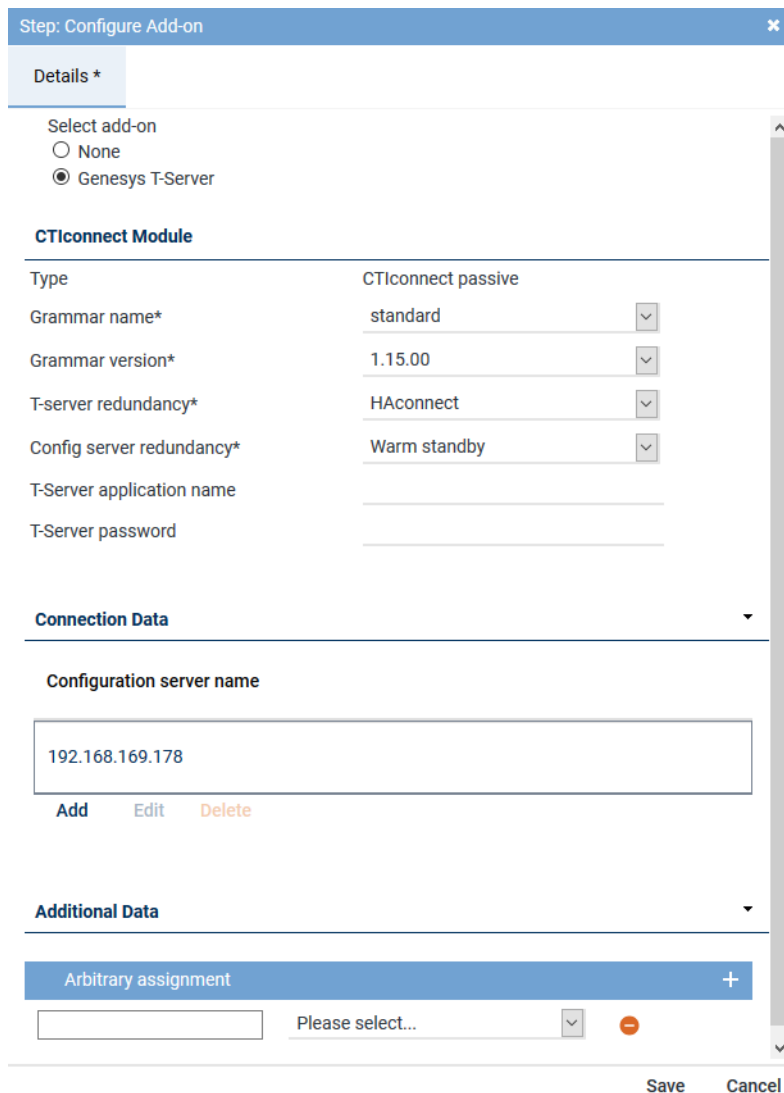
Adjust configuration file for Genesys add-on

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. 71: 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.

Parameter	Value/Description
	<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. 22: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

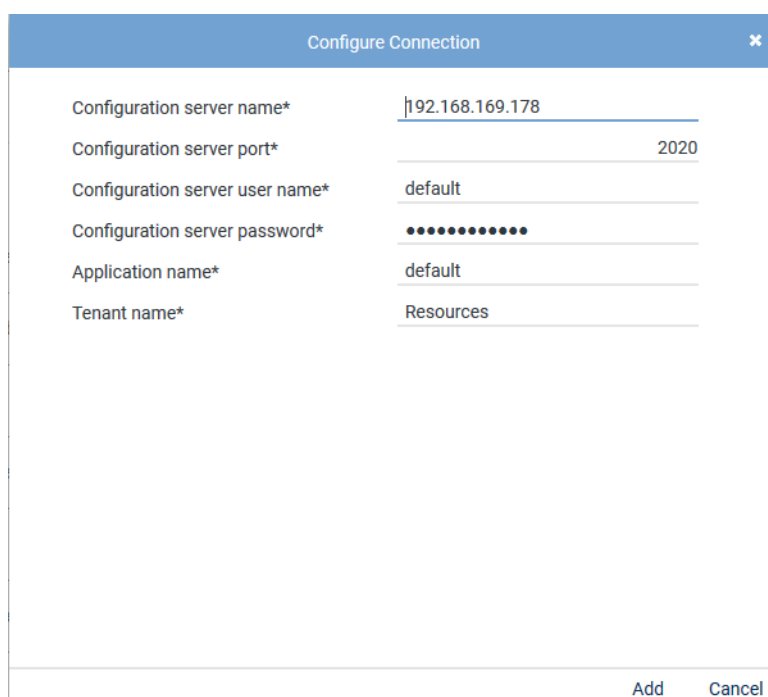


Fig. 72: Configure connection data

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.

Parameter	Value/Description
<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. 23: 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.

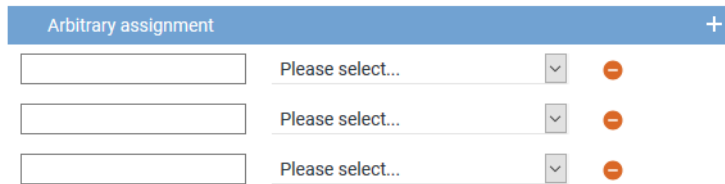



Fig. 73: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

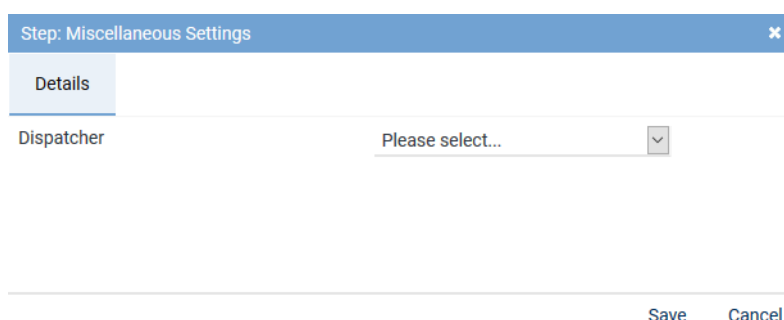


Fig. 74: Configure miscellaneous settings

2. 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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 75: Activate integration

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




+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		

Fig. 76: 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 active	SIP active		

Fig. 77: 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:

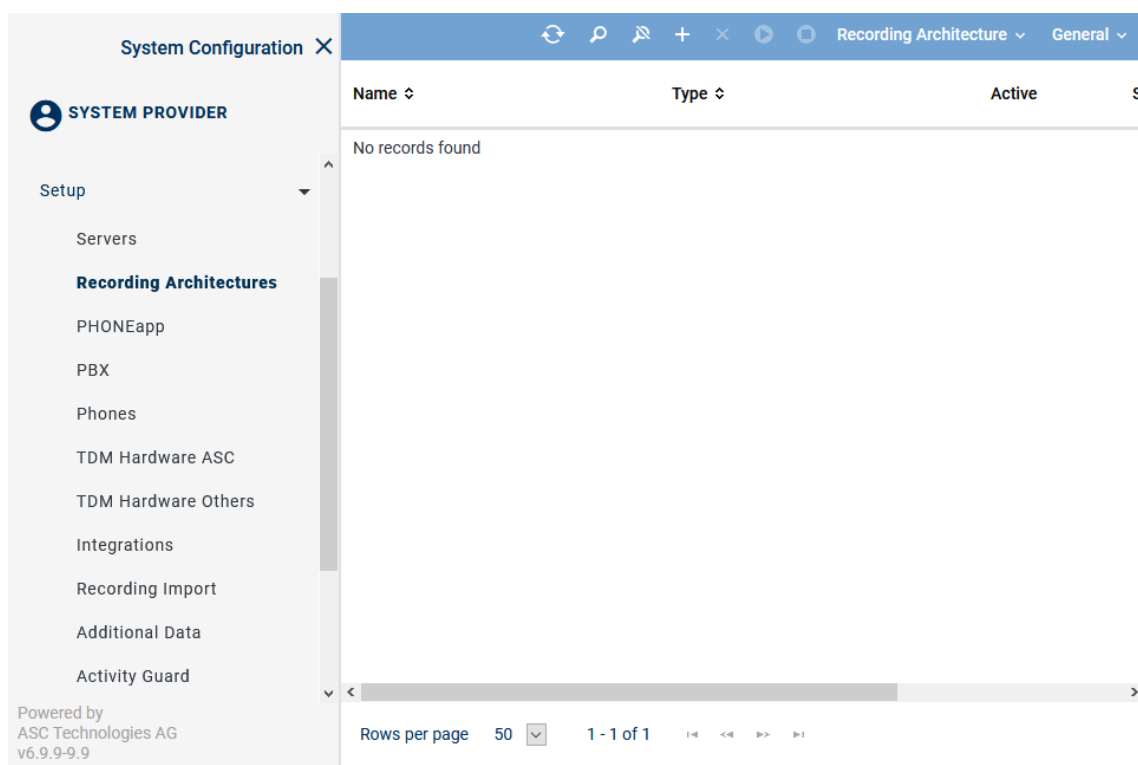


Fig. 78: Recording architectures - main view

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. 79: 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.

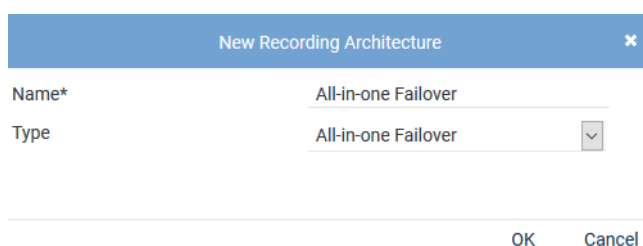



Fig. 80: Create recording architecture - All-in-one Failover

- 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. 81: Recording architecture - tab Details -
All-in-one Failover

As standby components may have been configured for the active recording server, a failover timeout may be configured in this recording architecture. For further information about failover architectures, see [chapter "Standby management for failover architectures", p. 374](#).

<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.

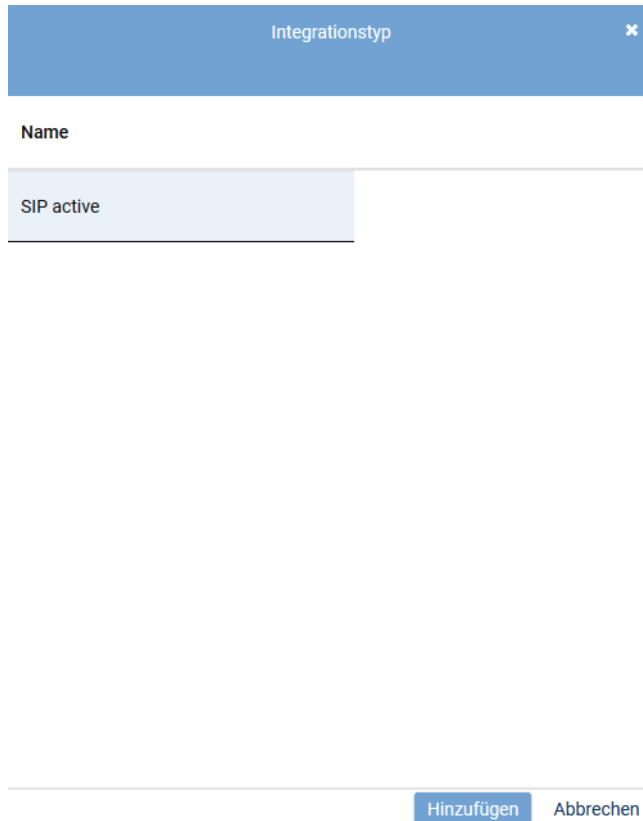


Fig. 82: Select integration type



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

Assign server for All-in-one Failover Recording

- 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. 83: Recording Architecture - tab Server Assignment

- 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:\

Fig. 84: 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.

- 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. 85: 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. 86: Recording architecture - activate recording architecture

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



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



For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See [chapter "Standby management for failover architectures"](#), p. 374.



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:

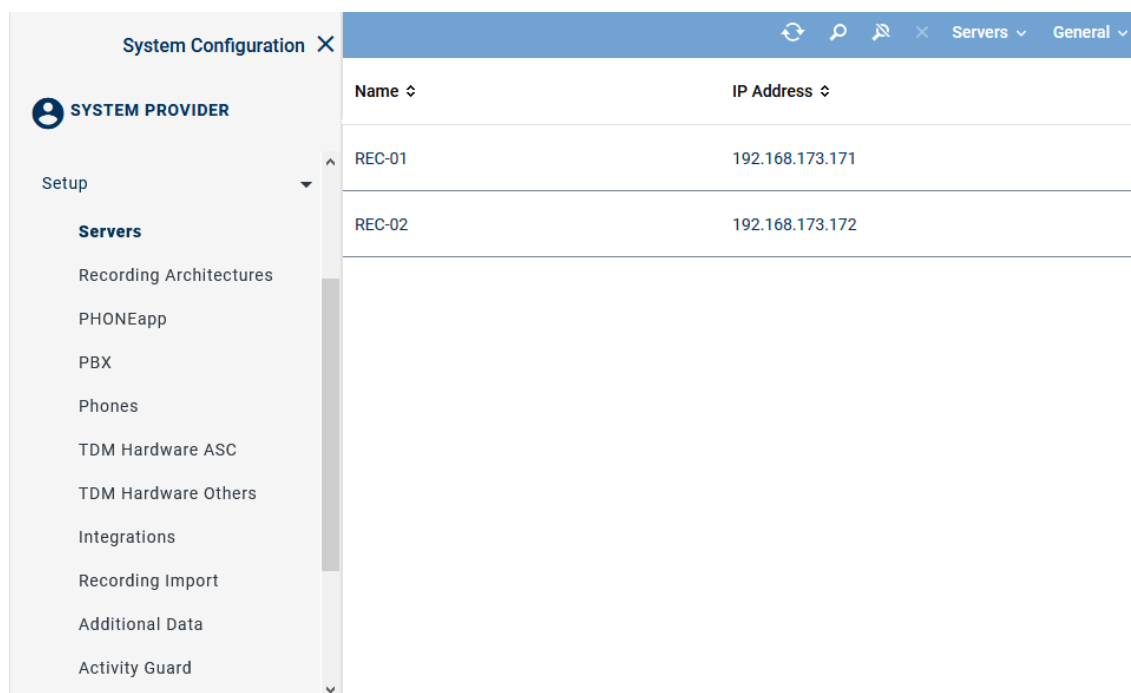


Fig. 87: Servers - main view

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.

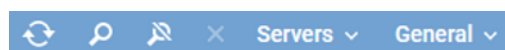








Fig. 88: Toolbar Servers module

	<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 <i>neo</i> 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. 82.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<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.



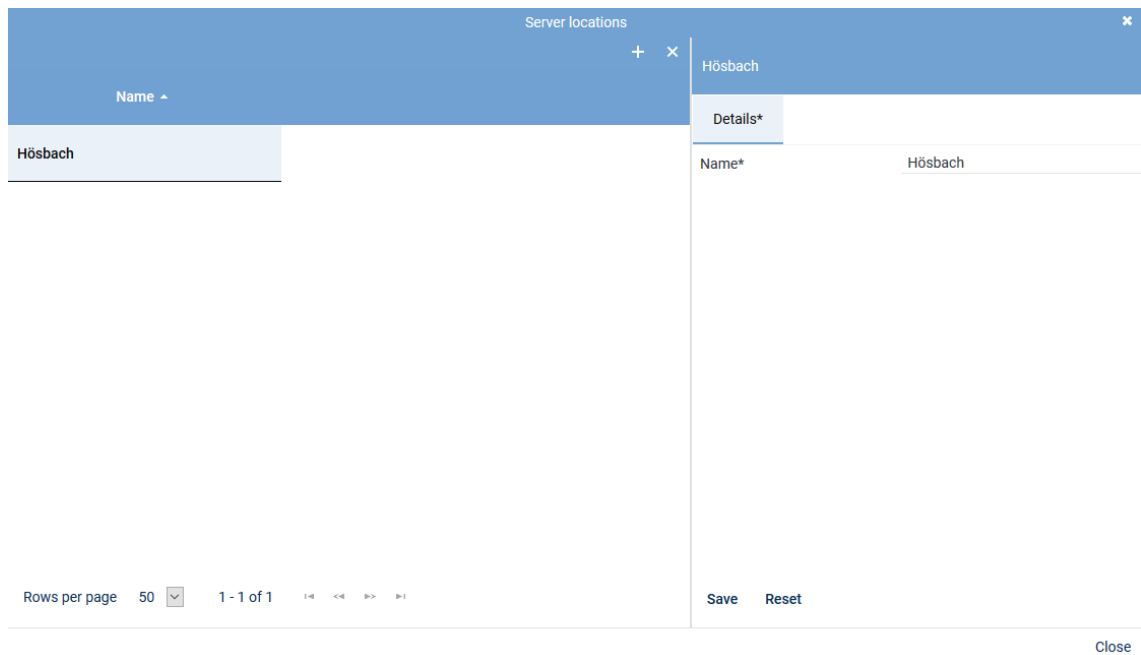
For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

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.



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 plus icon (+) and a minus 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 field labeled "Name*" with the value "Hösbach". At the bottom of the right pane are "Save" and "Reset" buttons. At the bottom of the left pane, there is a pagination bar showing "Rows per page 50", "1 - 1 of 1", and navigation icons. A "Close" button is located at the bottom right of the window.

Fig. 89: Add server locations

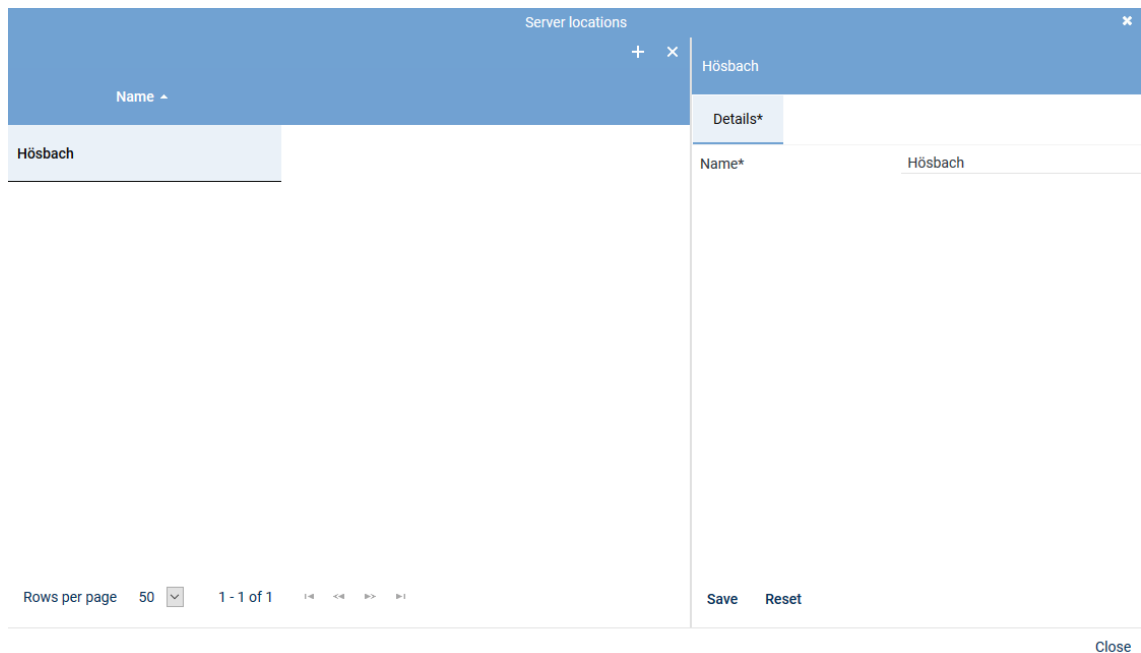
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

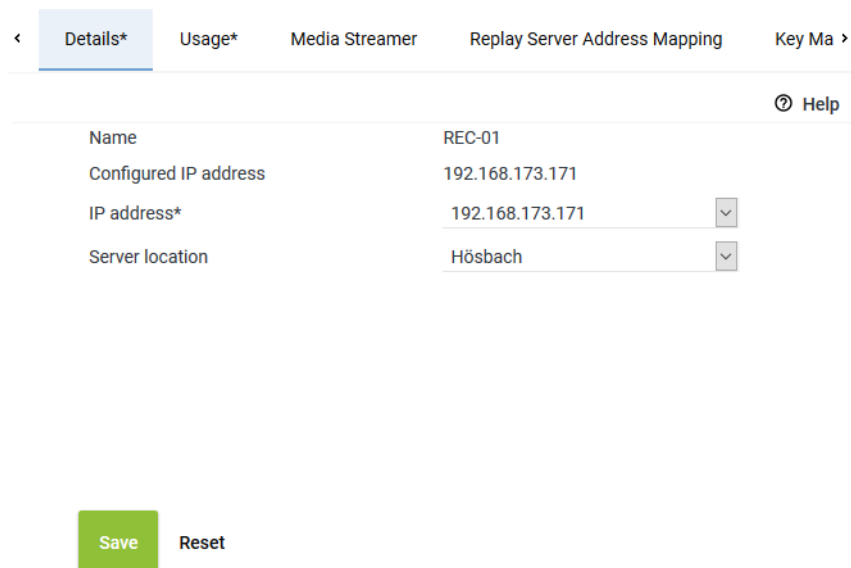
Close

Fig. 90: 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. 91: 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.

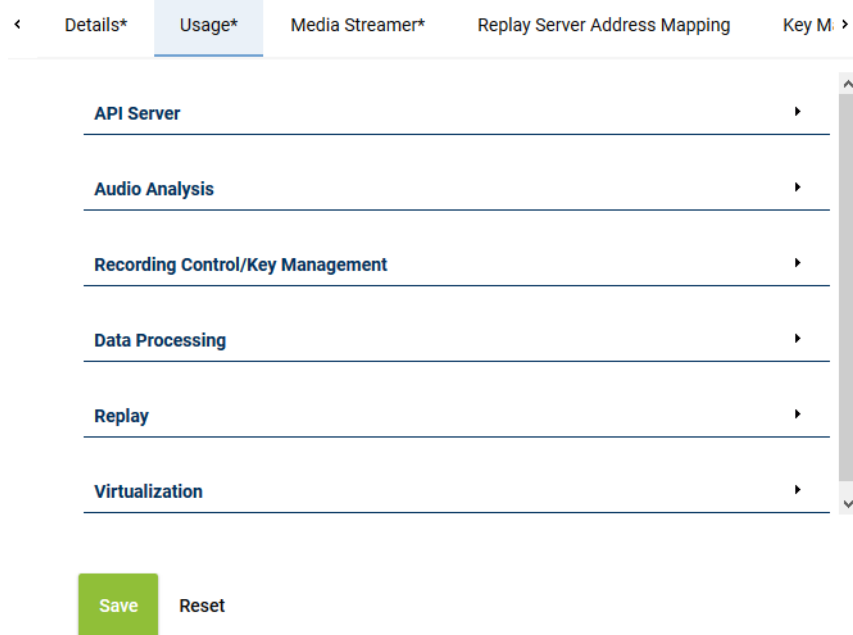


Fig. 92: Servers - tab usage

Group field API Server

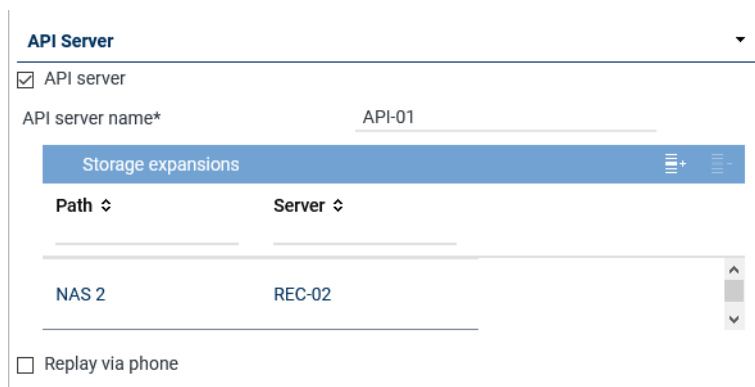




Fig. 93: Group field API Server

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. 96.</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. 87. • 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 <i>neo</i> 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 <i>PBX</i>, see chapter "Tab Media Streamer", p. 94. To be able to do so, at least 1 <i>PBX</i> 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. 94: 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

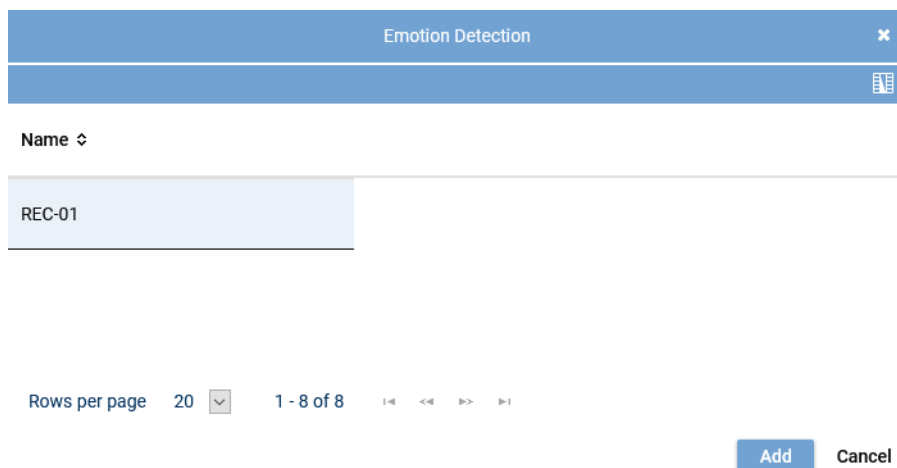
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 95: 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. 24: Configure audio analysis



Emotion Detection

Name ↕

REC-01

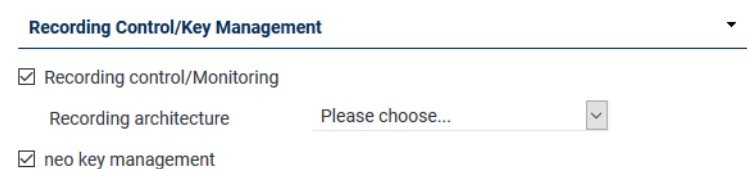
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 96: 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/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 97: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 25: 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. 98: 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. 91. 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. 91. 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 <i>neo</i> to <i>neo</i>, 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. 26: Data storage

Add target server to a list


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



Fig. 99: Select server



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

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

Group field Replay

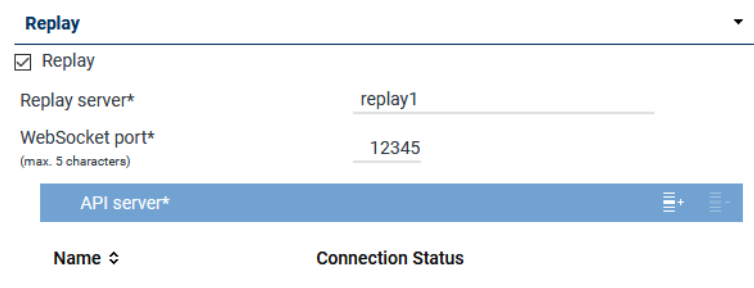




Fig. 100: Group field Replay

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  (Add), you can add the API server, see chapter "Add API server to a list", p. 92. • By clicking on the icon  (Remove), you can remove selected API servers from the list.

Tab. 27: 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. 101: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 85](#).

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. 102: 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. 28: 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*	123456	<input type="text"/>
<small>(max. 18 characters)</small>		
Media streamer IP address*	192.168.169.192	<input type="text"/>
Minimum port	24000	<input type="text"/>
Maximum port	24099	<input type="text"/>
Transport protocol	UDP	<input type="text"/>
SIP signaling port	5062	<input type="text"/>
User name		<input type="text"/>
Password		<input type="text"/>
PBX IP address		<input type="text"/>
PBX port	5060	<input type="text"/>
Registration required	<input checked="" type="checkbox"/>	
SIP registration expiration	3600	Second(s)

Save

Reset

Fig. 103: 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. 100.</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 <i>8000</i>.</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> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</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: <i>5062</i></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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<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 <i>5060</i>.</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. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.



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

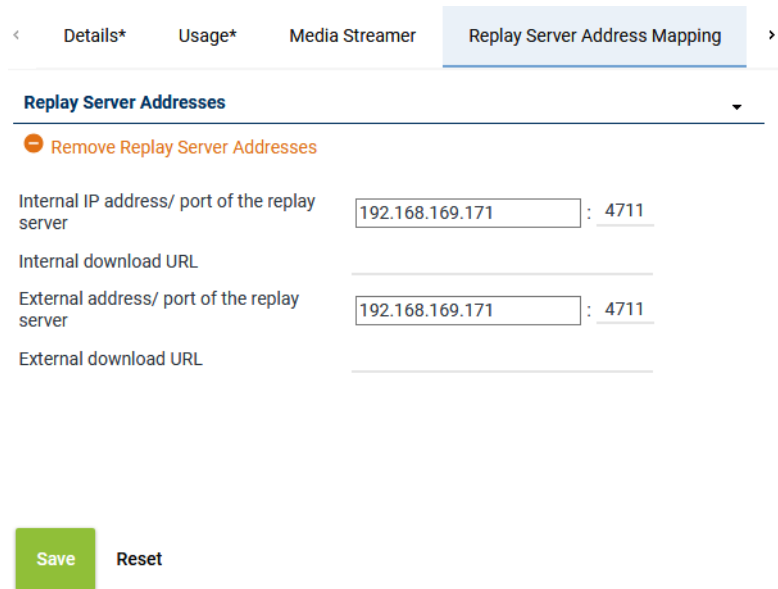


Fig. 104: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

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



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

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



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



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

Tab Key Management

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

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

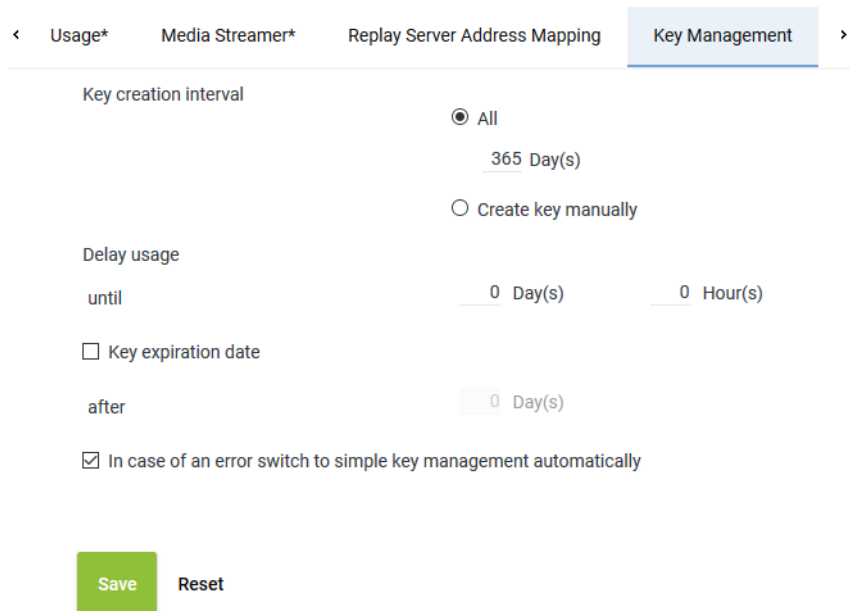


Fig. 105: Servers module - tab Key Management

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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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*

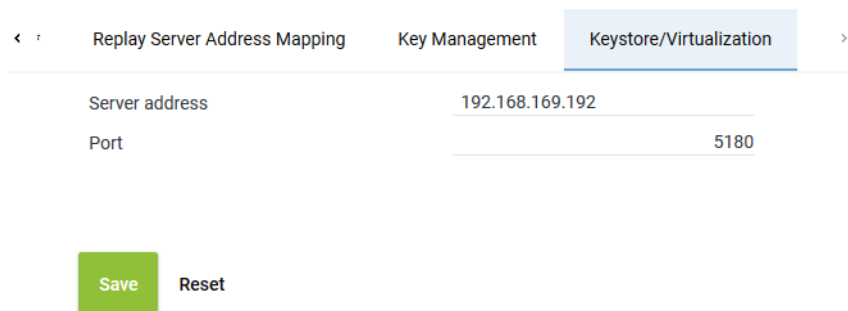
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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. It has three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization' (which is selected). Below the tabs 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' (grey).

Fig. 106: 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:

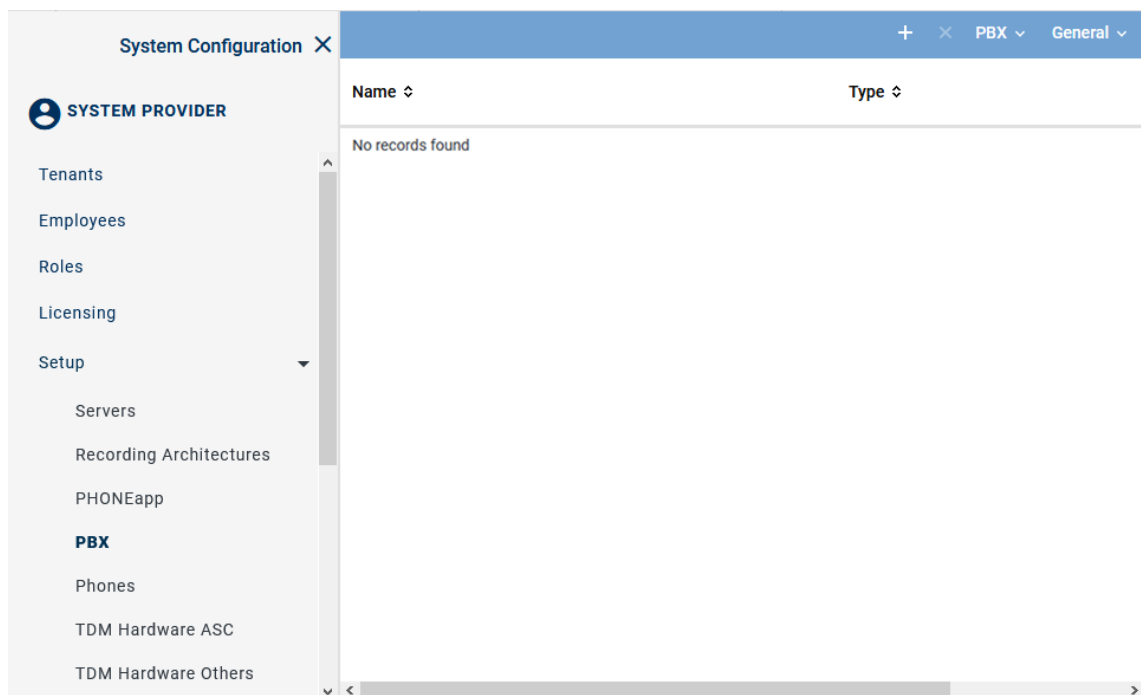


Fig. 107: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

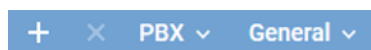




Fig. 108: Toolbar PBX module


	<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. 109: 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. 29: Create PBX

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

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

Tab. 30: PBX parameters with complete phone number

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

7.1.2.2.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

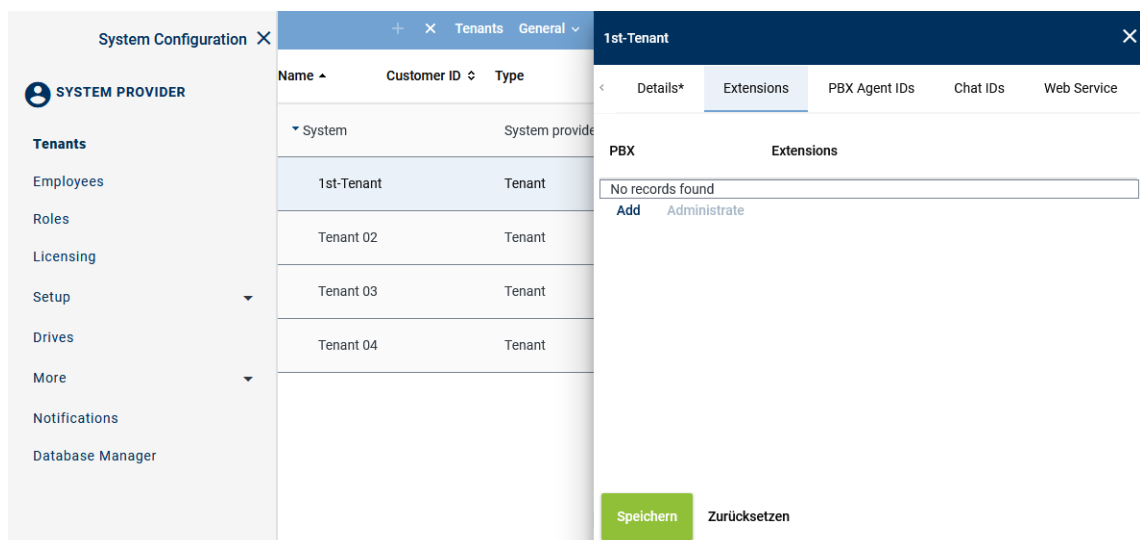


Fig. 110: Tenants - main view - tab Extensions

Add extensions

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

⇒ The following window appears:

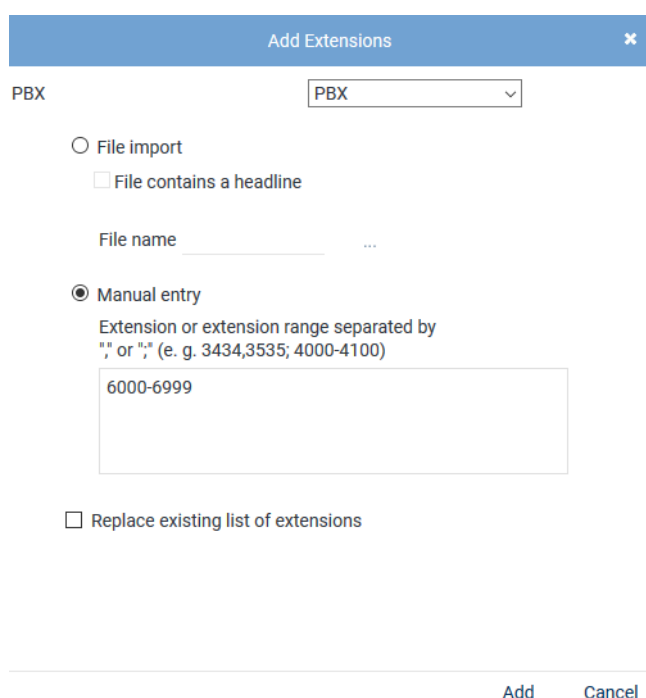




Fig. 111: Assign extensions to tenants

- 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"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <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.

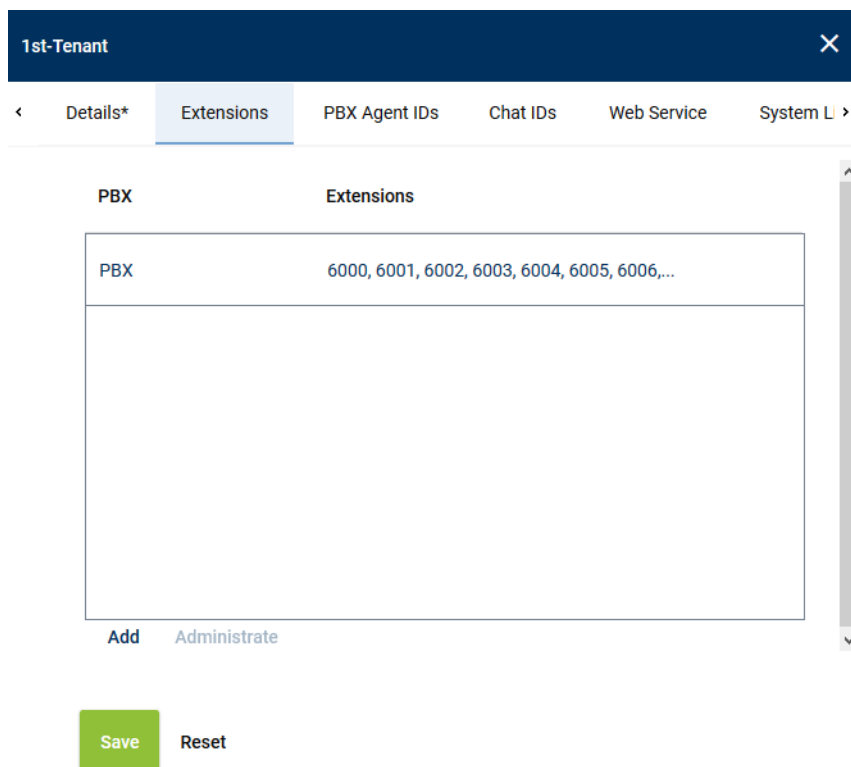
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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.



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. 112: 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. 113: 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.

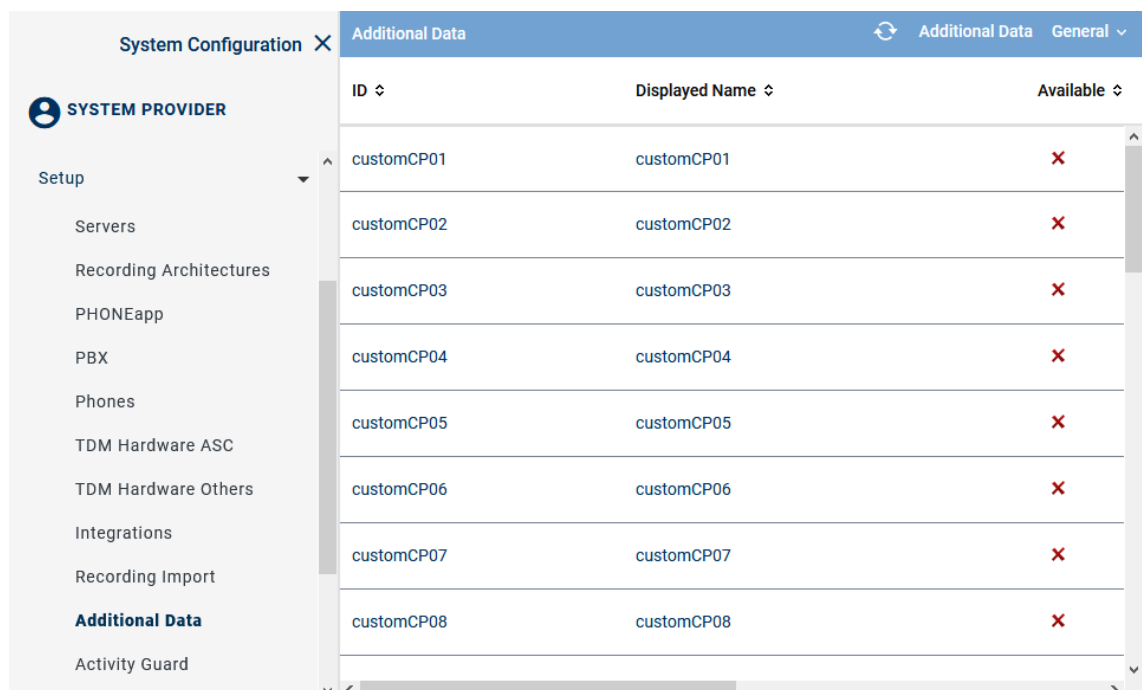


Fig. 114: Additional Data module main view

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. 115: 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. 116: 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:

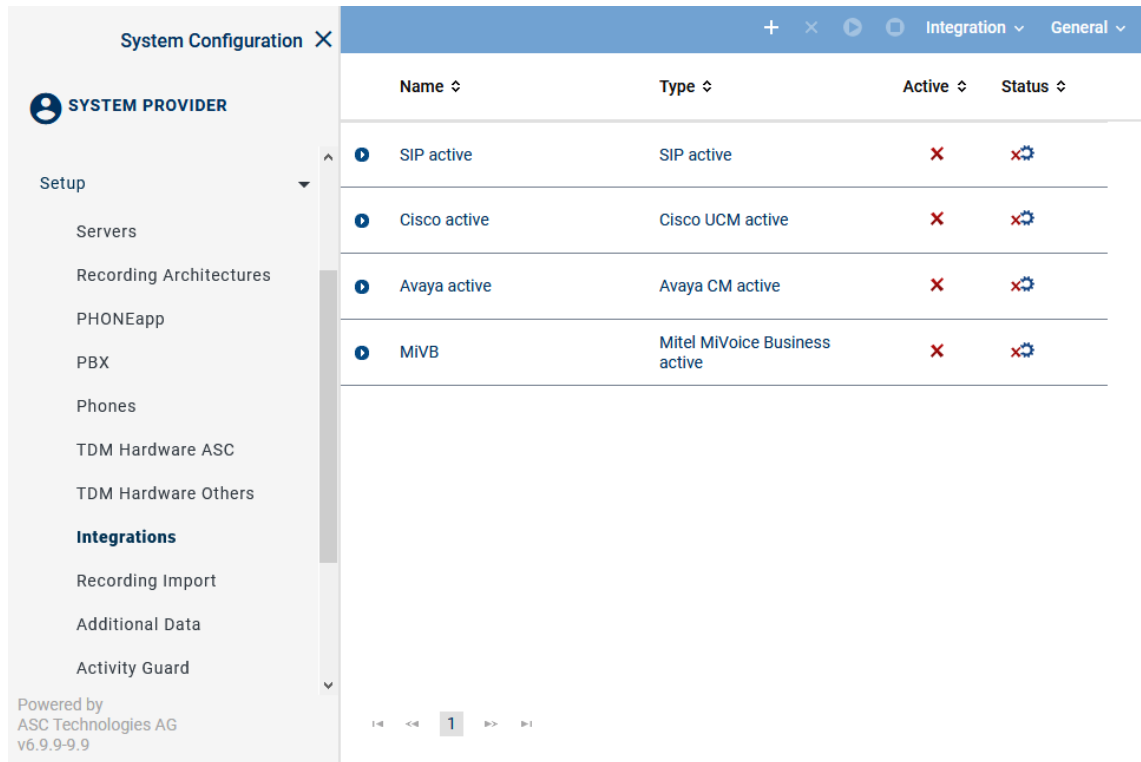




Fig. 117: Integrations - main view

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. 118: 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.

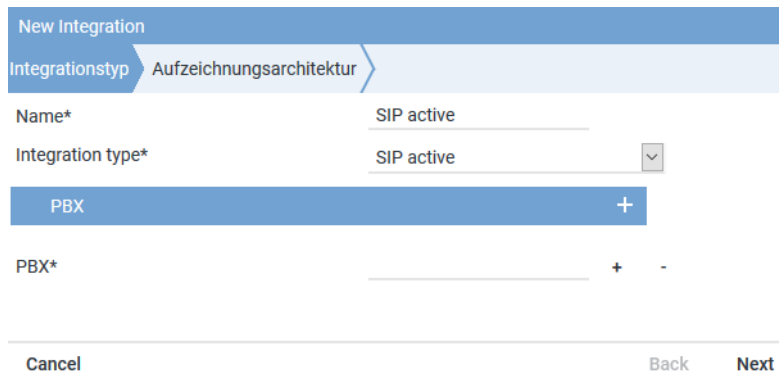



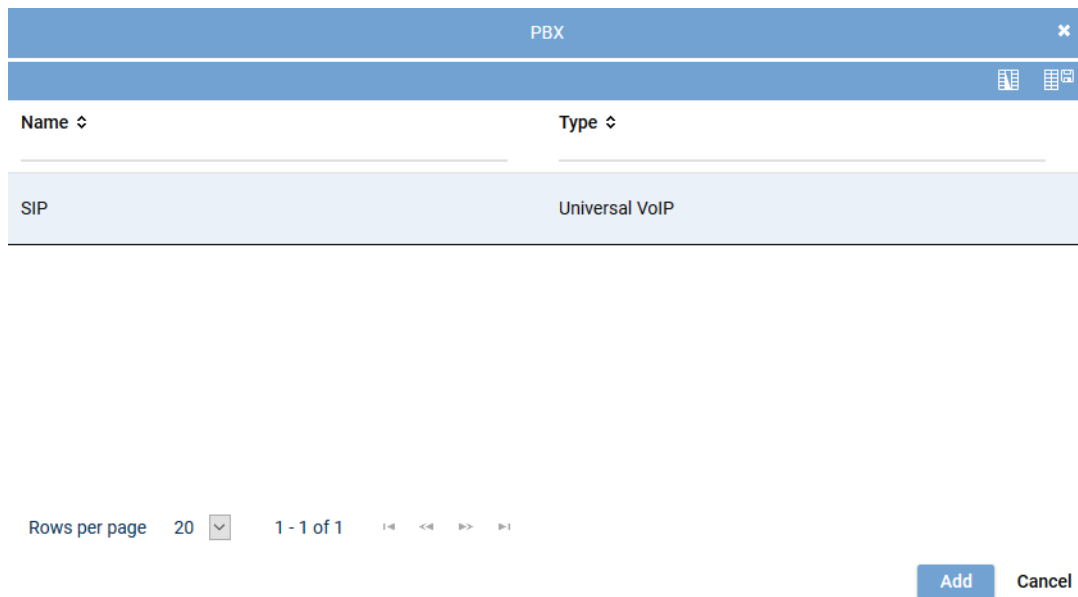
Fig. 119: Create integration type

- 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 31: Create integration type

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



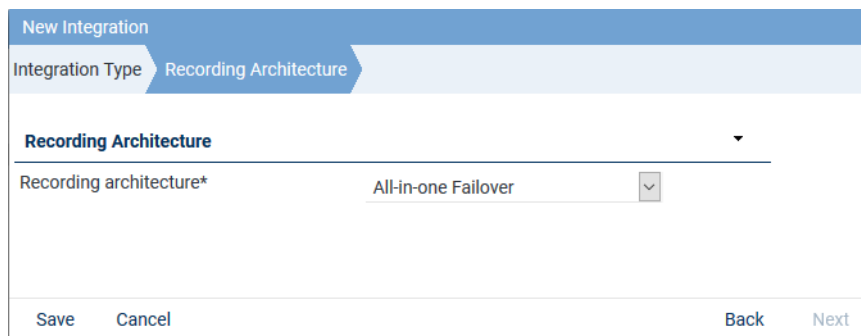
The interface shows a table titled 'PBX' with two columns: 'Name' and 'Type'. There is one row with 'SIP' under 'Name' and 'Universal VoIP' under 'Type'. Below the table, there is a pagination bar showing 'Rows per page' set to 20, and '1 - 1 of 1'. At the bottom right, there are 'Add' and 'Cancel' buttons.

Fig. 120: 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.



The interface shows a 'New Integration' section with two tabs: 'Integration Type' and 'Recording Architecture'. The 'Recording Architecture' tab is active. Below the tabs, there is a dropdown menu labeled 'Recording architecture*' with 'All-in-one Failover' selected. At the bottom, there are 'Save', 'Cancel', 'Back', and 'Next' buttons.

Fig. 121: 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 active		SIP active	X	⚙️
Step	Configuration			
Configure recording architecture	✓ 			
Global recording settings	✗ 			
Configure recording servers	✗ 			
Configure add-on	✓ 			
Configure miscellaneous settings	✓ 			

Fig. 122: 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. 123: 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.

Global recording settings for All-in-one Failover

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

Step: Global Recording Settings
✕

Details *

SIP Header Tagging*

Transport protocol
UDP ▼

Port SIP signaling*
5060

Activate SIP authentication
☒

User name for the SIP registration
123456

Password for the SIP registration
••••••

Activate PBX connection
☒

SIP registration expiration*
3600

PBX IP address*
192.168.170.178

PBX port*
5060

Activate SMS recording
☒

Save Cancel

Fig. 124: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
<i>Port SIP signaling</i>	<p>Enter the port for the SIP signaling, where the recording server is expecting the signaling.</p> <p>Default value for UDP and TCP is 5060.</p> <p>Default value with TLS encryption is 5061.</p> <p>NOTICE! If you would like to use several integrations, you have to configure a separate SIP port for each integration.</p> <p>NOTICE! If you would like to use a media streamer for replay, configure another SIP port for it, too. In case of communication issues with the media streamer, this could otherwise affect the recording.</p>
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password of the SIP registration</i>	Enter the password, if an authentication for the SIP registration is used.
<i>Activate PBX connection</i>	Activate this check box if the recording server is supposed to register itself on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration runs out, e. g. 3600.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port on which the SIP signaling is sent to the PBX . The default value is 5060.

Parameter	Value/Description
<i>Activate SMS recording</i>	Activate the check box if you would like to use SMS recording.

Tab. 32: Global recording settings

Tab SIP Header Tagging

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

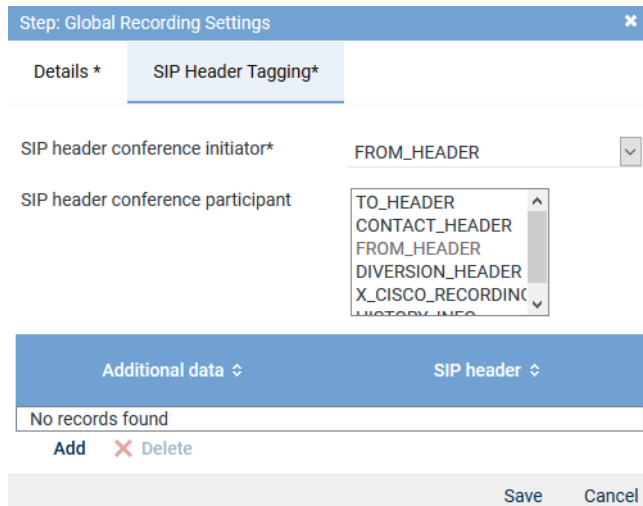


Fig. 125: Tab SIP Header Tagging Configure sources

2. Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

Tab. 33: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down. To deselect an entry, click on it again without releasing the [Ctrl] key.

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

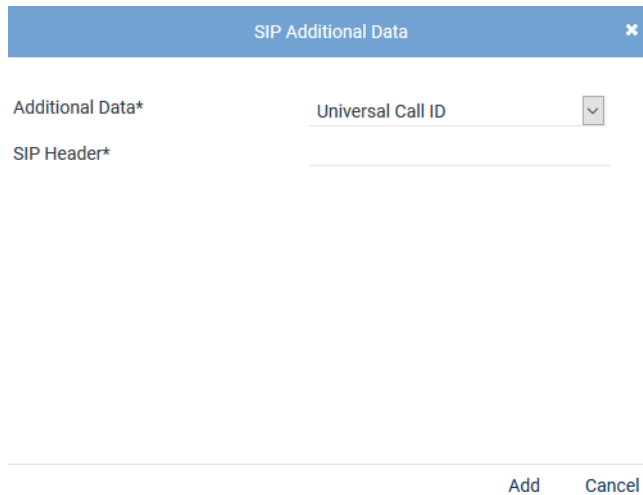


Fig. 126: SIP Additional Data



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

4. Enter the following parameters:

Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.


Tab. 34: Configure SIP conversation parameters

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

Configure recording server for All-in-one Failover

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

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

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

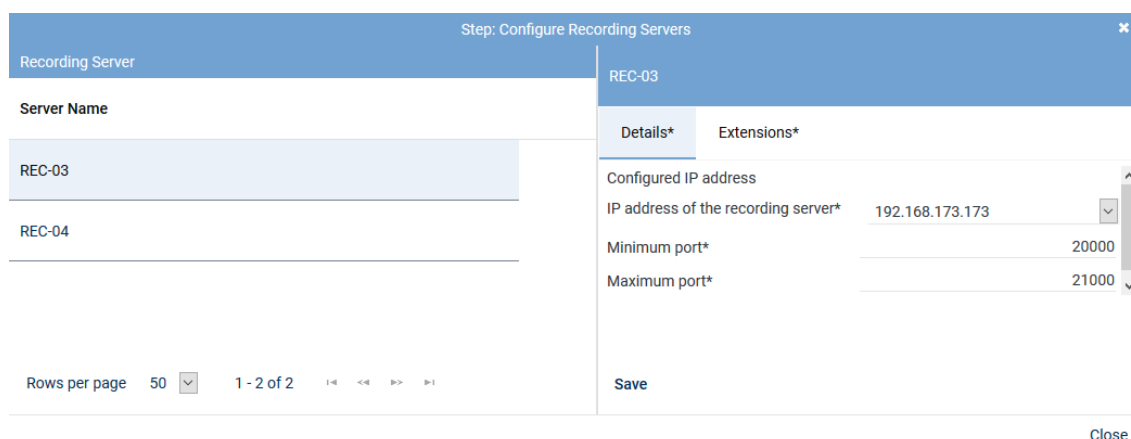


Fig. 127: Configuration step - Configure recording servers

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

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

Tab. 35: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

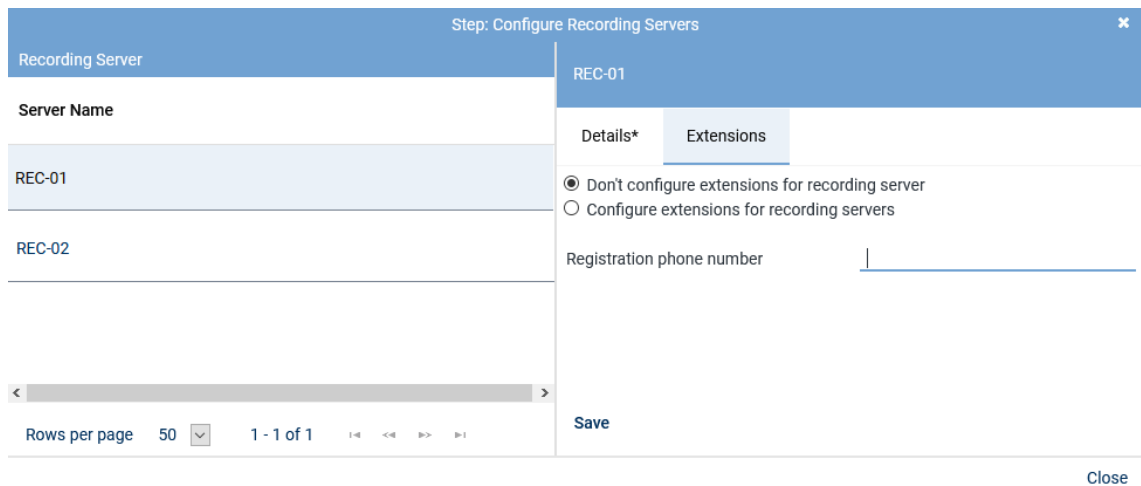


Fig. 128: Recording server - Configure extension for SIP trunk

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a [SIP](#) trunk phone number instead.



If you do not define a phone number for the [SIP](#) trunk of the recording server, all incoming [SIP](#) connections are accepted without being examined.

Registration phone number Enter a registration phone number for the [SIP](#) trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the [SIP](#) trunk, see [chapter "Global recording settings for All-in-one Failover"](#), p. 111.

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

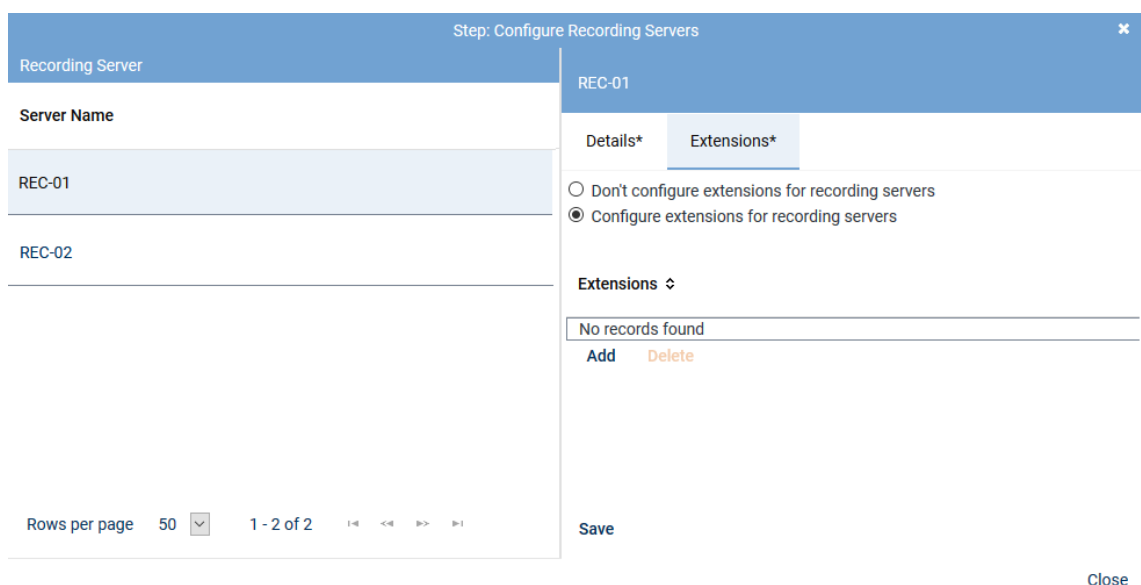


Fig. 129: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

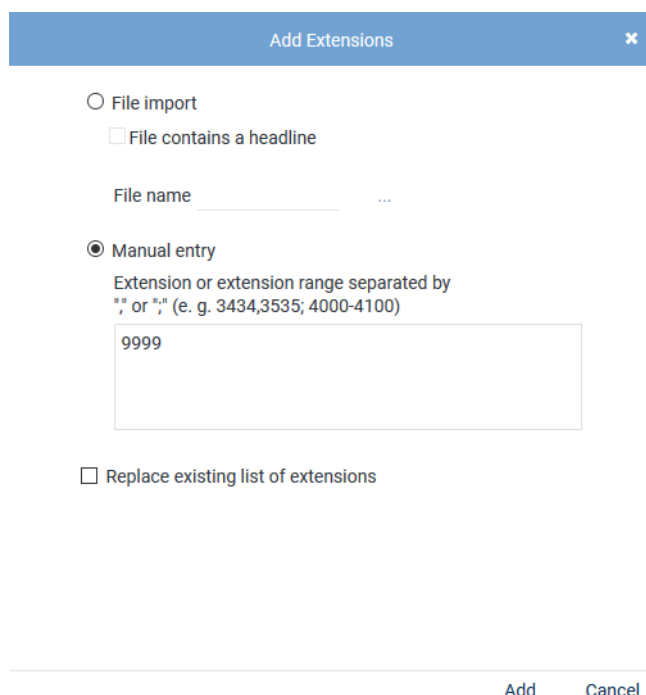


Fig. 130: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
5. If errors have been 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*.
6. The configured extensions now appear in the detail view.

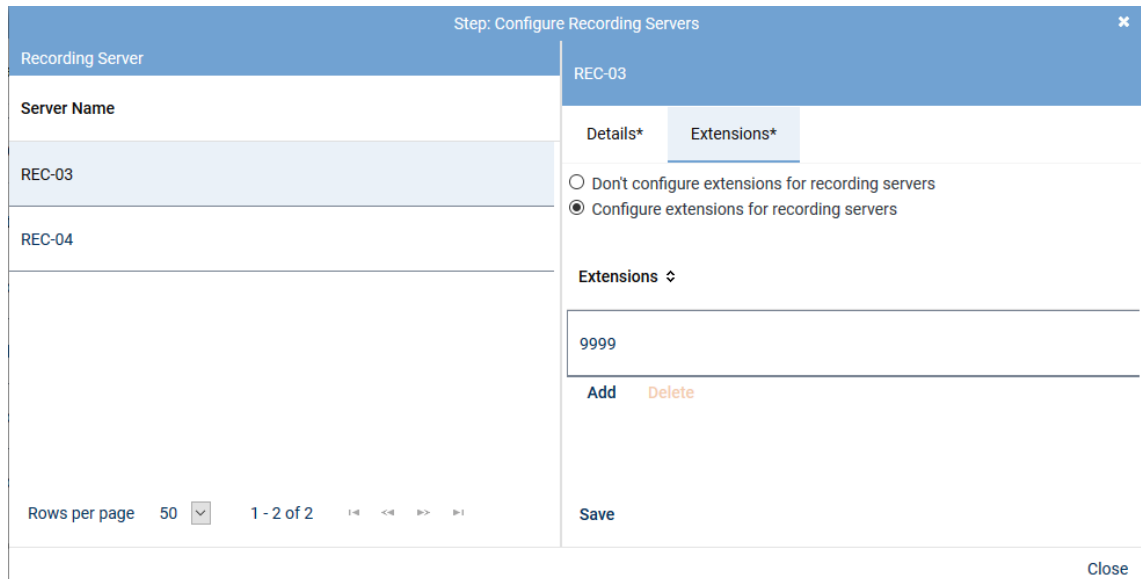


Fig. 131: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the **SIP** registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the **SIP** end-points again.

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

Configure add-on



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

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



The additional data delivered by an add-on supplements the additional data which is delivered by the 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 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

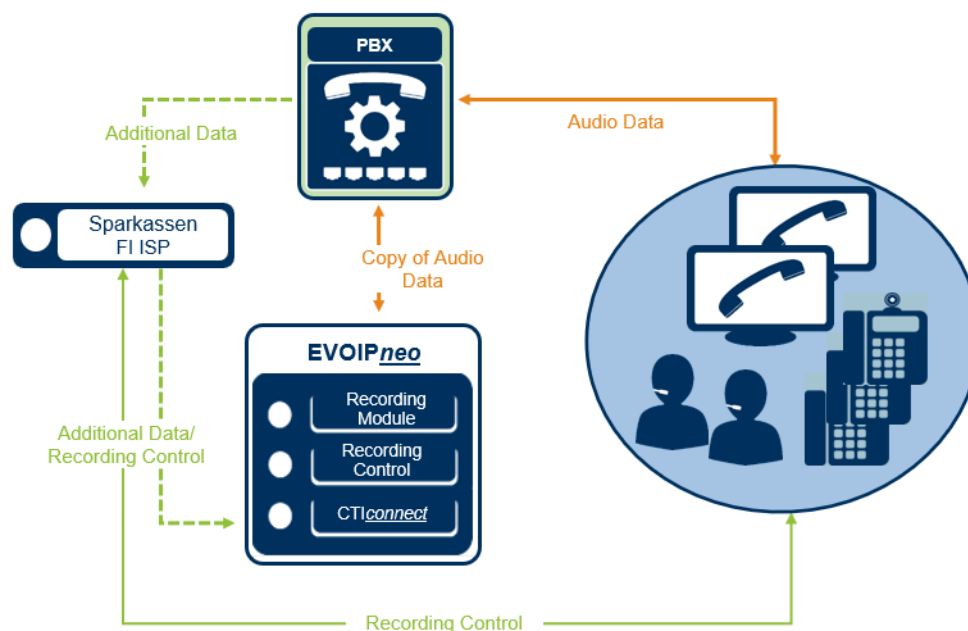



Fig. 132: Overview of Sparkassen FI ISP

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. 133: 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. 36: Configure CTIconnect module



For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

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

Tab. 37: 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.

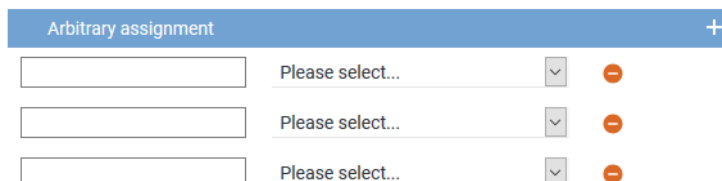



Fig. 134: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)", p. 384](#).

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. 135: 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. 38: 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:

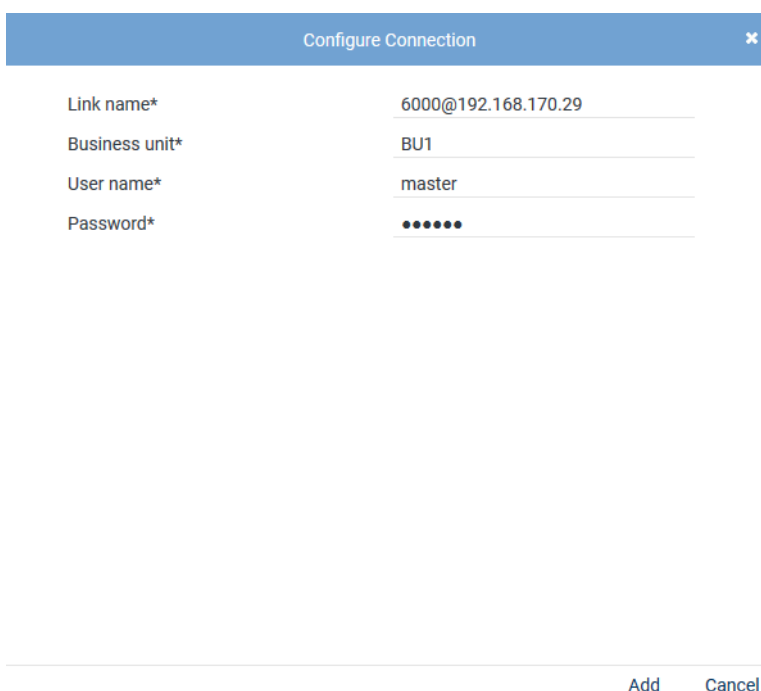


Fig. 136: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 39: 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.

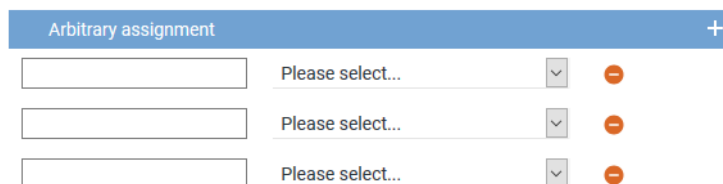




Fig. 137: Arbitrary assignment of the additional data

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 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

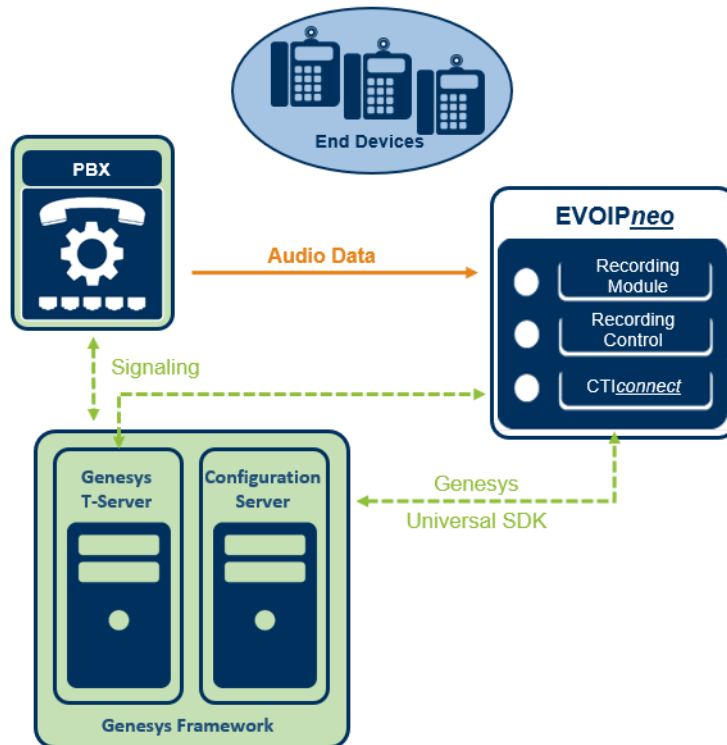


Fig. 138: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

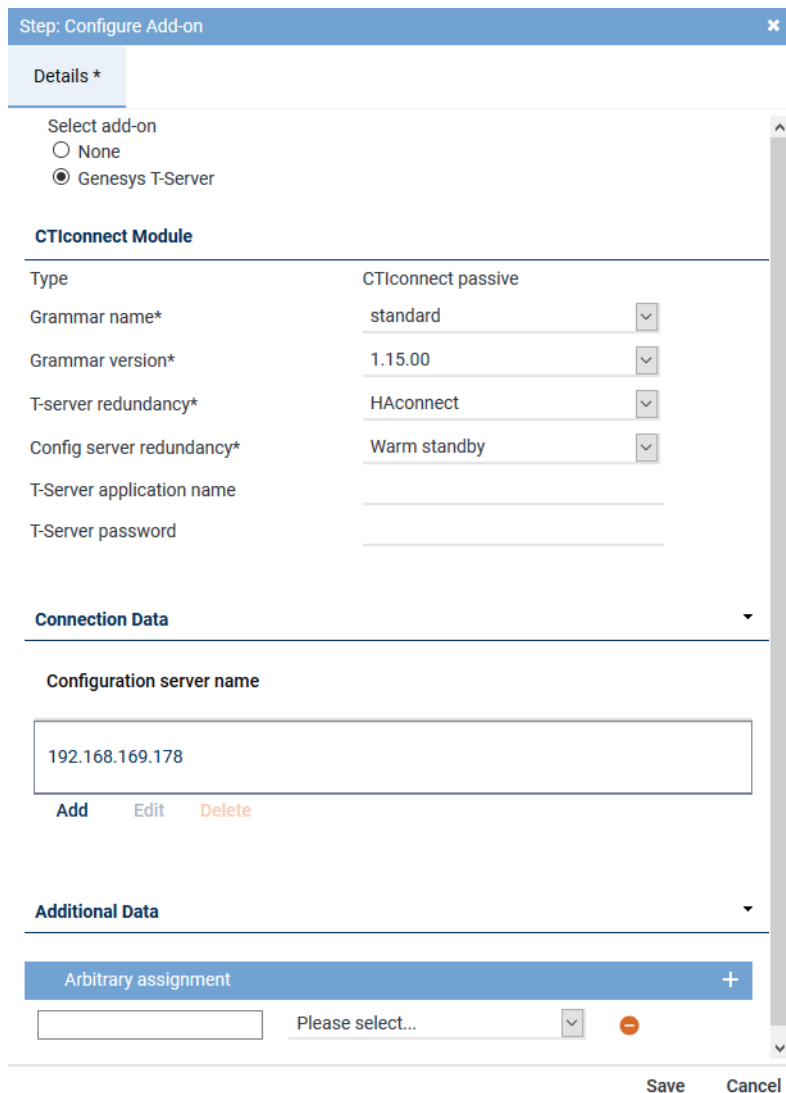


Fig. 139: Configure add-on for Genesys T-Server

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.

Parameter	Value/Description
	<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. 40: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

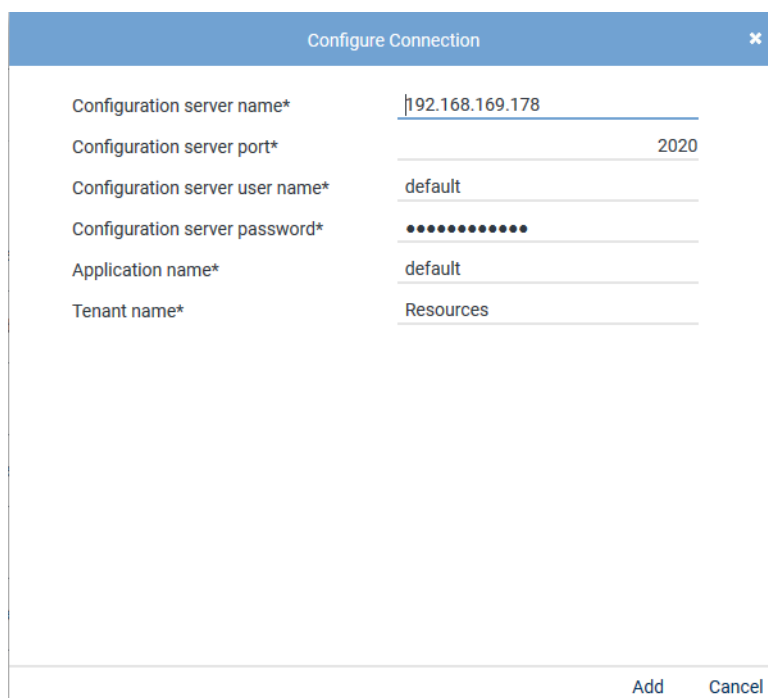


Fig. 140: Configure connection data

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.

Parameter	Value/Description
<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. 41: 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.

Arbitrary assignment			+
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖

Fig. 141: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select... ▼

Save

Cancel

Fig. 142: Configure miscellaneous settings

2. 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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 143: Activate integration

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




+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		

Fig. 144: 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 active	SIP active		

Fig. 145: 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:

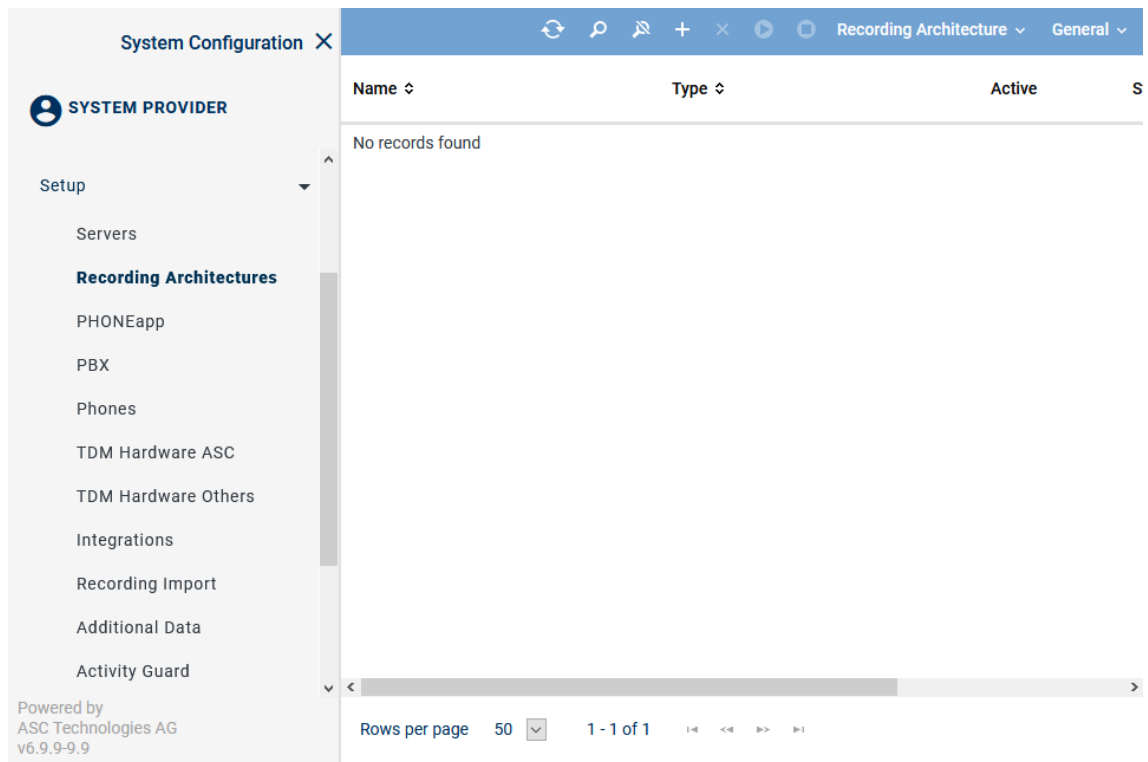




Fig. 146: Recording architectures - main view

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. 147: 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.

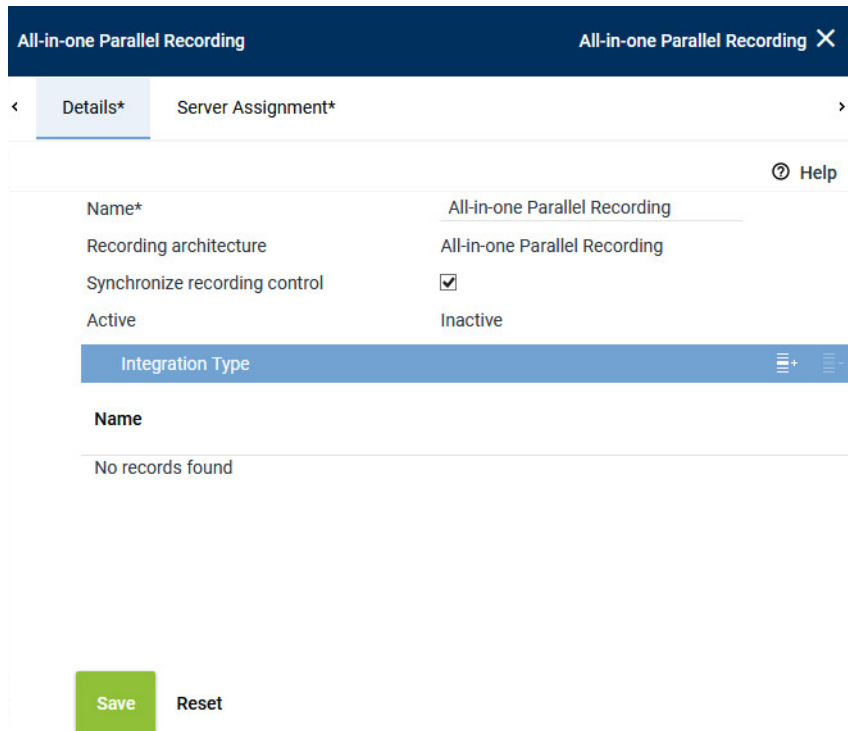
⇒ The window *New Recording Architecture* appears.



Fig. 148: Create recording architecture - All-in-one 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 *All-in-one Parallel Recording*.
NOTICE! The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.
⇒ Your entries now appear in the detail view.



The screenshot shows a configuration window titled "All-in-one Parallel Recording" with a close button (X). Below the title bar is a tabbed interface with two tabs: "Details*" (selected) and "Server Assignment*". The "Details*" tab contains a form with the following fields:

- Name***: All-in-one Parallel Recording
- Recording architecture**: All-in-one Parallel Recording
- Synchronize recording control**: ☒
- Active**: Inactive

Below the form is a section titled "Integration Type" with a blue header bar and a list of integration types. The list is currently empty, showing "No records found". At the bottom of the window are two buttons: "Save" (green) and "Reset" (grey).


Fig. 149: Recording architecture - tab Details - All-in-one Parallel Recording

5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see [chapter "Synchronization of recording control", p. 366](#).

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 [chapter "Duplicates in parallel recording architectures", p. 370](#).

Add integration type

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

Integrationstyp

Name

SIP active

Hinzufügen

Abbrechen

Fig. 150: Select integration type



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

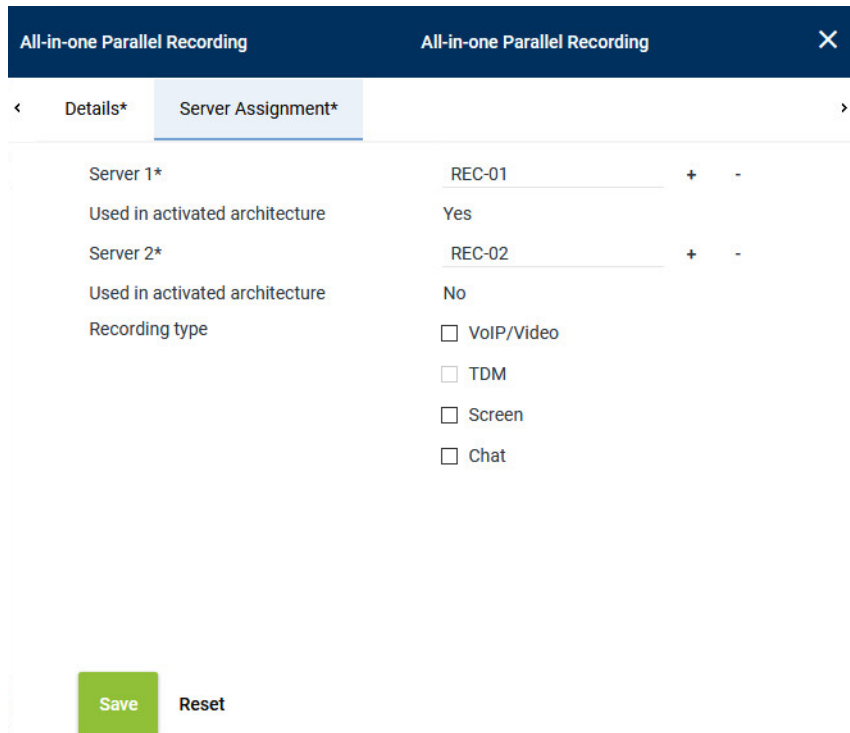


Any number of integration types can be assigned to a recording architecture.

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

Assign server for All-in-one Parallel Recording

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



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. 151: 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. 152: 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. 153: 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. 154: Activate recording architecture

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



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



Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see [chapter "Configure duplicate detection", p. 370](#).



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:

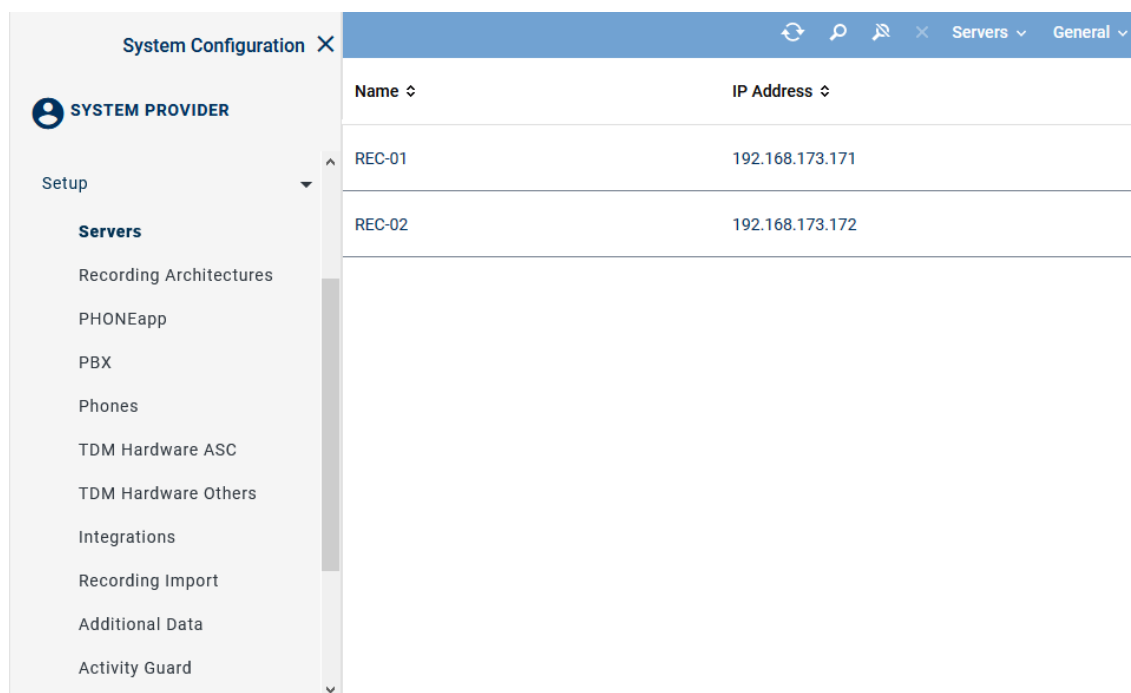


Fig. 155: Servers - main view

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.

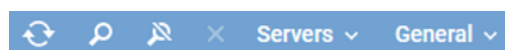








Fig. 156: Toolbar Servers module

	<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 <i>neo</i> 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. 140.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<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.



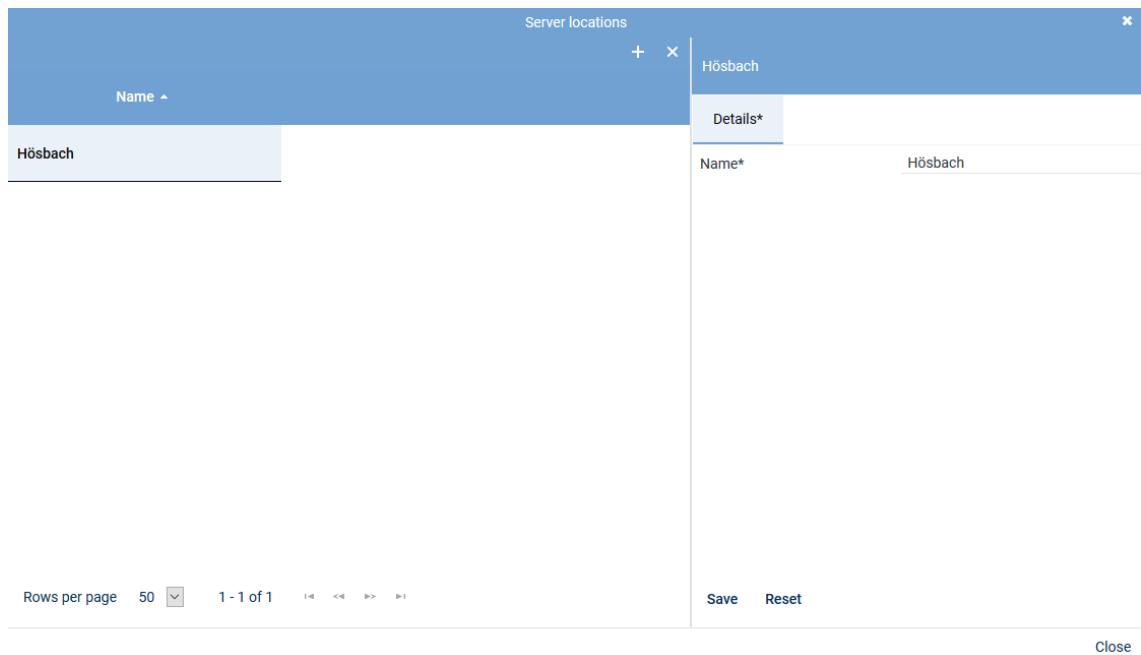
For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

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.



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 plus icon (+) and a minus icon (-). The main area is divided into two panes. The left pane contains a table with one row: "Hösbach". The right pane is titled "Hösbach" and contains a "Details*" tab. Below the tab, there is a form with a label "Name*" and a text input field containing "Hösbach". At the bottom of the right pane, there are "Save" and "Reset" buttons. At the bottom of the left pane, there is a pagination bar showing "Rows per page 50", "1 - 1 of 1", and navigation icons. A "Close" button is located at the bottom right of the window.

Fig. 157: Add server locations

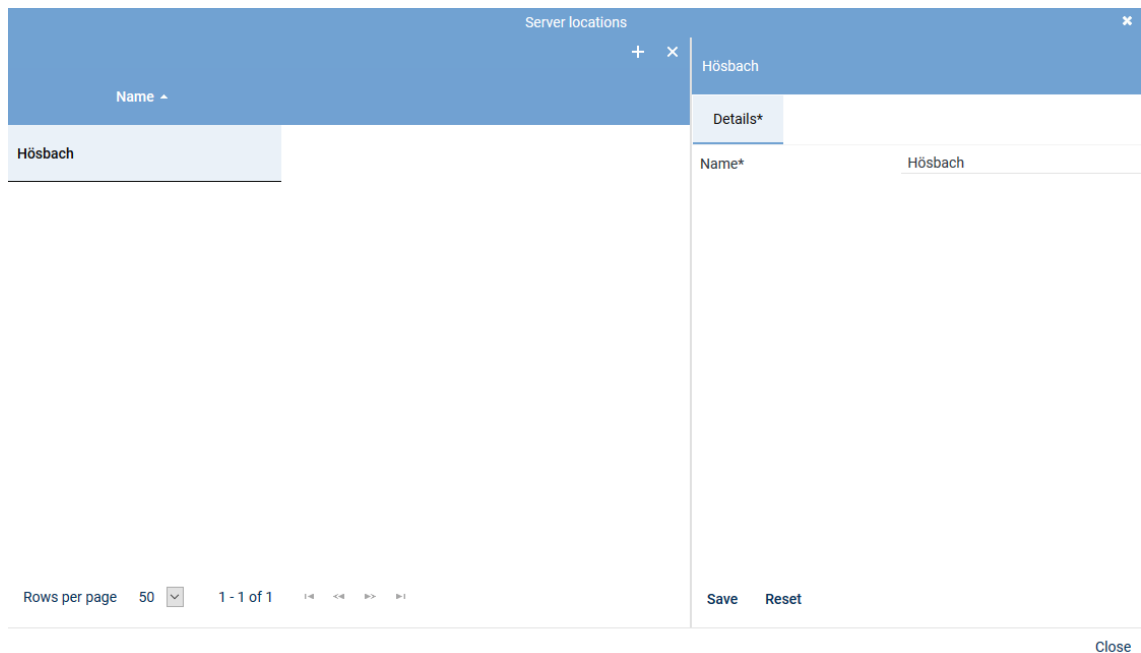
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

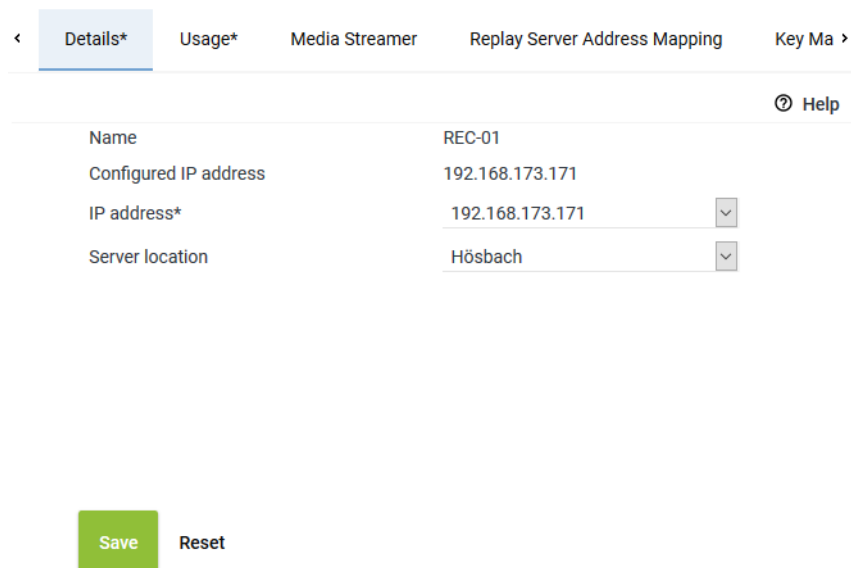
Close

Fig. 158: 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. 159: 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.

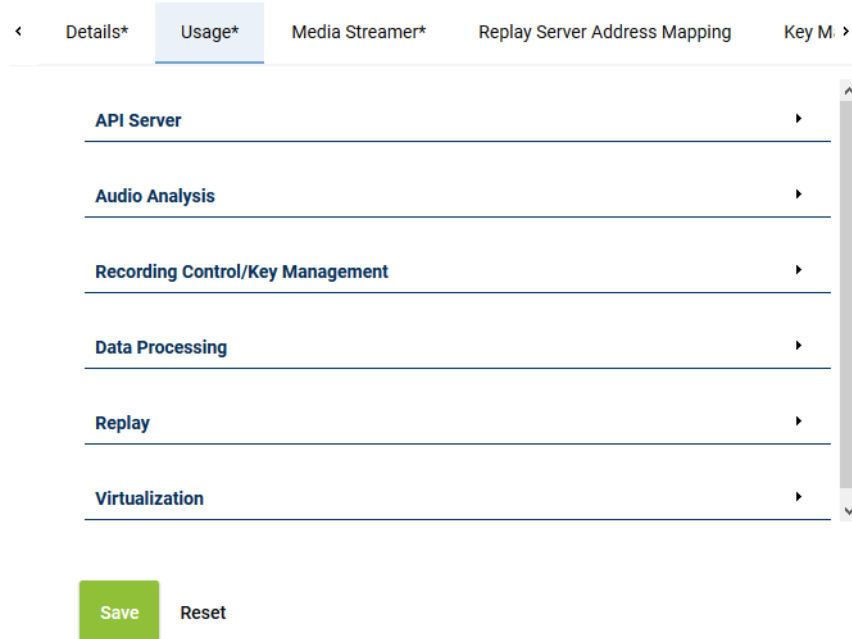


Fig. 160: Servers - tab usage

Group field API Server

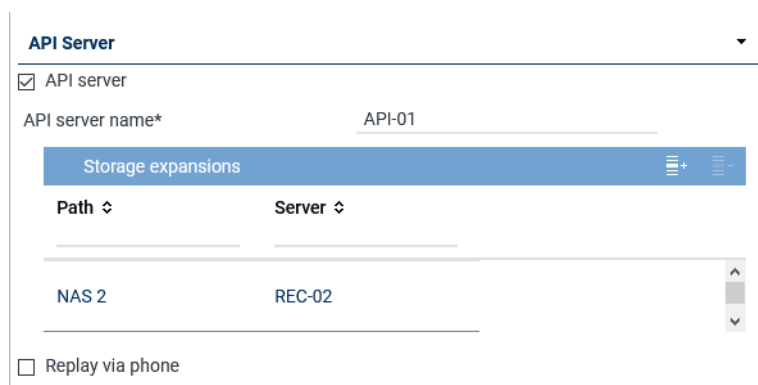




Fig. 161: Group field API Server

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.

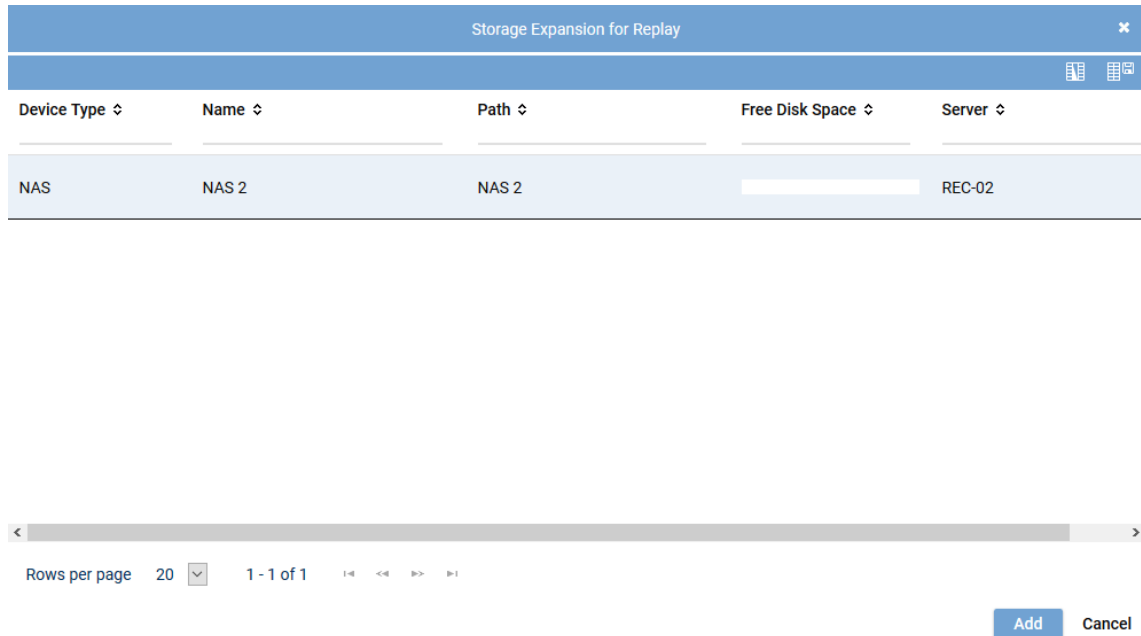
Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

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. 154.</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. 145. • 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 <i>neo</i> 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 <i>PBX</i>, see chapter "Tab Media Streamer", p. 152. To be able to do so, at least 1 <i>PBX</i> 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. 162: 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

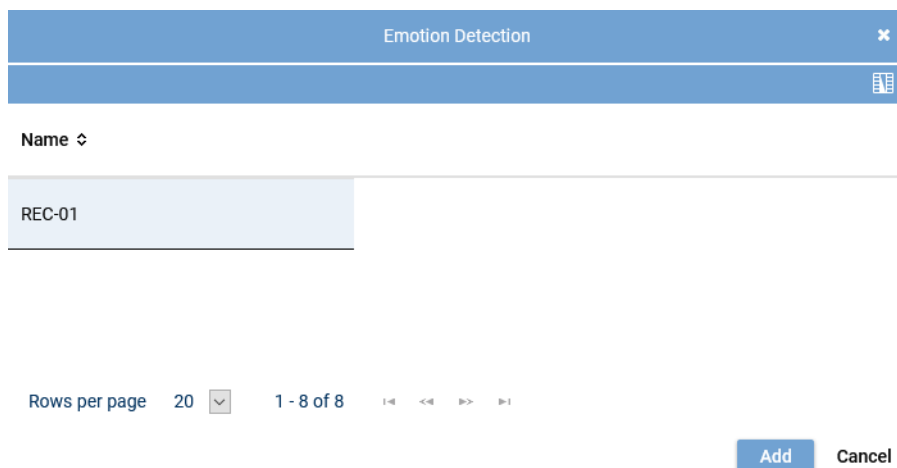
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 163: 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. 42: Configure audio analysis



Emotion Detection

Name ↕

REC-01

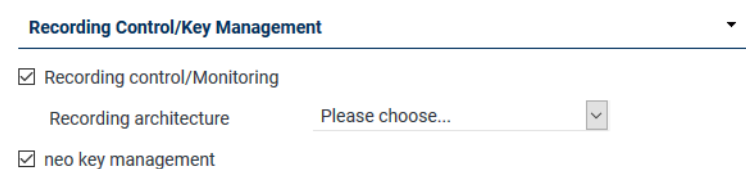
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 164: 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/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 165: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 43: 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. 166: 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  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 149. 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 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. 149. 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 <i>neo</i> to <i>neo</i>, 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. 44: 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

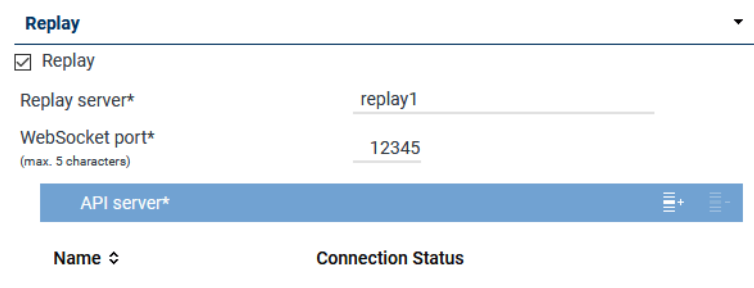
Fig. 167: Select server



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. 168: 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. 150. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 45: 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. 169: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 143](#).

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. 170: 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. 46: 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. 171: 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. 158.</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 <i>8000</i>.</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> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</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: <i>5062</i></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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<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 <i>5060</i>.</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

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

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



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

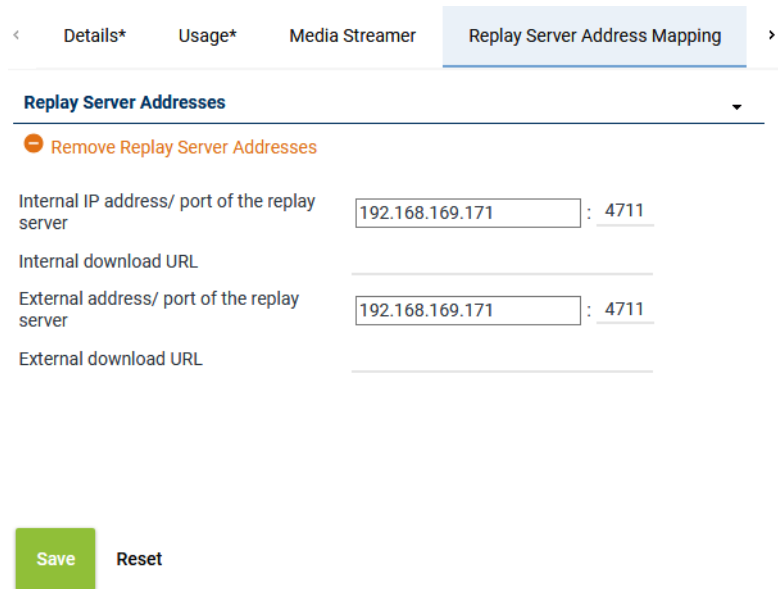


Fig. 172: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

- Enter the following parameters

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



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

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



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

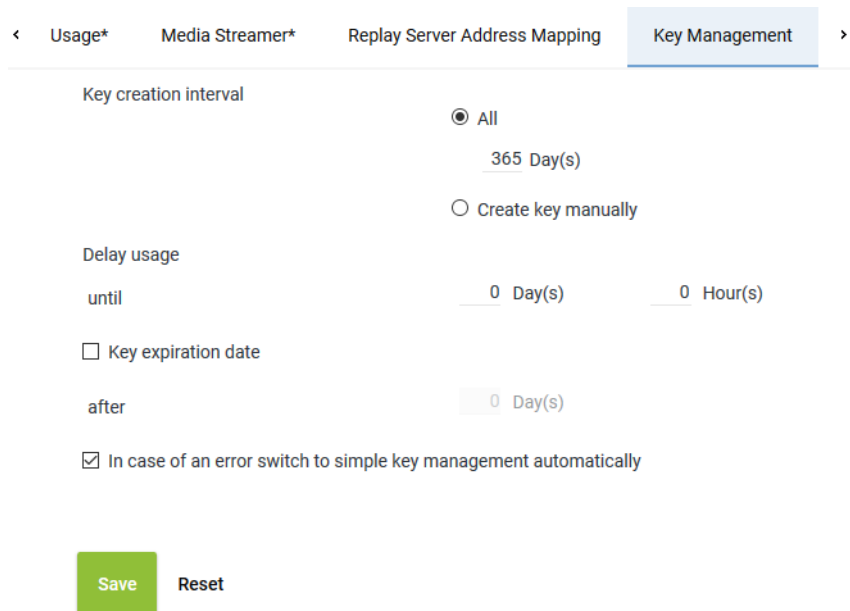


For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

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

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



< 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. 173: 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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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*

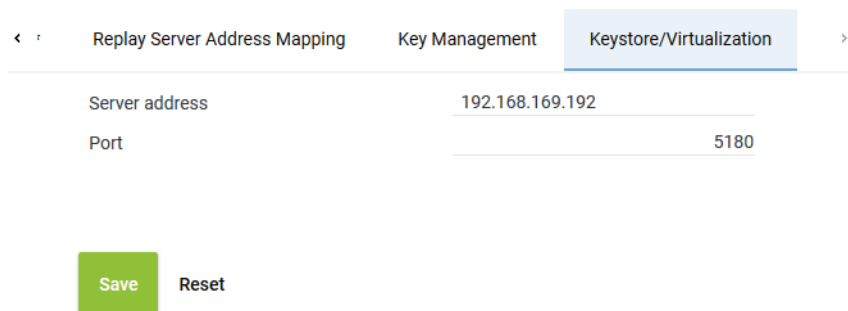
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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. It has three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization' (which 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' (grey).

Fig. 174: 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:

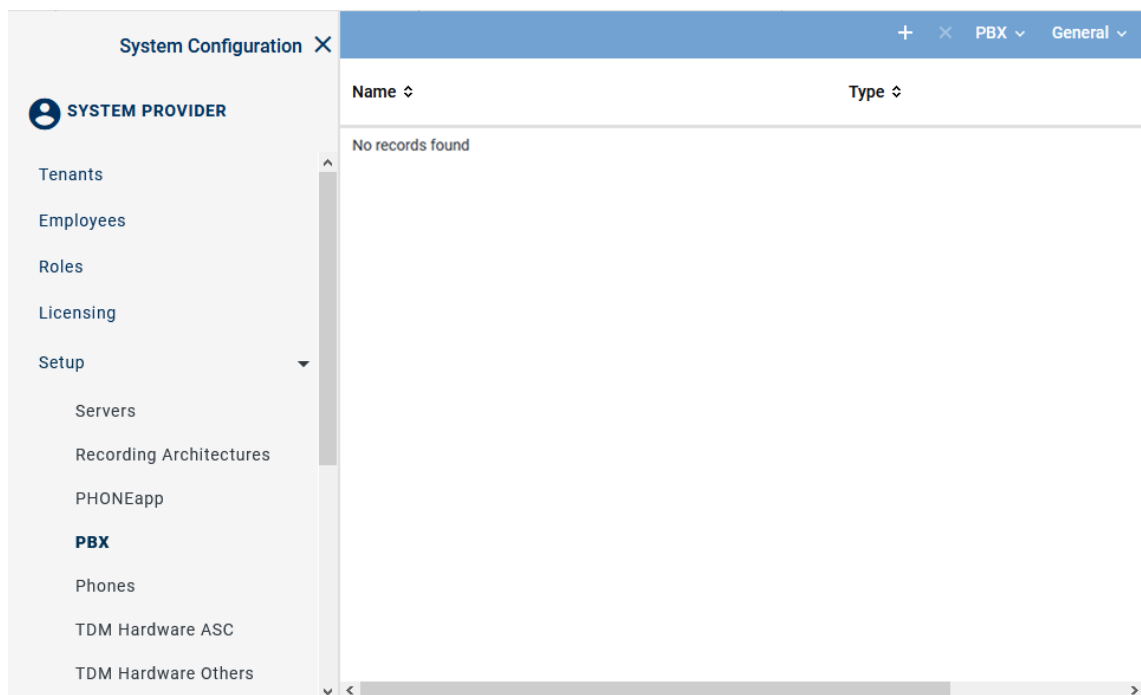


Fig. 175: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

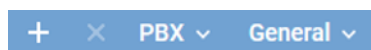




Fig. 176: Toolbar PBX module


	<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. 177: 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 <i>094</i>.
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. 47: Create PBX

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

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

Tab. 48: PBX parameters with complete phone number

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

7.1.2.3.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

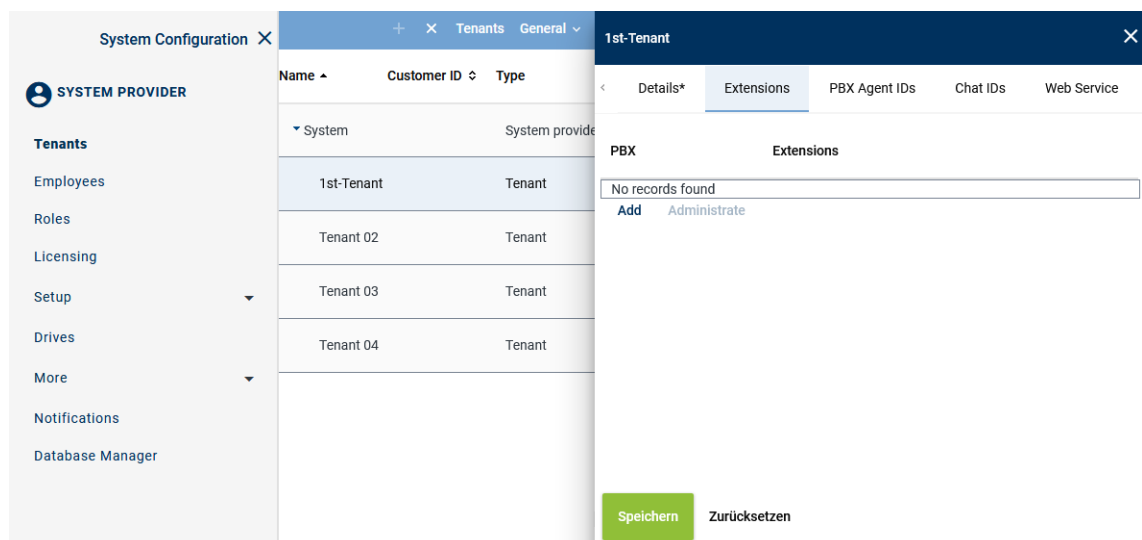


Fig. 178: Tenants - main view - tab Extensions

Add extensions

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

⇒ The following window appears:

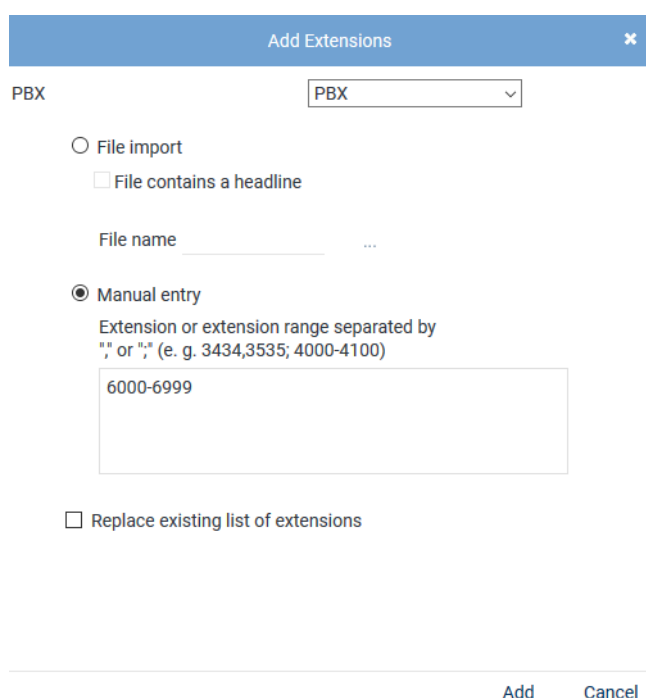




Fig. 179: Assign extensions to tenants

- 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"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <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.

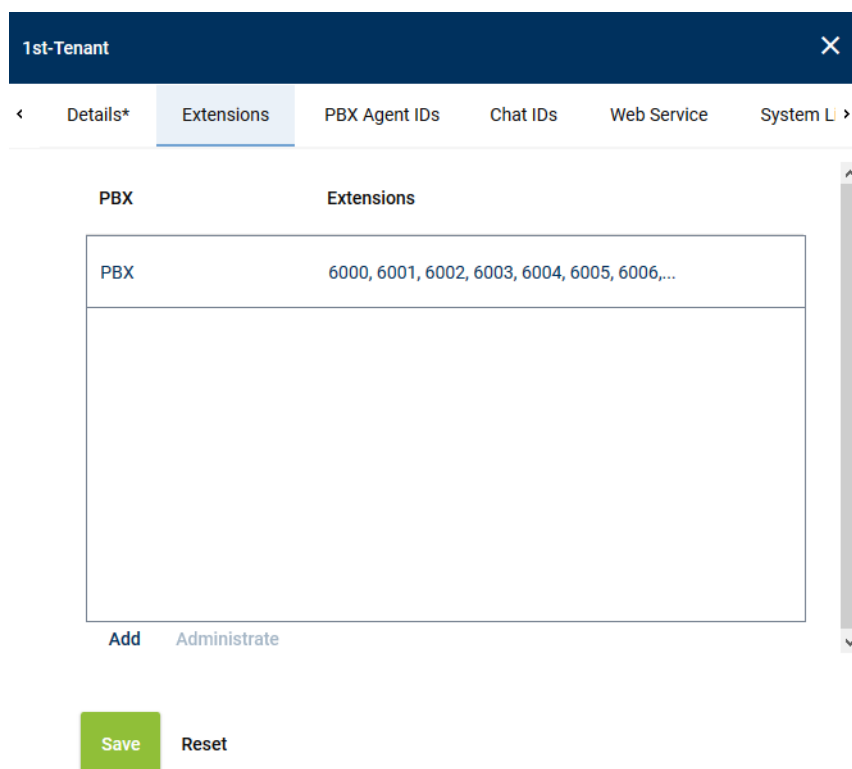
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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.



The screenshot shows a configuration window for '1st-Tenant'. The 'Extensions' tab is active, displaying a table with two columns: 'PBX' and 'Extensions'. The 'PBX' column has a single entry 'PBX', and the 'Extensions' column has the range '6000, 6001, 6002, 6003, 6004, 6005, 6006,...'. Below the table, there are 'Add' and 'Administrate' buttons. At the bottom of the window, there are 'Save' and 'Reset' buttons.

Fig. 180: 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. 181: 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.

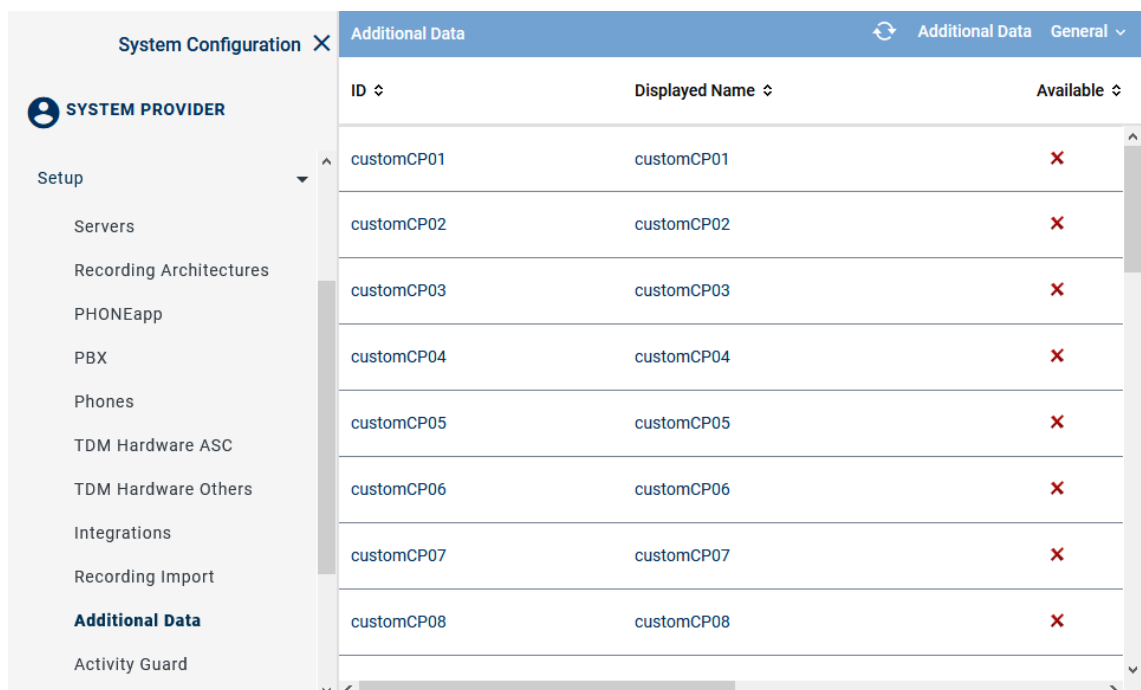


Fig. 182: Additional Data module main view

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. 183: 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. 184: Additional data - configure availability

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



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



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

7.1.2.3.6 Create integration for All-in-one Parallel Recording

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

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

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

1. In the navigation bar, select the menu item *Setup > Integrations*.

⇒ The following window appears:

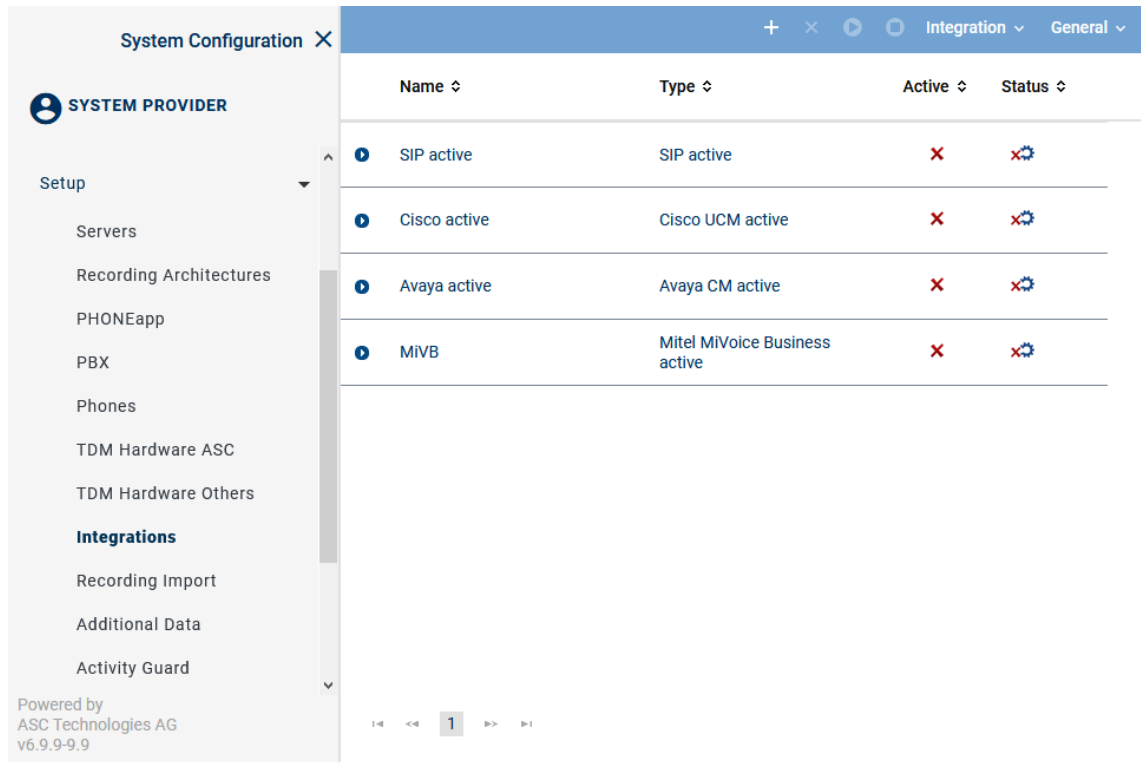


Fig. 185: Integrations - main view

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 ⏏. ✗ = 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. ⚙️ = Configuration is incomplete. </div>

Toolbar of the Integrations module


The toolbar offers the following functions.



Fig. 186: 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.

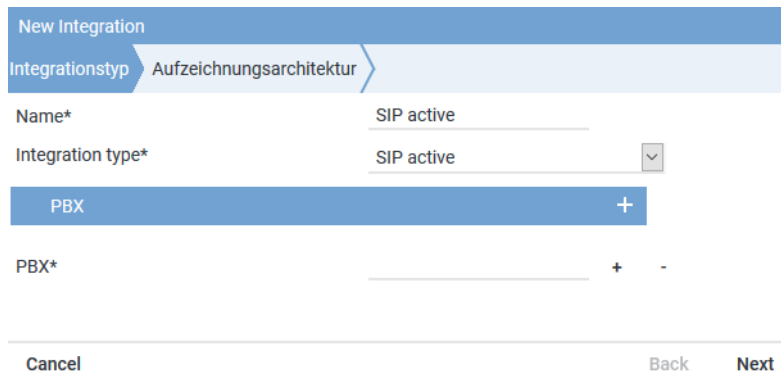



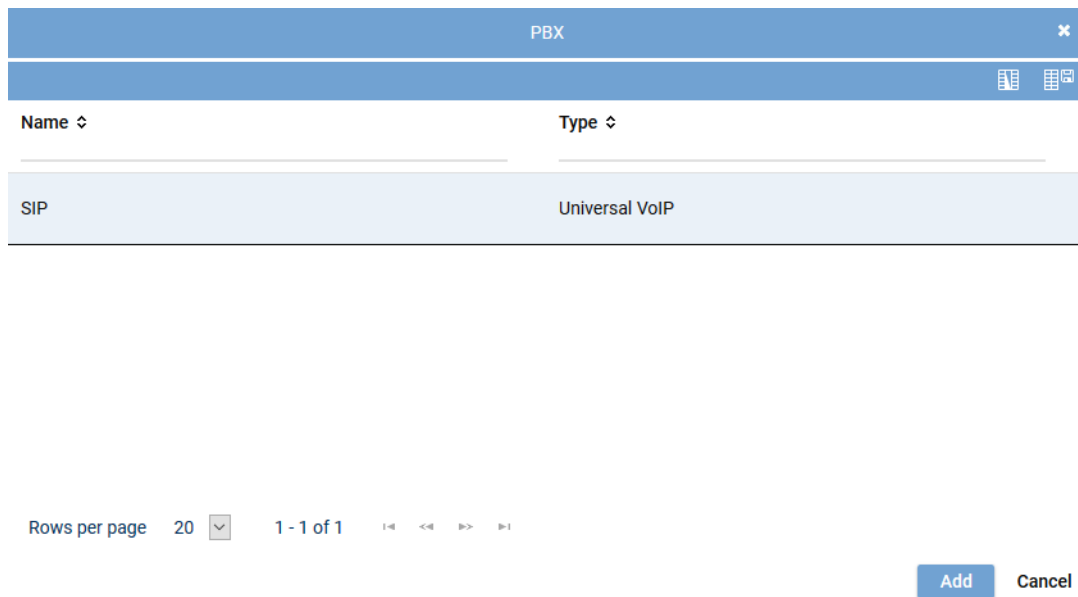
Fig. 187: Create integration type

- 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 49: 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

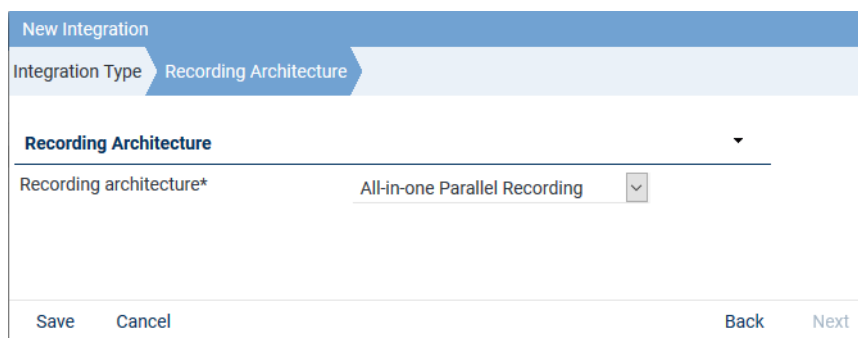
Add Cancel

Fig. 188: 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. 189: Assign recording architecture - All-in-one Parallel

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




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

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



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see [chapter "Duplicates in parallel recording architectures", p. 370](#).

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 active		SIP active	X	⚙️
Step	Configuration			
Configure recording architecture	✓			
Global recording settings	✗			
Configure recording servers	✗			
Configure add-on	✓			
Configure miscellaneous settings	✓			

Fig. 190: 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. 191: 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.

Global recording settings for All-in-one Parallel Recording

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

Step: Global Recording Settings ✕

Details *	Device Group 1*	Device Group 2*	SIP Header Tagging*
Activate PBX connection	<input checked="" type="checkbox"/>		
PBX IP address*	192.168.170.178		
PBX port*	5060		

Save Cancel

Fig. 193: Configure device group 1

Parameter	Description
<i>Activate PBX connection</i>	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
<i>PBX IP address</i>	Enter the IP address of the PBX for the first device group.
<i>PBX port</i>	Enter the port of the PBX which is used to communicate with the PBX.

2. Select the tab *Device Group 2* to configure the connection to PBX 2.

Step: Global Recording Settings ✕

Details *	Device Group 1*	Device Group 2*	SIP Header Tagging*
Activate PBX connection	<input checked="" type="checkbox"/>		
PBX IP address*	192.168.170.178		
PBX port*	5060		

Save Cancel

Fig. 194: Configure device group 2

Parameter	Description
<i>Activate PBX connection</i>	Activate the check box to configure the connection data. If the option has been activated, the entry fields for the IP address and the port become active.
<i>PBX IP address</i>	Enter the IP address of the PBX for the second device group.

Parameter	Description
<i>PBX port</i>	Enter the port of the PBX which is used to communicate with the PBX.

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

Tab SIP Header Tagging

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

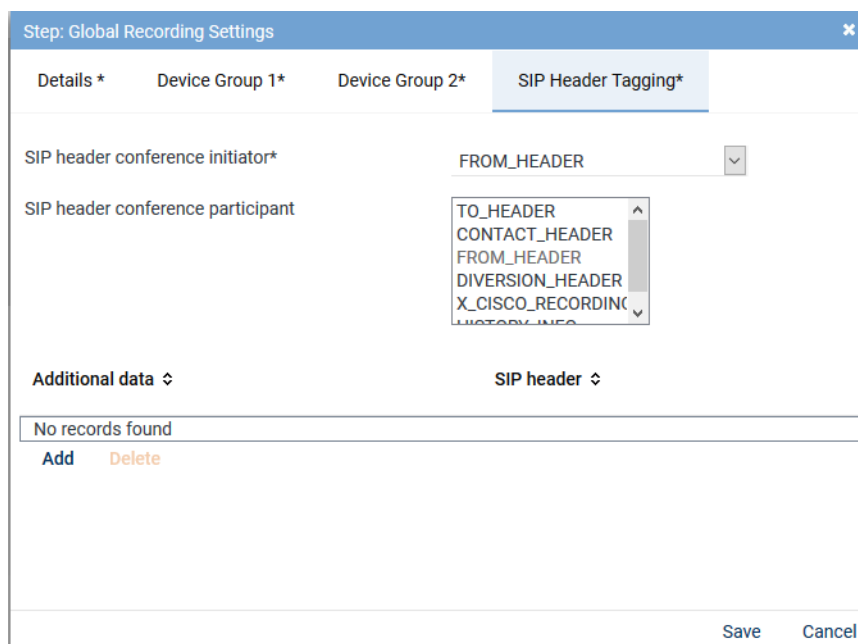


Fig. 195: Tab SIP Header Tagging Configure sources

- Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

Tab. 51: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down.
To deselect an entry, click on it again without releasing the [Ctrl] key.

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

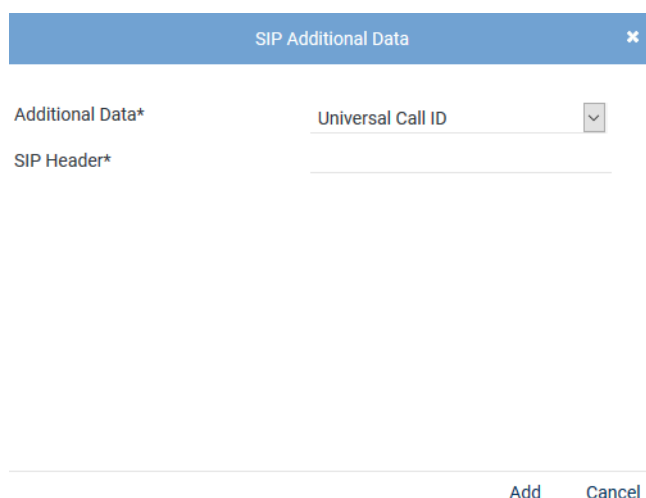


Fig. 196: SIP Additional Data



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

4. Enter the following parameters:

Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.


Tab. 52: Configure SIP conversation parameters

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

Configure recording server for All-in-one Parallel Recording

For parallel recording to run smoothly, you must define a port range for both recording servers. The range may be the same on both recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

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

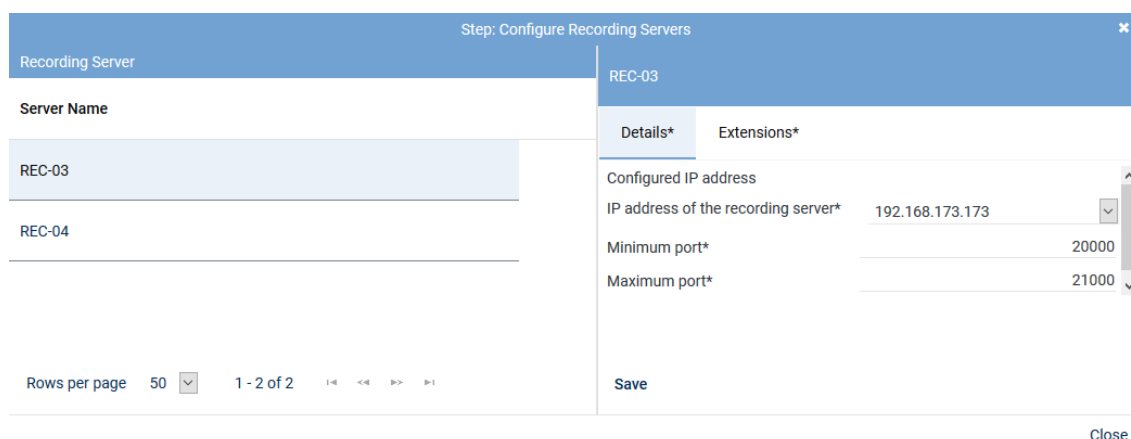


Fig. 197: Configuration step - Configure recording servers

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

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

Tab. 53: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

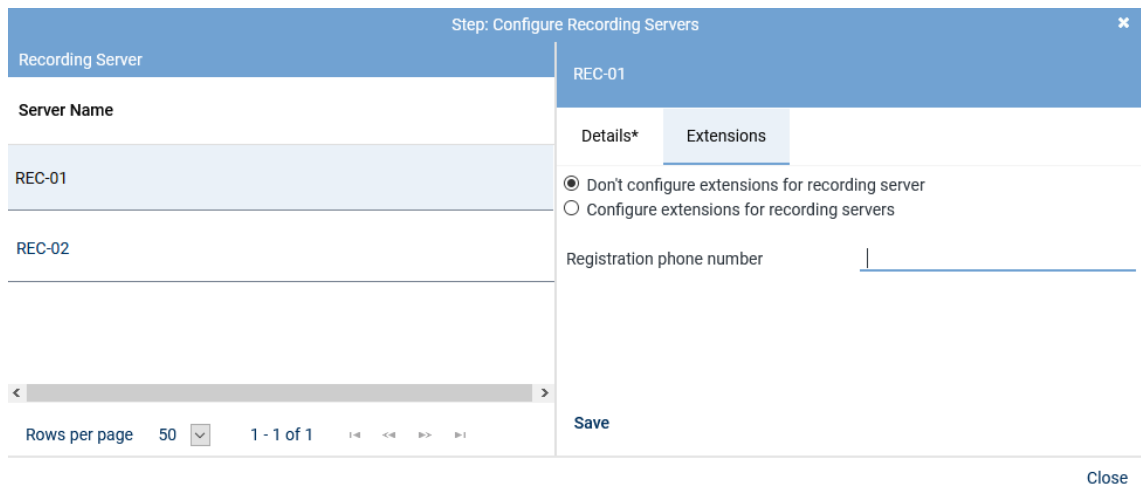


Fig. 198: Recording server - Configure extension for SIP trunk



Ask your provider whether registering 2 servers in parallel mode is supported. To do so, it must be possible to assign a [SIP](#) trunk phone number to 2 different IP addresses at the same time.

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a [SIP](#) trunk phone number instead.



If you do not define a phone number for the [SIP](#) trunk of the recording server, all incoming [SIP](#) connections are accepted without being examined.

Registration phone number Enter a registration phone number for the [SIP](#) trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the [SIP](#) trunk, see [chapter "Global recording settings for All-in-one Parallel Recording", p. 169](#).

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

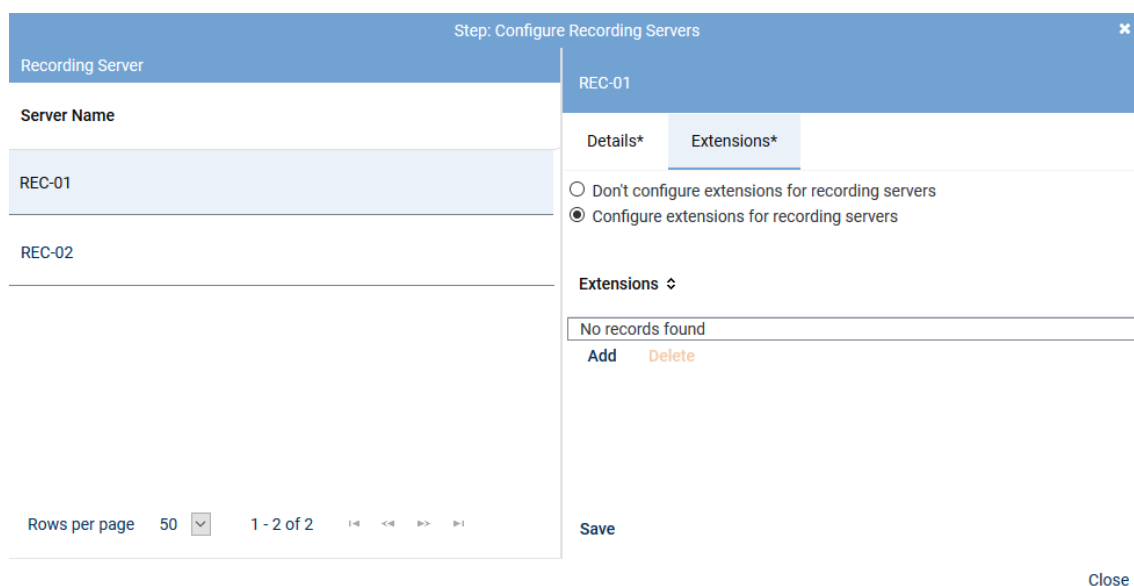


Fig. 199: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

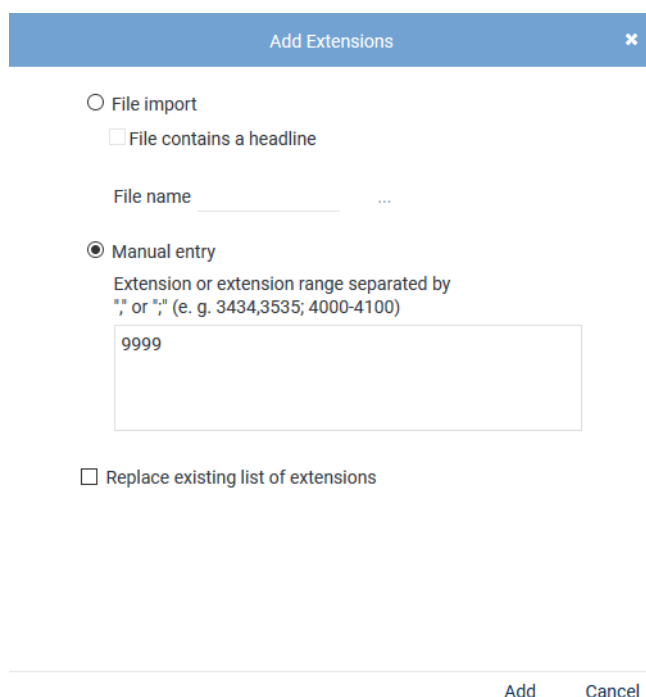


Fig. 200: Add extensions

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

6. The configured extensions now appear in the detail view.

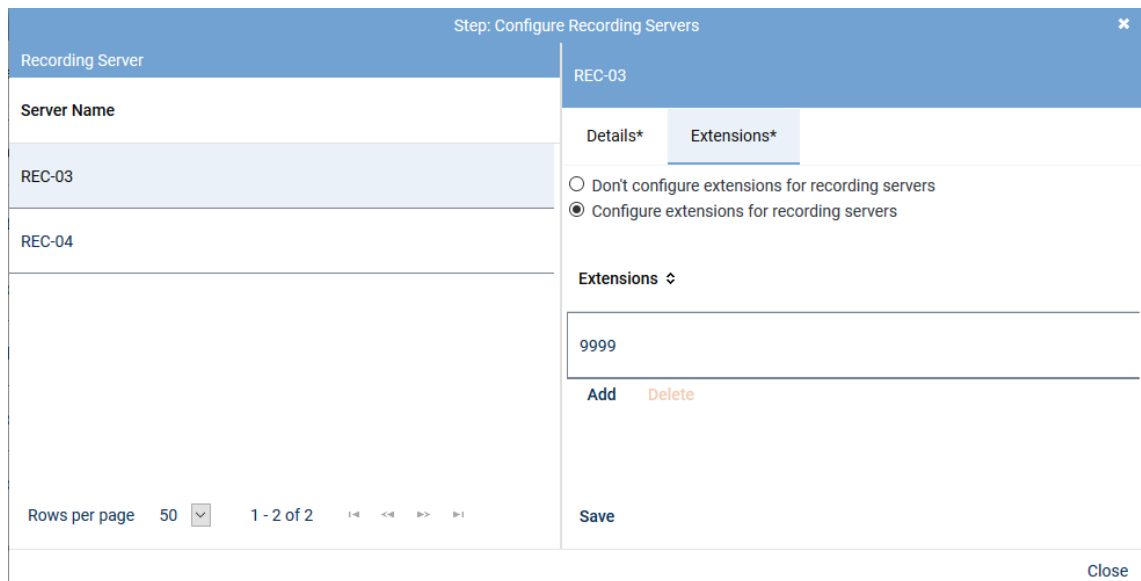


Fig. 201: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the [SIP](#) registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the [SIP](#) end-points again.

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

Configure add-on



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

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



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



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

Configure add-on for Sparkassen FI ISP (optional)

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



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

The integration runs in combination with a PBX and the recording server. The service **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

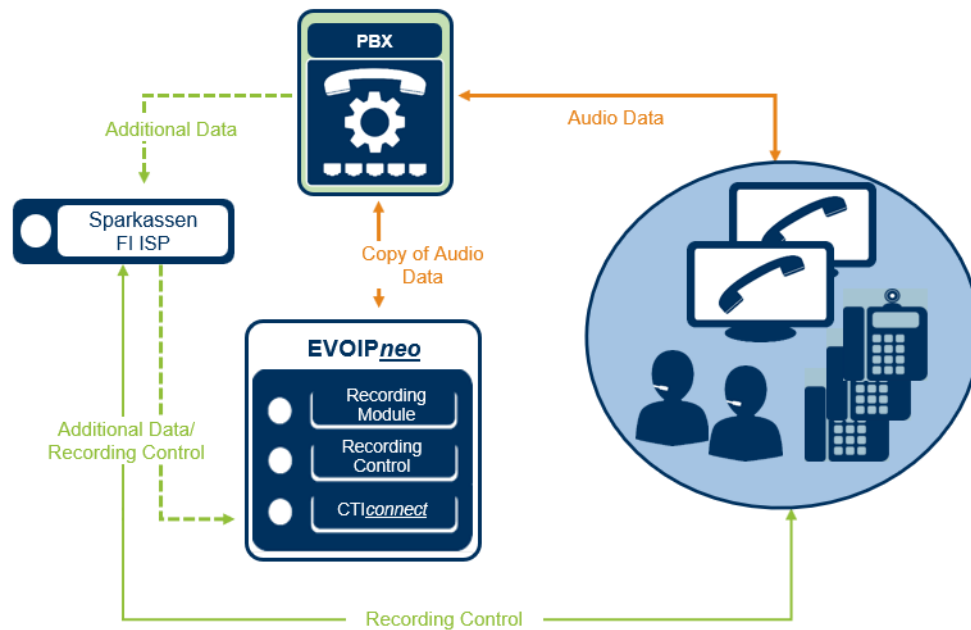



Fig. 202: Overview of Sparkassen FI ISP

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

TypeCTIconnect passive
Grammar name*ISP Sparkassen FI
Grammar version*1.00.05

Connection Data

Listener port*3468

Additional Data

ID des Call CentersCall Center ID
ID des Calls aus GenesysUniversal Call ID
Anmeldename des KundenUser name
Name des KundenCustomer name
Personennummer des KundenCustomer ID

Arbitrary assignment

Please select...
Please select...
Please select...

SaveCancel

Fig. 203: 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. 54: Configure CTIconnect module



For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

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

Tab. 55: 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.

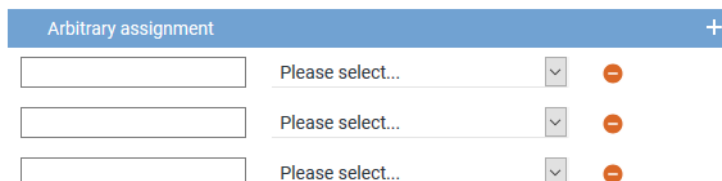



Fig. 204: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)"](#), p. 384.

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. 205: 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. 56: 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:

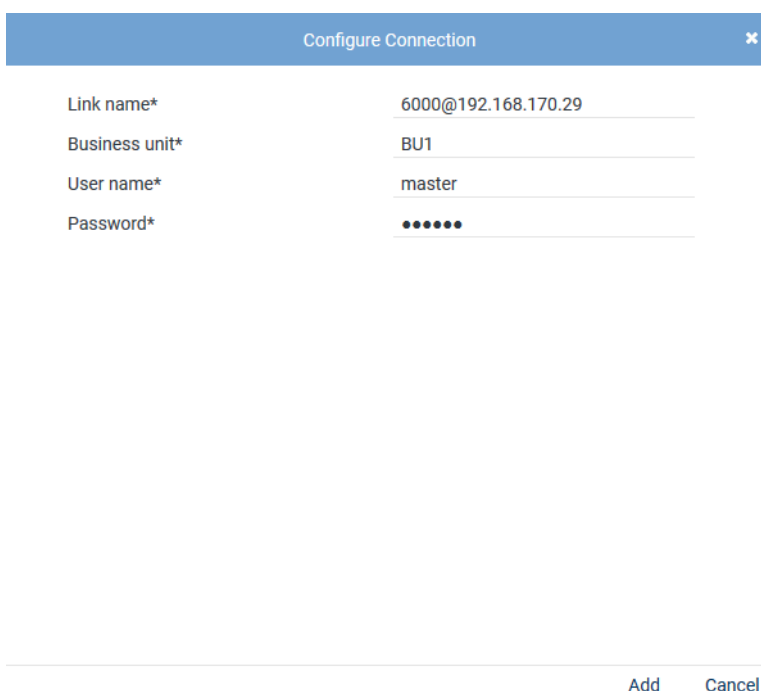


Fig. 206: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 57: 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.

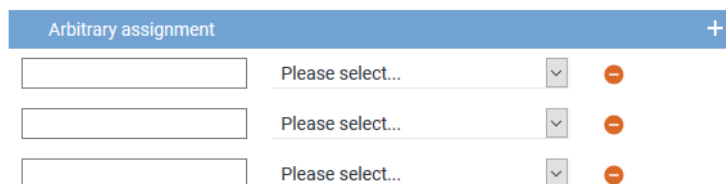




Fig. 207: Arbitrary assignment of the additional data

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 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

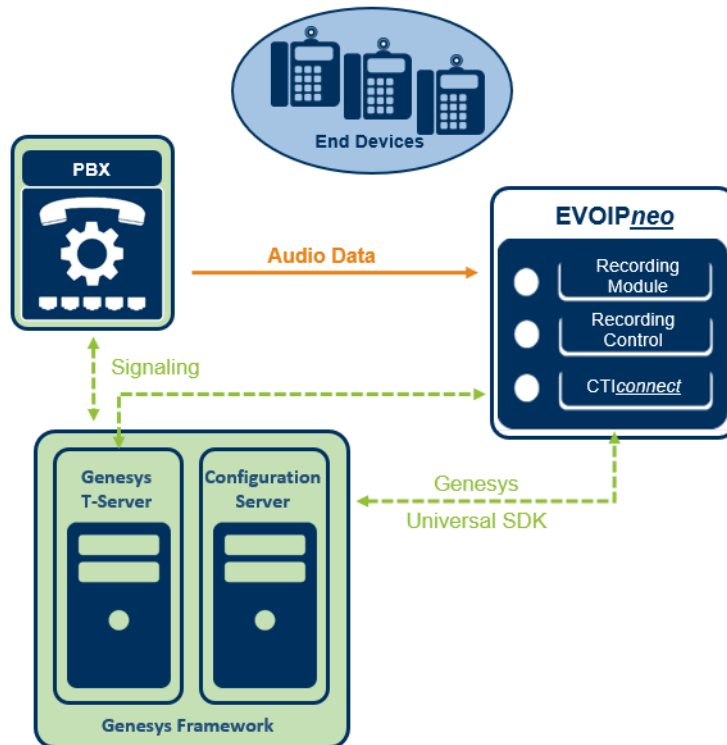


Fig. 208: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

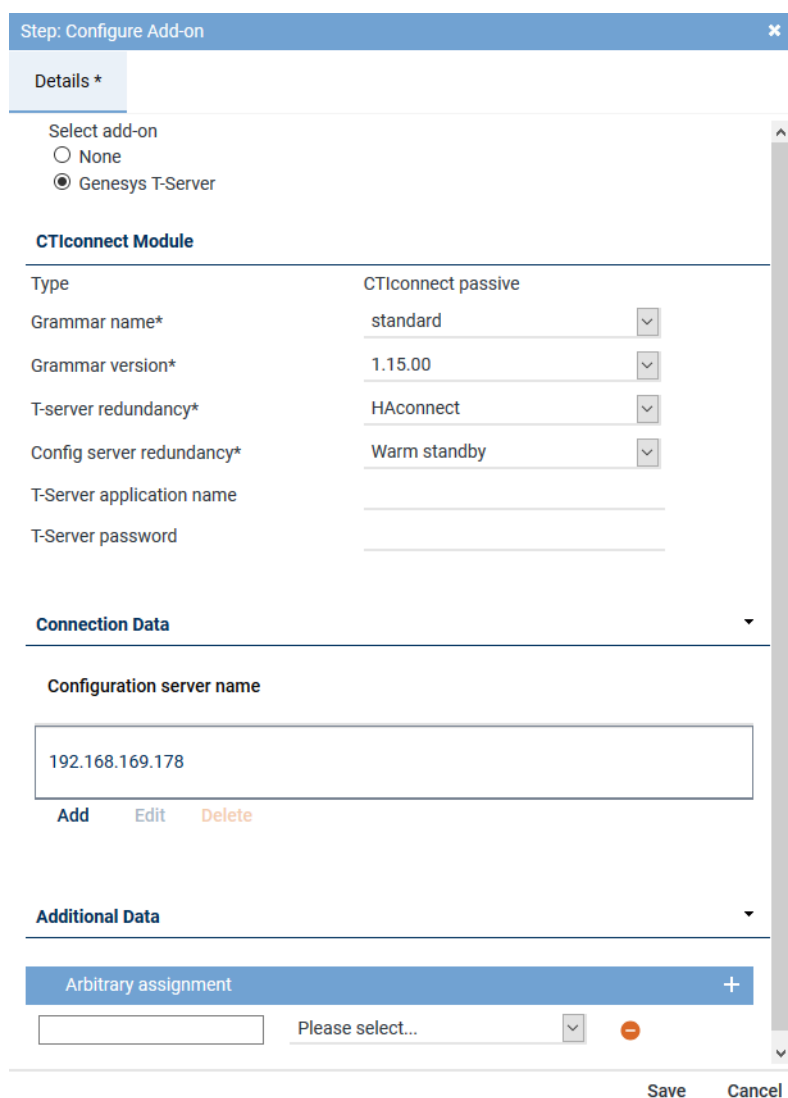


Fig. 209: Configure add-on for Genesys T-Server

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.

Parameter	Value/Description
	<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. 58: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

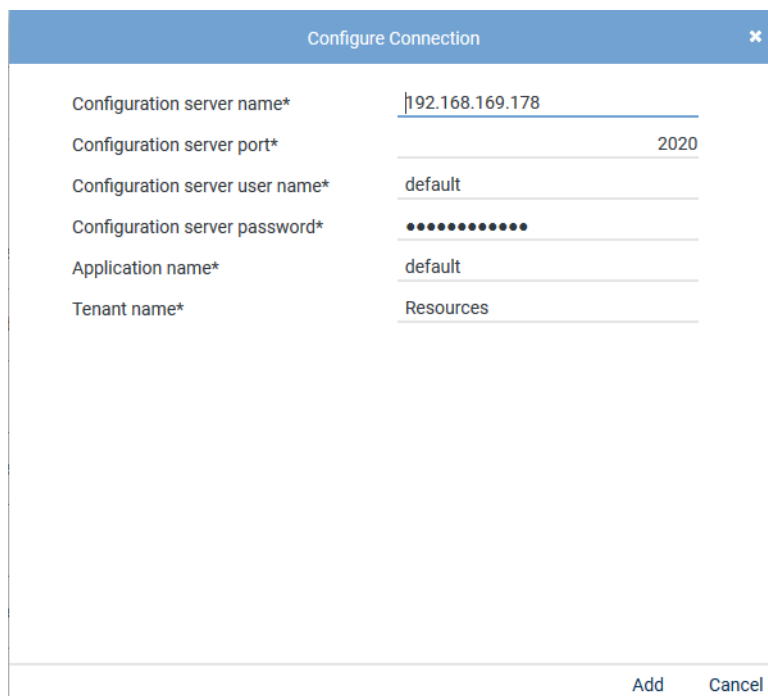


Fig. 210: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<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.

Parameter	Value/Description
<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. 59: 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.

Arbitrary assignment			+
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖

Fig. 211: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select... ▼

Save

Cancel

Fig. 212: 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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 213: 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 active	SIP active		

Fig. 214: Activated integration



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



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






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

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

Deactivate/Delete integration

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

- 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 active	SIP active		

Fig. 215: 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:

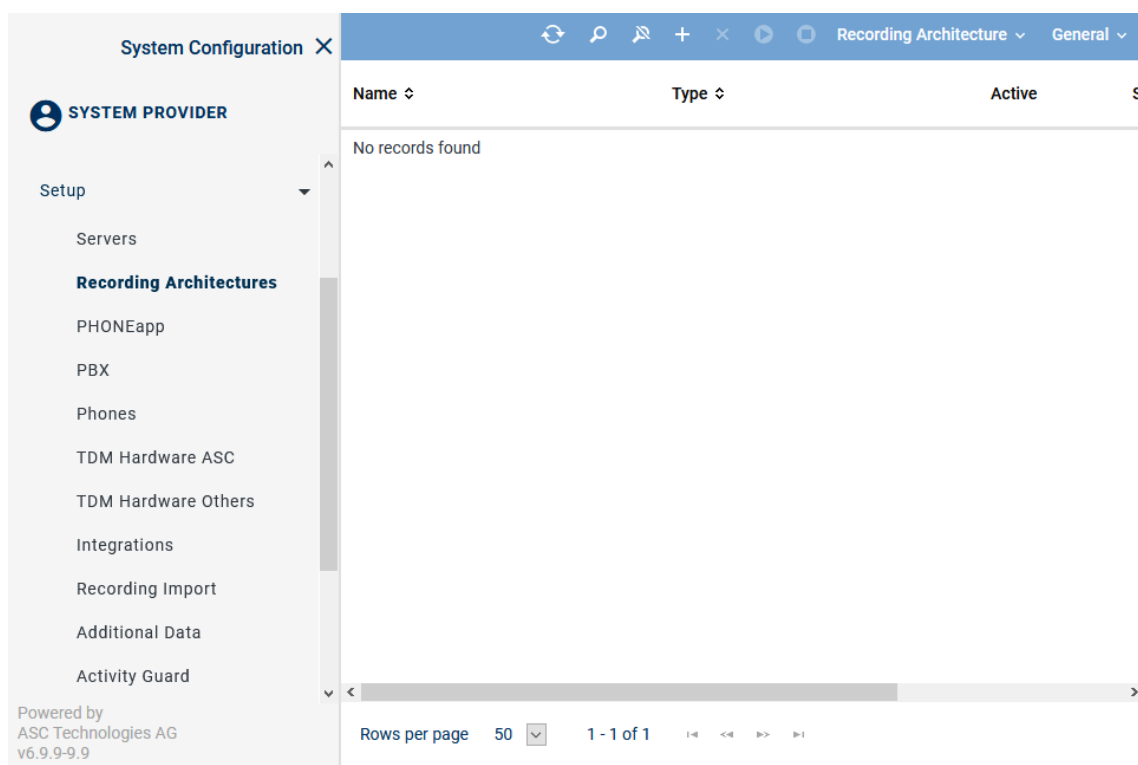




Fig. 216: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. <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. 217: 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.

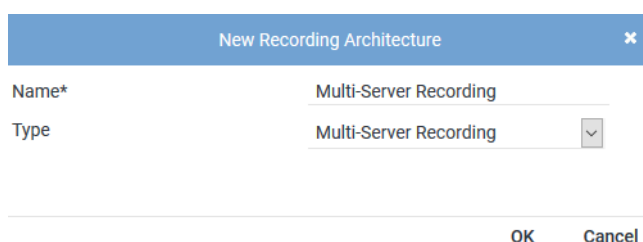
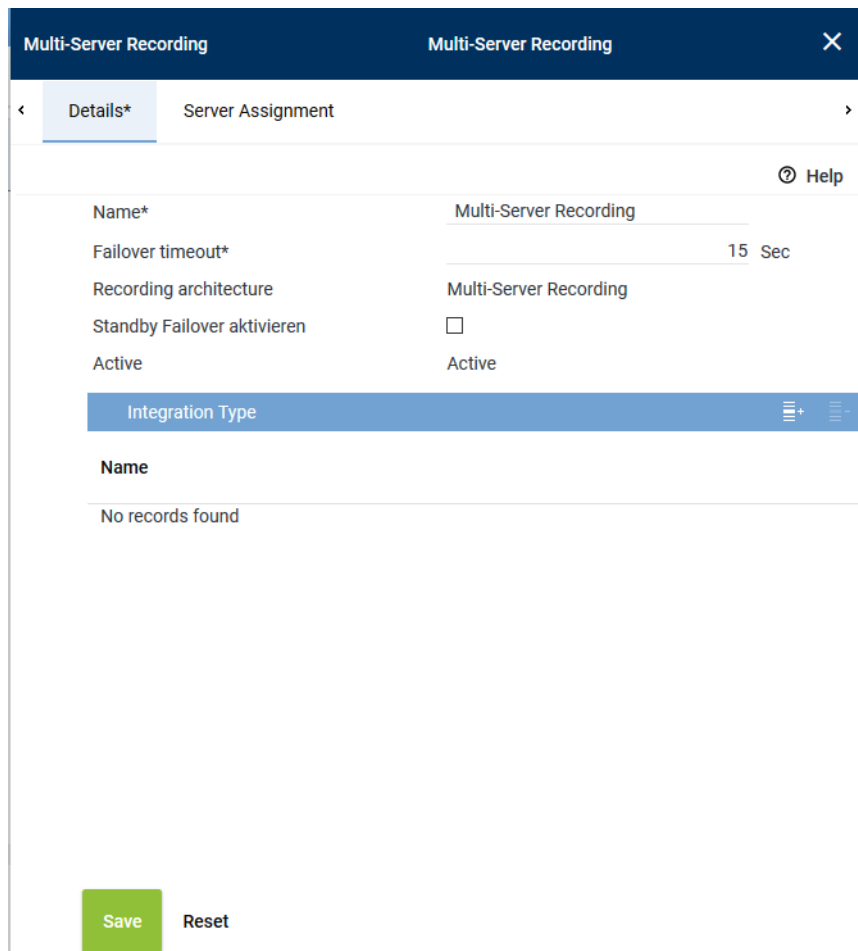


Fig. 218: Create recording architecture - Multi-Server Recording

- 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 "Save" and "Reset" buttons.


Fig. 219: Recording architecture - tab Details - Multi-Server Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture.



Set the failover timeout to a minimum of 15 seconds until the failover process is initiated. Depending on the system architecture it may be useful to set the timeout even higher. The timeout defines how long to wait until the failover process is started. If the state switches back to OK within this time, the failover process is not initiated.

Add integration type

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

Integrationstyp

Name

SIP active

Hinzufügen

Abbrechen

Fig. 220: Select integration type



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



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

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

Assign server for Multi-Server Recording

1. Click on the tab *Server Assignment* to configure the distribution of the recording components for the recording architecture *Multi-Server Recording*.

Group field Recording Control and 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. 221: 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. 222: Recording architecture - assign server - example


2. Select the server for the *Recording Control module*.
3. Click on the button *Add*.
⇒ The name of the server appears in the detail view.
4. To delete an assignment, click on the icon .

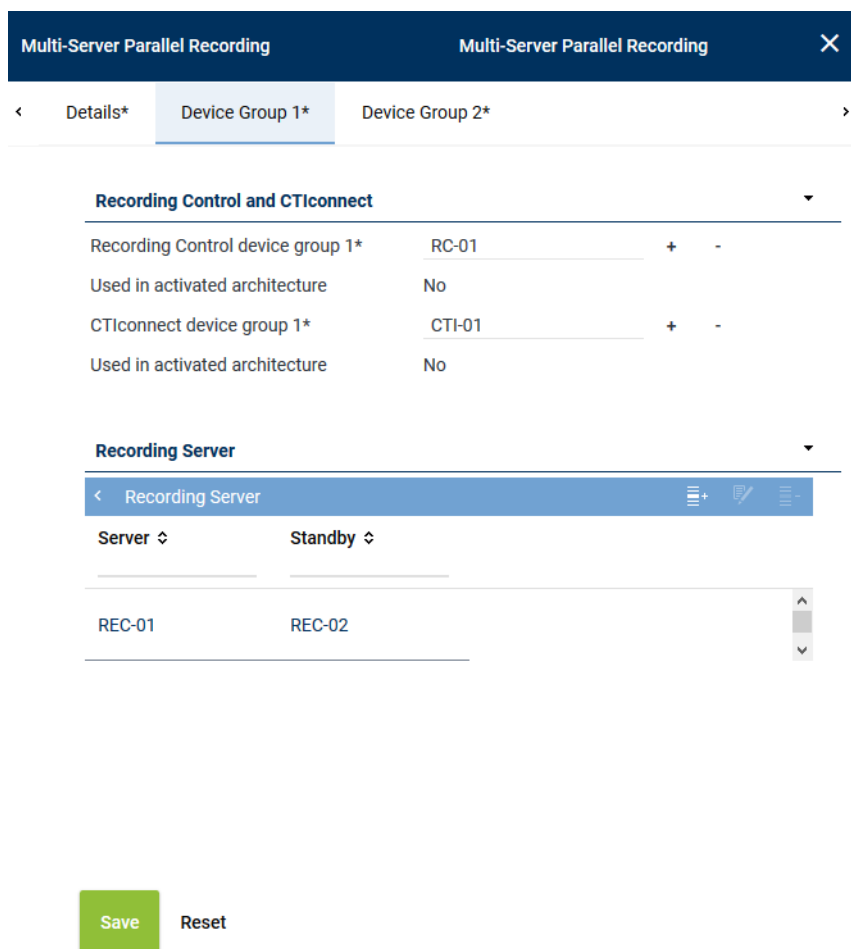


A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the *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. 223: Add recording server

2. Following the steps described above, go to the entry field *Primary server* and click on the icon  to select the primary server where recording is supposed to be active.
3. In the entry field *Standby server*, click on the icon  to select the standby server which is supposed to do the recording in case of an error.
4. Tick the check box to activate the recording type you would like to use for this server.
NOTICE! You can activate several recording types if the integration supports them and if the corresponding licenses have been installed.

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

Activate recording architecture

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










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

Fig. 224: Recording architecture - activate recording architecture

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



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

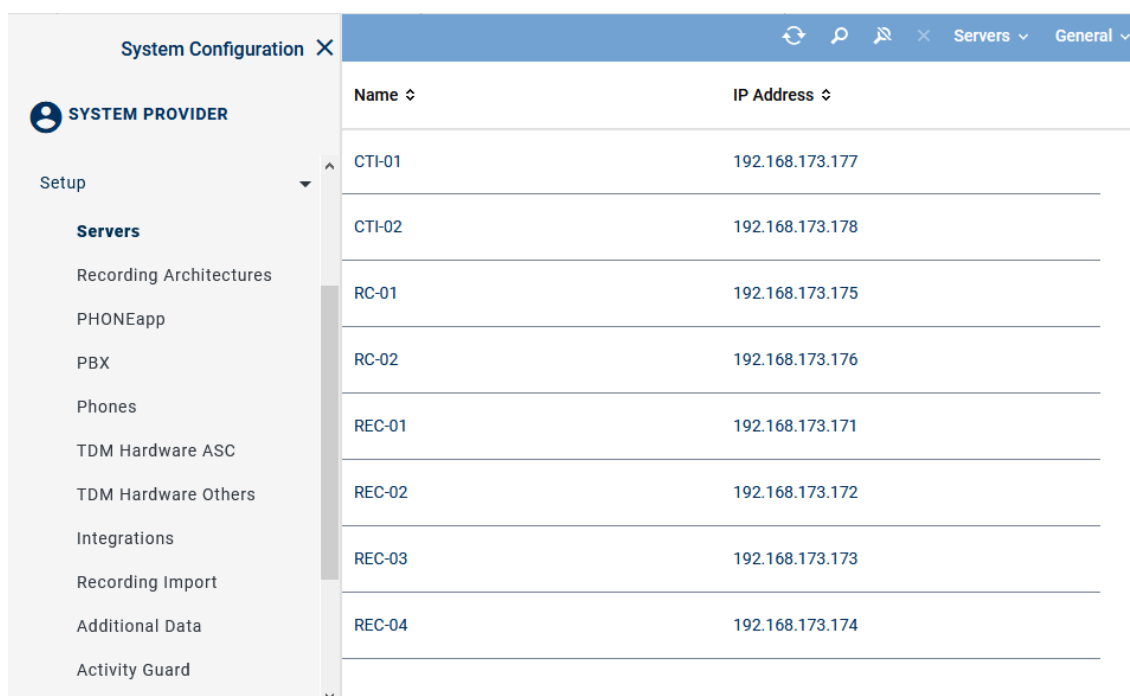


If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.1.2.4.2 Configure server

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

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



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. 225: 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.

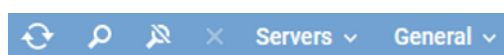







Fig. 226: Toolbar Servers module

	<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. 200.
	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.

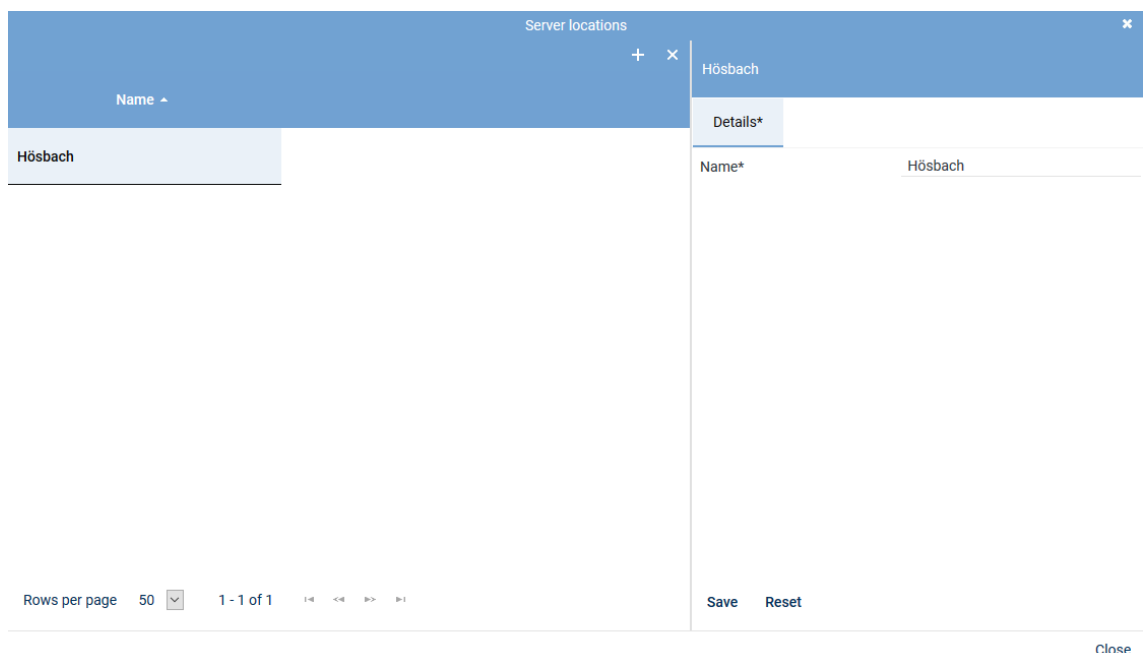



Fig. 227: Add server locations

- 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.

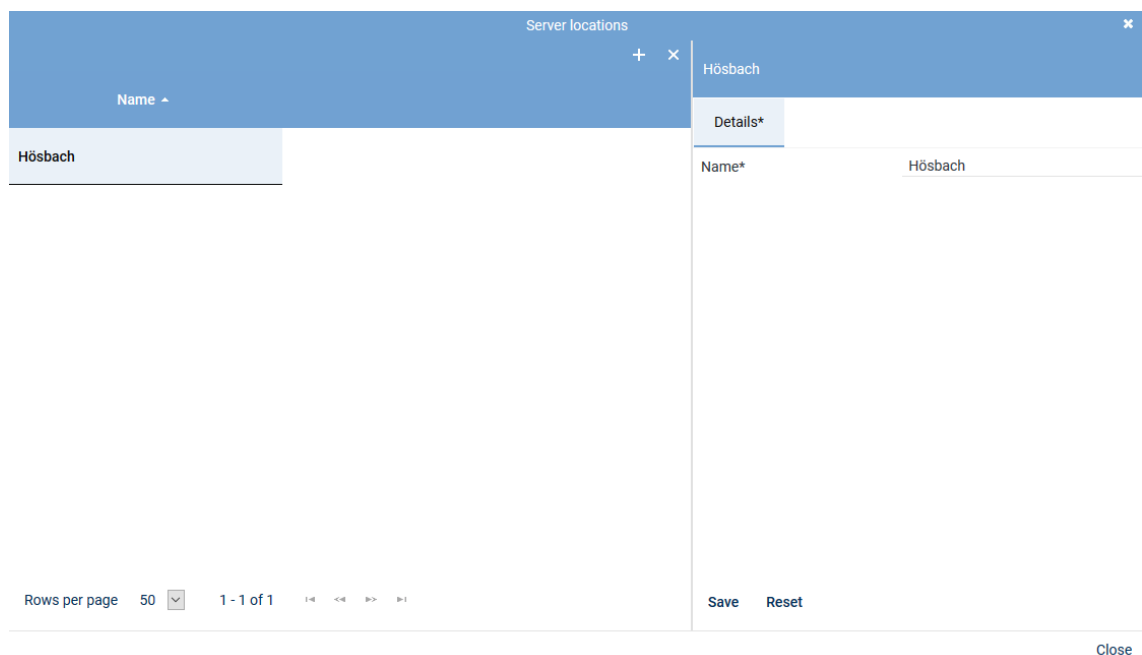



Fig. 228: Delete server location

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

Tab Details

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

<
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. 229: 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. 230: Servers - tab usage

Group field API Server

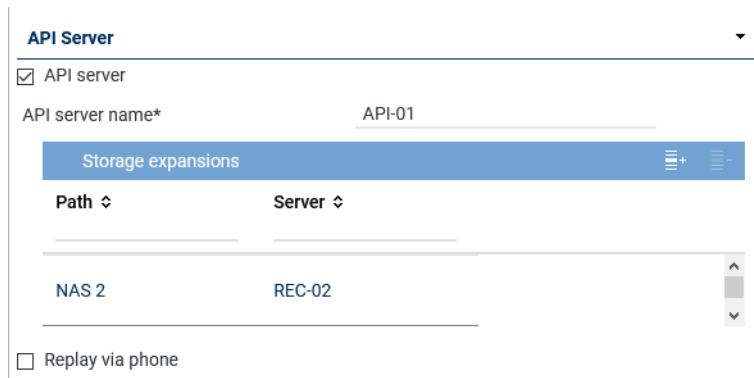




Fig. 231: Group field API Server

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


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

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


Parameter	Value/Description
<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. 213.</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. 204. By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.

Parameter	Value/Description
	<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. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> 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. 211. 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. 232: 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. 233: 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. 60: Configure audio analysis

Emotion Detection ×

📋

Name ↕

REC-01

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

Add Cancel

Fig. 234: 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/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 235: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 61: 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

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 236: Group field Data Processing

EVOIP_{neo} active for SIP - _{neo} 6.x Rev. 17


206 / 406

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<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  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 208. 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. 208. 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!</p> <p>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>

Parameter	Value/Description
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<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 <i>neo</i> to <i>neo</i>, 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. 62: 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

Rows per page 20 1 - 6 of 6

Add Cancel

Fig. 237: Select server



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

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

Group field *Replay*

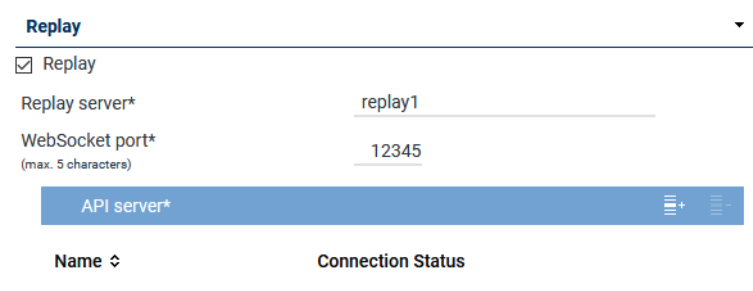




Fig. 238: Group field *Replay*

Parameter	Value/Description
<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>

Parameter	Value/Description
	<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. 210. By clicking on the icon  (Remove), you can remove selected API servers from the list.

Tab. 63: 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. 239: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 203.

- 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. 240: 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. 64: 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. 241: 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. 218.</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> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</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 UDP = unencrypted 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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address 169.254.254.101.</p>
<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 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. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.



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

[Details*](#)
[Usage*](#)
[Media Streamer](#)
[Replay Server Address Mapping](#)

Replay Server Addresses

 Remove Replay Server Addresses

Internal IP address/ port of the replay server: :

Internal download URL:

External address/ port of the replay server: :

External download URL:

Fig. 242: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

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



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

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



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



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

Tab Key Management

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

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

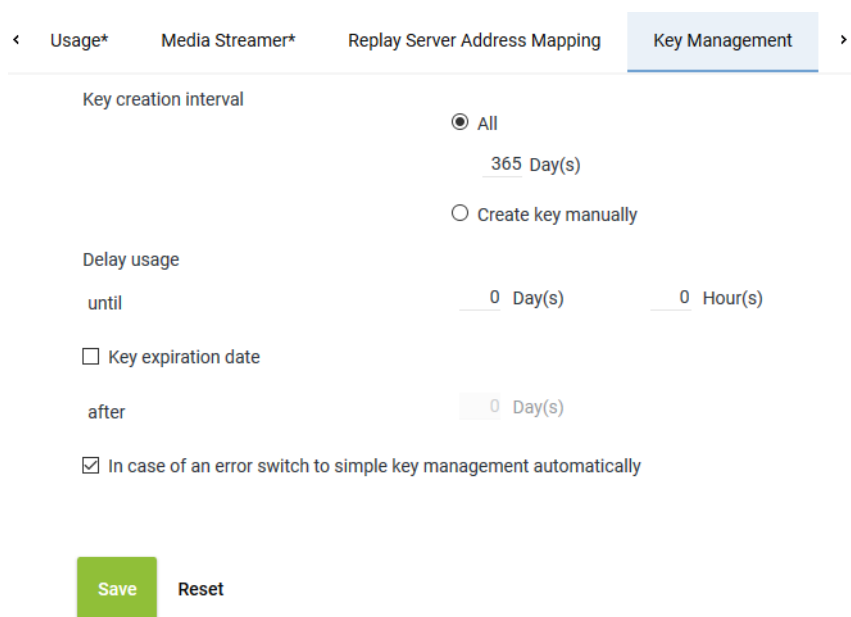


Fig. 243: Servers module - tab Key Management

Key creation interval	<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. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.
Delay usage	<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. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
Key expiration date	<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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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.

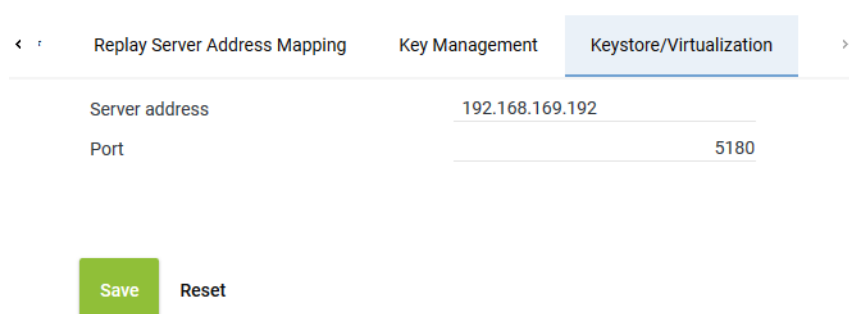
- *Trusted Virtualization License*

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' (grey).

Fig. 244: 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:

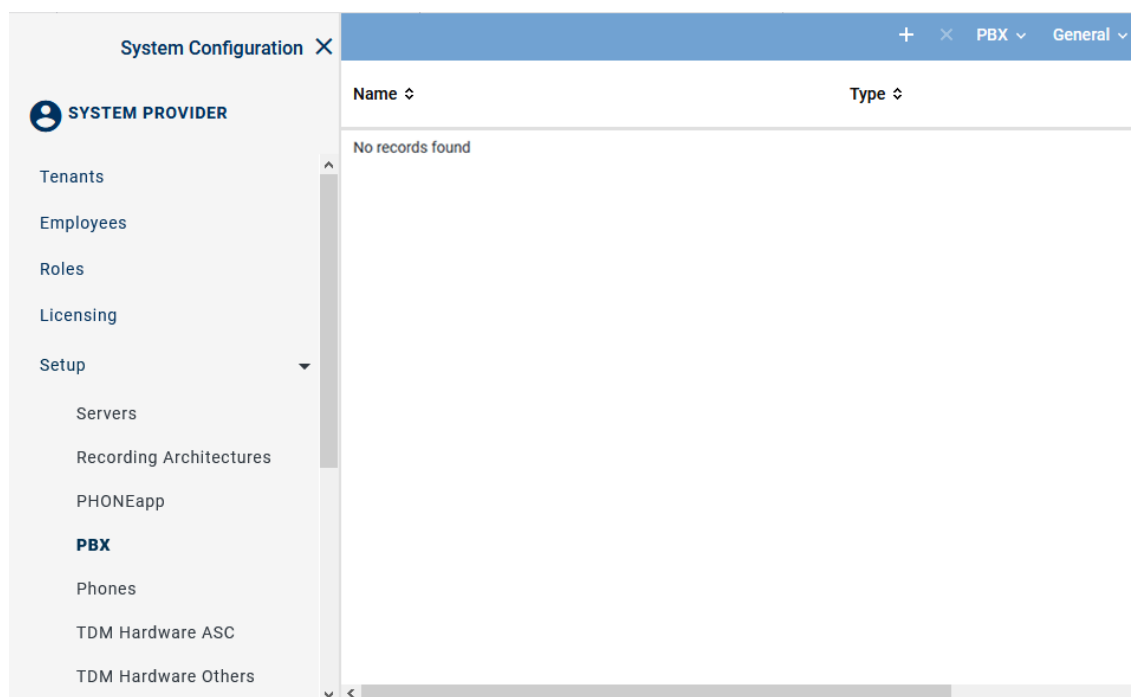


Fig. 245: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

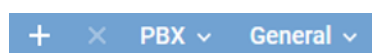




Fig. 246: Toolbar PBX module


	<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.

Module Help Opens the module-specific online help.



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

Create new PBX

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

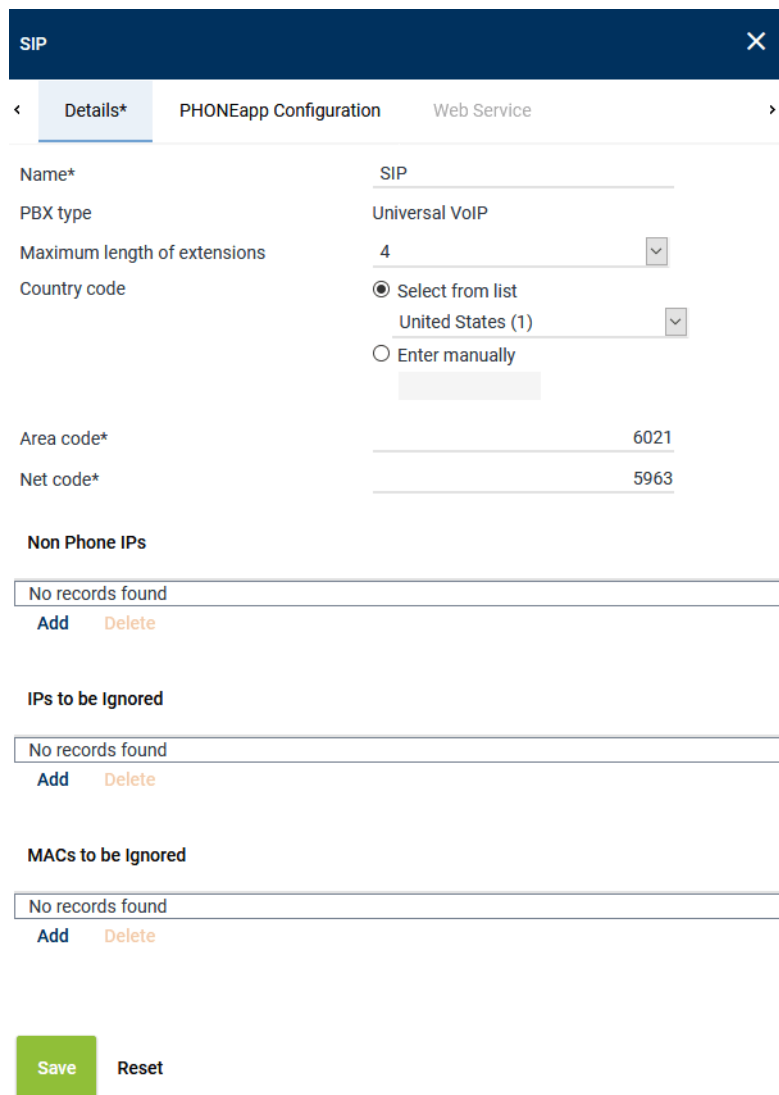


Fig. 247: Create new PBX - tab Details

- 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.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Enter manually</i> <p>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>.</p>
<i>Area code</i>	Enter the area code without the preceding <i>0</i> , e. g. <i>6021</i> .
<i>Net code</i>	Enter the net code, e. g. <i>5963</i> . Do not enter an extension here.

Tab. 65: Create PBX

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

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

Tab. 66: PBX parameters with complete phone number

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

7.1.2.4.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

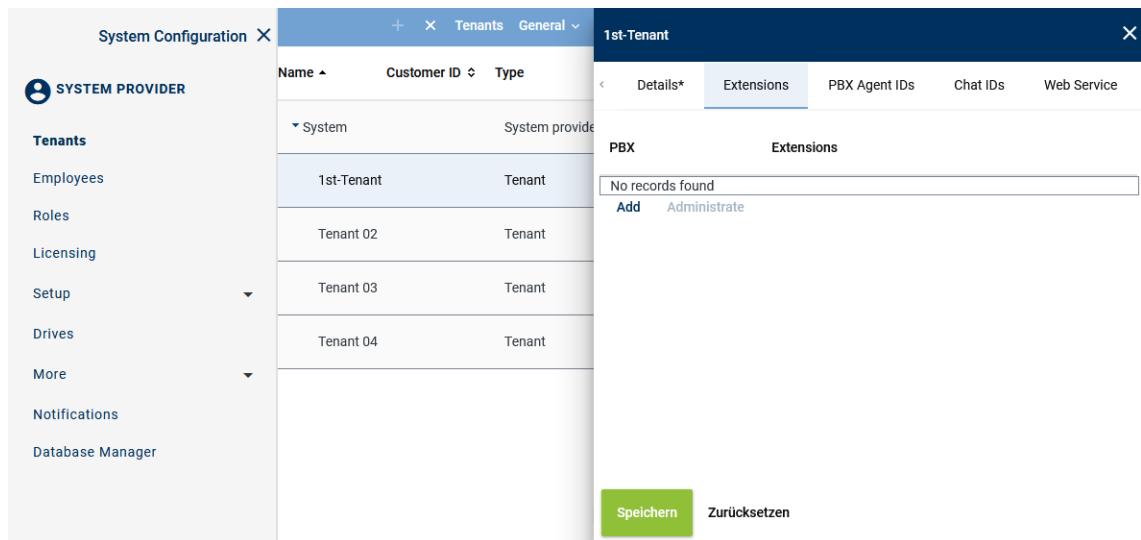
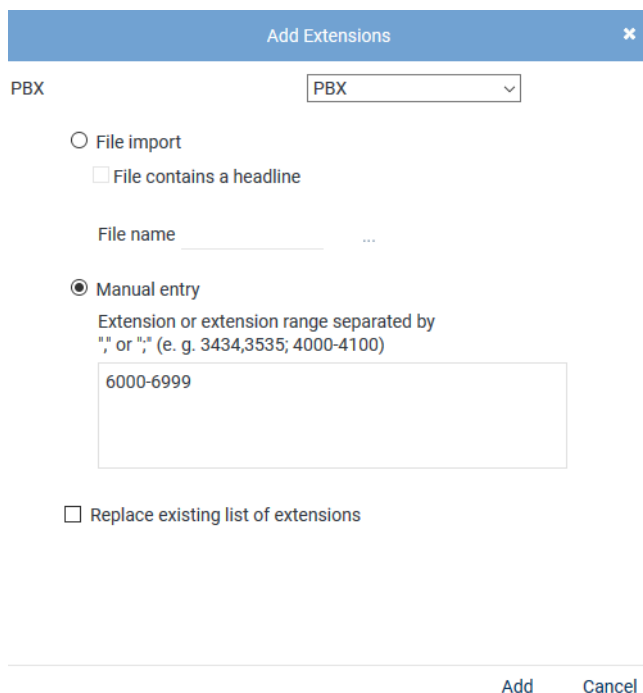


Fig. 248: Tenants - main view - tab Extensions

Add extensions

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



The 'Add Extensions' dialog box has a 'PBX' dropdown menu set to 'PBX'. It offers two options: 'File import' (with a sub-option 'File contains a headline') and 'Manual entry' (selected). The 'Manual entry' section includes a text input field containing '6000-6999' and a checkbox for 'Replace existing list of extensions'. At the bottom are 'Add' and 'Cancel' buttons.

Fig. 249: Assign extensions to tenants

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

File import	<p>Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported:</p> <ul style="list-style-type: none"> • ZIP • TXT
--------------------	---

- CSV

NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.



File contains a headline

Activate this option so that this structured is recognized correctly when importing the file.

The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.

File name

To import the file, proceed as follows:

- Click on the button  behind the field *File name*.
- Click on the button *Choose File*.
- Select the respective file in the Explorer and click on the button *Open*.
- Click on the button  *Upload File*.

Manual entry

Select this option to enter extensions or extension ranges manually.

To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100.

Enter country codes as number ranges as follows:

+4984496800--+4984496810

NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

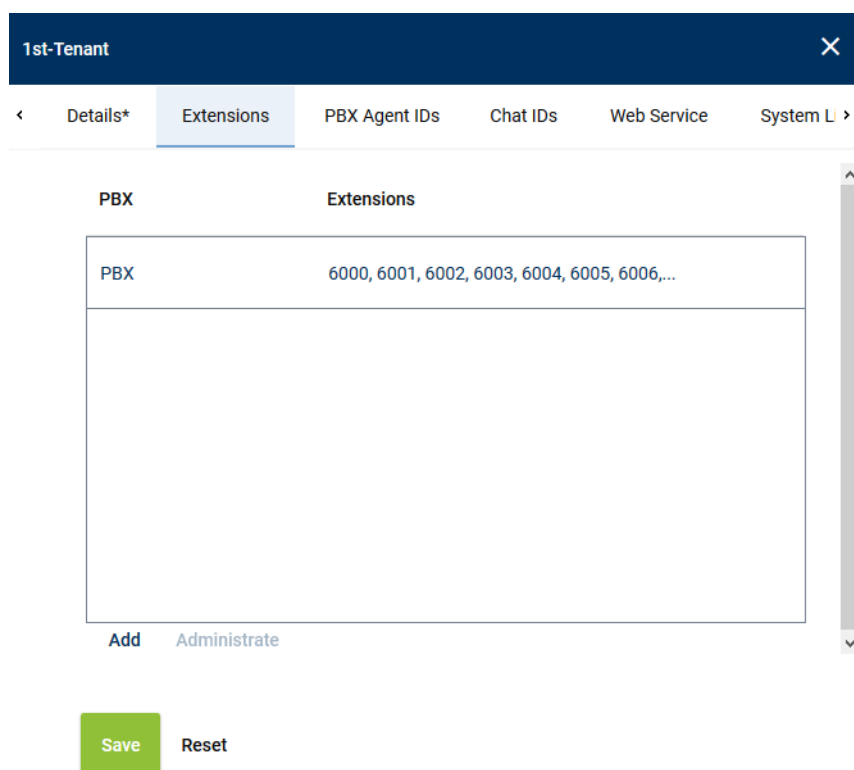
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

- Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
- 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*.
- The configured extensions now appear in the detail view.
- Click on the button *Save* in the detail view to save the entries.

Remove extensions

- 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. 250: Remove extensions

- 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.



Administrate Extensions

6993
6994
6995
6996
6997
6998
6999

Remove Cancel

Fig. 251: Select extensions

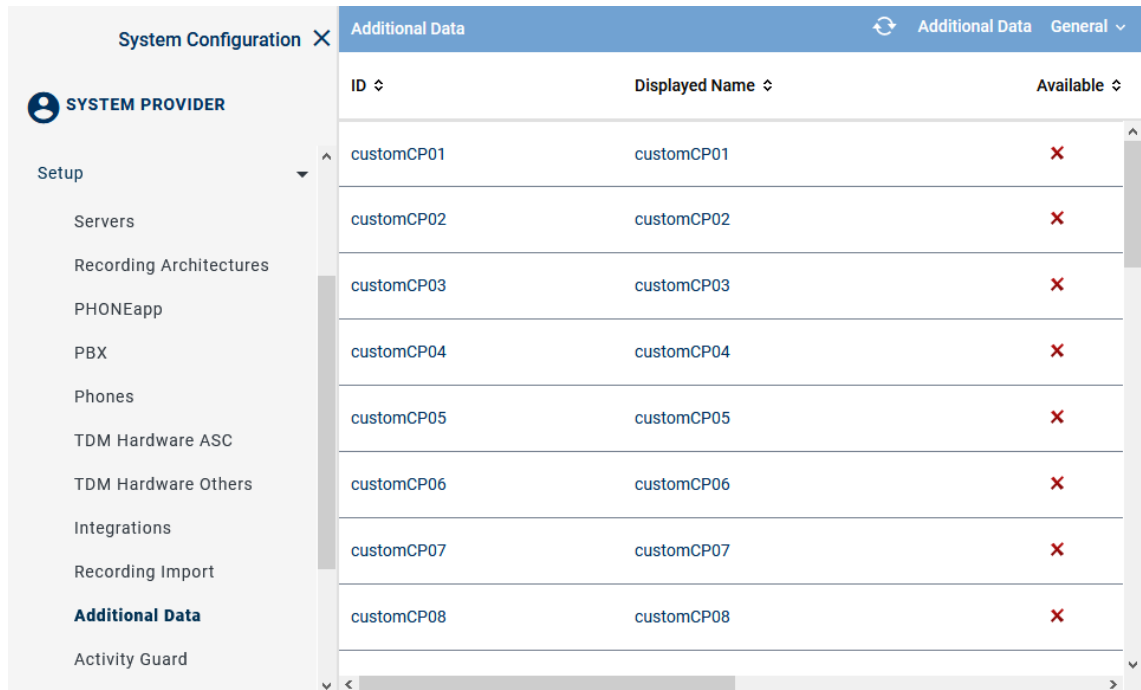
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

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.

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



ID	Displayed Name	Available
customCP01	customCP01	X
customCP02	customCP02	X
customCP03	customCP03	X
customCP04	customCP04	X
customCP05	customCP05	X
customCP06	customCP06	X
customCP07	customCP07	X
customCP08	customCP08	X

Fig. 252: 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. 253: 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"/>

Save
Reset

Fig. 254: 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:

System Configuration

SYSTEM PROVIDER

Setup

Servers

Recording Architectures

PHONEapp

PBX

Phones

TDM Hardware ASC

TDM Hardware Others

Integrations

Recording Import

Additional Data

Activity Guard

Powered by

ASC Technologies AG

v6.9.9-9.9

+

×

▶

◻

Integration



General

Name	Type	Active	Status
<div><div></div>SIP active</div>	SIP active	<div>✗</div>	<div><div></div></div>
<div><div></div>Cisco active</div>	Cisco UCM active	<div>✗</div>	<div><div></div></div>
<div><div></div>Avaya active</div>	Avaya CM active	<div>✗</div>	<div><div></div></div>
<div><div></div>MIVB</div>	Mitel MiVoice Business active	<div>✗</div>	<div><div></div></div>

1

Fig. 255: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.


+ × ⏮ ⏭	Integration ▾	General ▾
---------	---------------	-----------

Fig. 256: Toolbar Integrations module

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

<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.

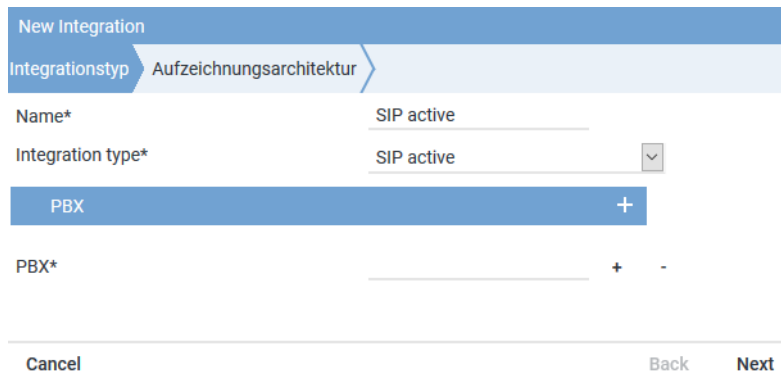



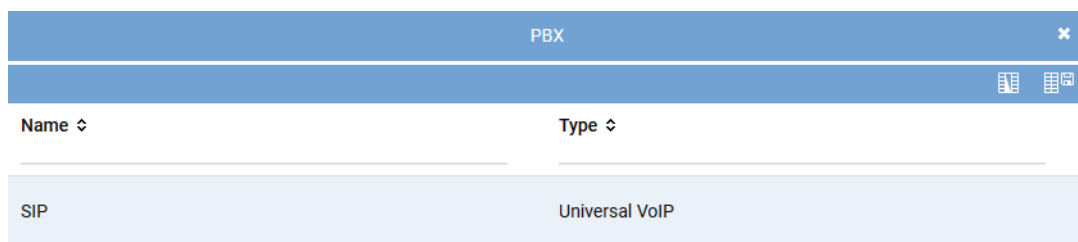
Fig. 257: Create integration type

- 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 67: 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. 258: Select PBX

- Select the respective *PBX* from the list of available PBXs.

- Click on the button *Add*.

Assign recording architecture for Multi-Server Recording

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

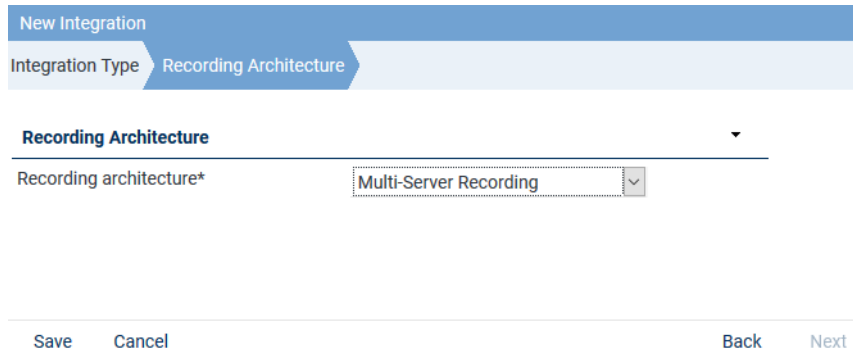


Fig. 259: Assign recording architecture - Multi-Server Recording


- 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.

- Click on the button *Save*.
⇒ The integration now appears in the main view.

Configuration steps

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

Fig. 260: 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.

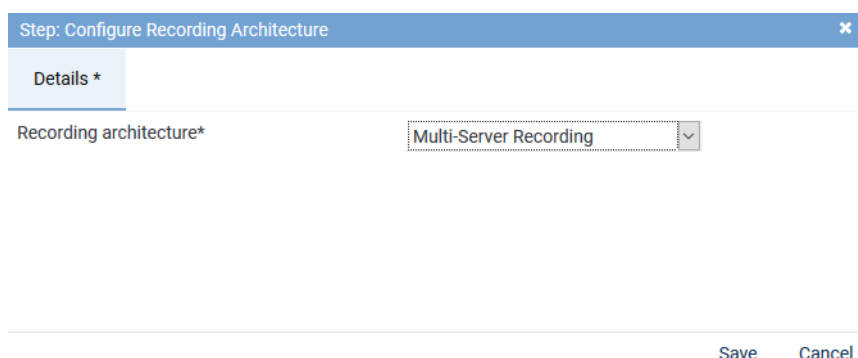



Fig. 261: Configuration step - Configure Recording Architecture

- 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.

Global recording settings for Multi-Server Recording

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

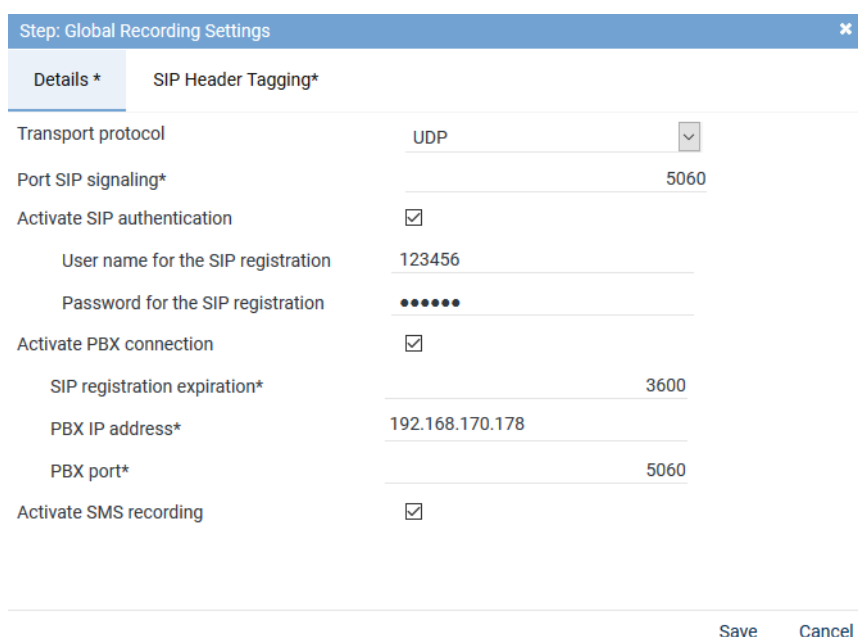


Fig. 262: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted

Parameter	Value/Description
<i>Port SIP signaling</i>	<p>Enter the port for the SIP signaling, where the recording server is expecting the signaling.</p> <p>Default value for UDP and TCP is 5060.</p> <p>Default value with TLS encryption is 5061.</p> <p>NOTICE! If you would like to use several integrations, you have to configure a separate SIP port for each integration.</p> <p>NOTICE! If you would like to use a media streamer for replay, configure another SIP port for it, too. In case of communication issues with the media streamer, this could otherwise affect the recording.</p>
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password of the SIP registration</i>	Enter the password, if an authentication for the SIP registration is used.
<i>Activate PBX connection</i>	Activate this check box if the recording server is supposed to register itself on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration runs out, e. g. 3600.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port on which the SIP signaling is sent to the PBX . The default value is 5060.
<i>Activate SMS recording</i>	Activate the check box if you would like to use SMS recording.

Tab. 68: Global recording settings

Tab SIP Header Tagging

- If you would like to configure the SIP header tagging, click on the tab *SIP Header Tagging*.

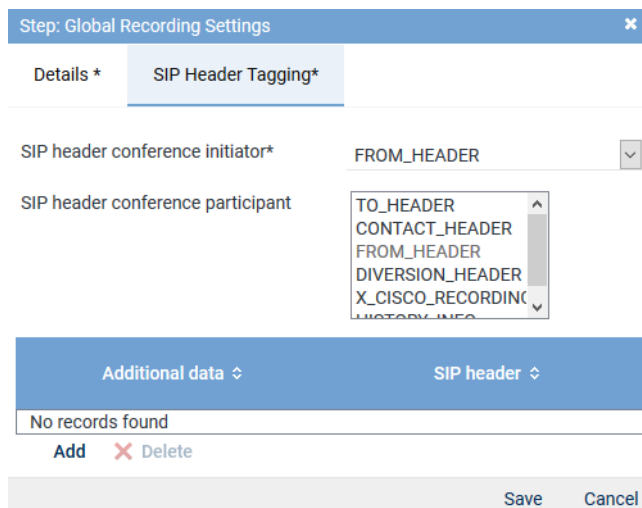


Fig. 263: Tab SIP Header Tagging Configure sources

- Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.

Parameter	Value/Description
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

Tab. 69: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down. To deselect an entry, click on it again without releasing the [Ctrl] key.

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

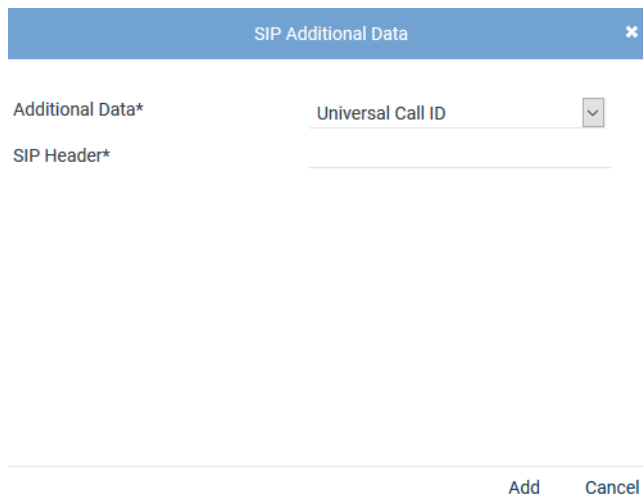


Fig. 264: SIP Additional Data



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

- Enter the following parameters:

Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.


Tab. 70: Configure SIP conversation parameters

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

Configure recording server for Multi-Server Recording

When using several recording servers, you must configure the port range for each recording server separately. The range may be the same for all recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

1. In the main view in the line *Configure recording servers* click on the button  (*Edit configuration step*).

⇒ The window *Step: Configure Recording Servers* appears.

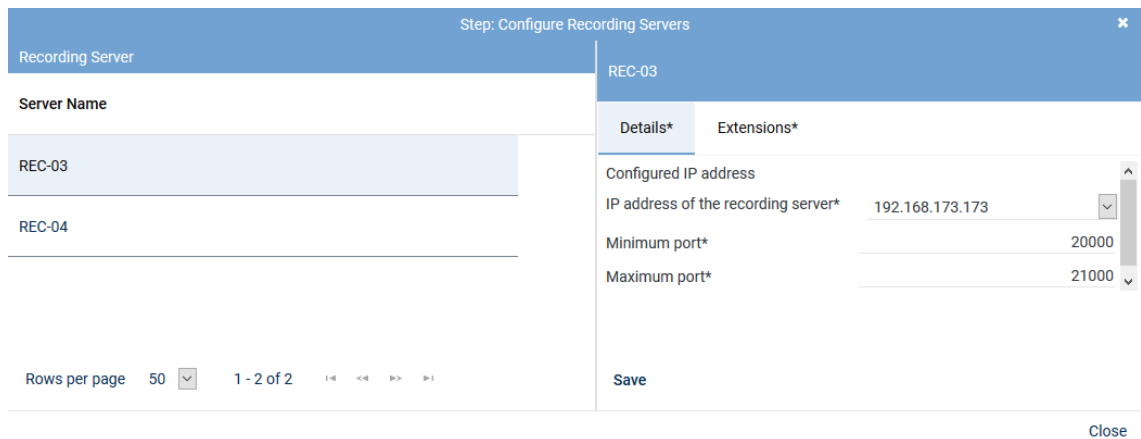


Fig. 265: Configuration step - Configure recording servers

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

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

Tab. 71: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

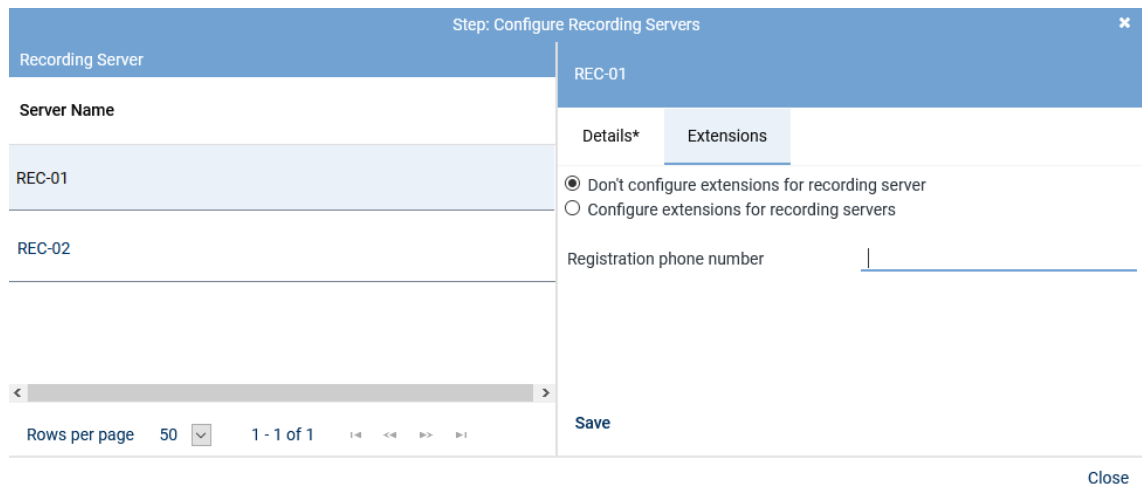


Fig. 266: Recording server - Configure extension for SIP trunk



Ask your provider whether registering 2 servers in parallel mode is supported. To do so, it must be possible to assign a [SIP](#) trunk phone number to 2 different IP addresses at the same time.

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a [SIP](#) trunk phone number instead.



If you do not define a phone number for the [SIP](#) trunk of the recording server, all incoming [SIP](#) connections are accepted without being examined.

Registration phone number Enter a registration phone number for the [SIP](#) trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the [SIP](#) trunk, see [chapter "Global recording settings for All-in-one Parallel Recording", p. 169](#).

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

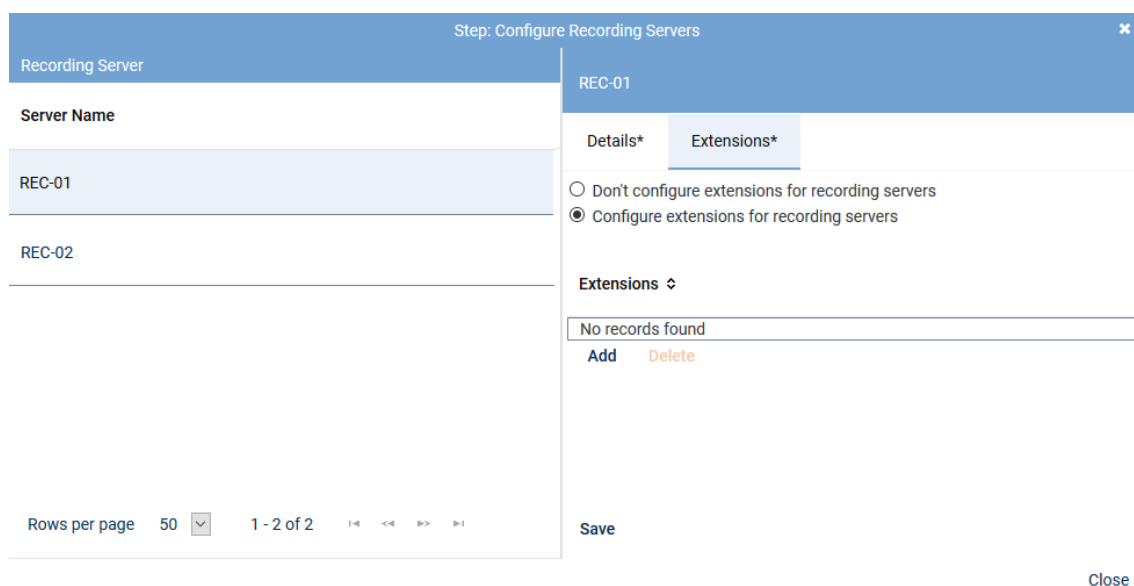


Fig. 267: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

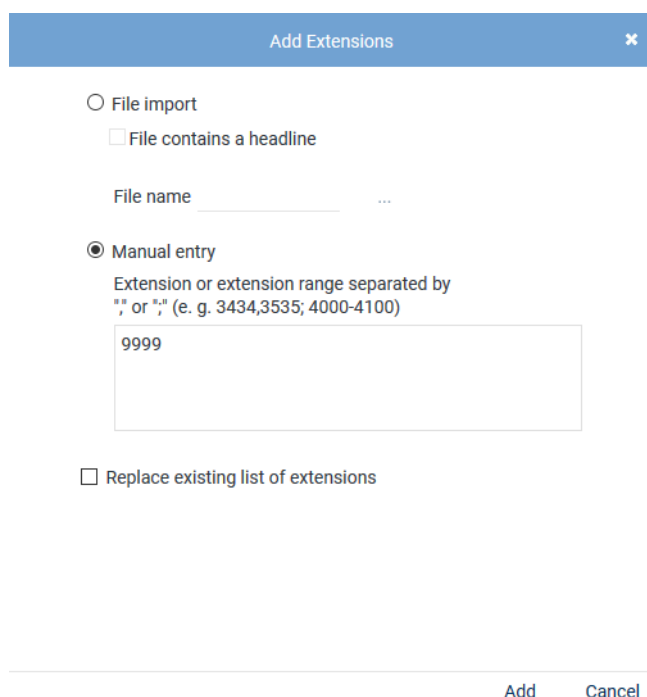


Fig. 268: Add extensions

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

6. The configured extensions now appear in the detail view.

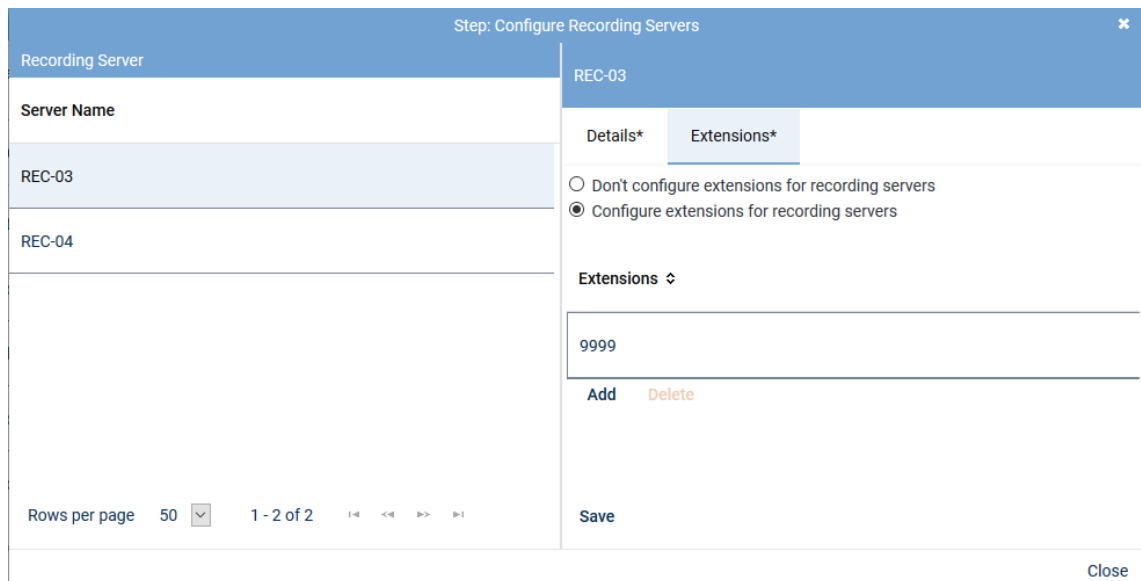


Fig. 269: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the [SIP](#) registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the [SIP](#) end-points again.

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

Configure add-on



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

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



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



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

Configure add-on for Sparkassen FI ISP (optional)

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



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

The integration runs in combination with a PBX and the recording server. The service **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

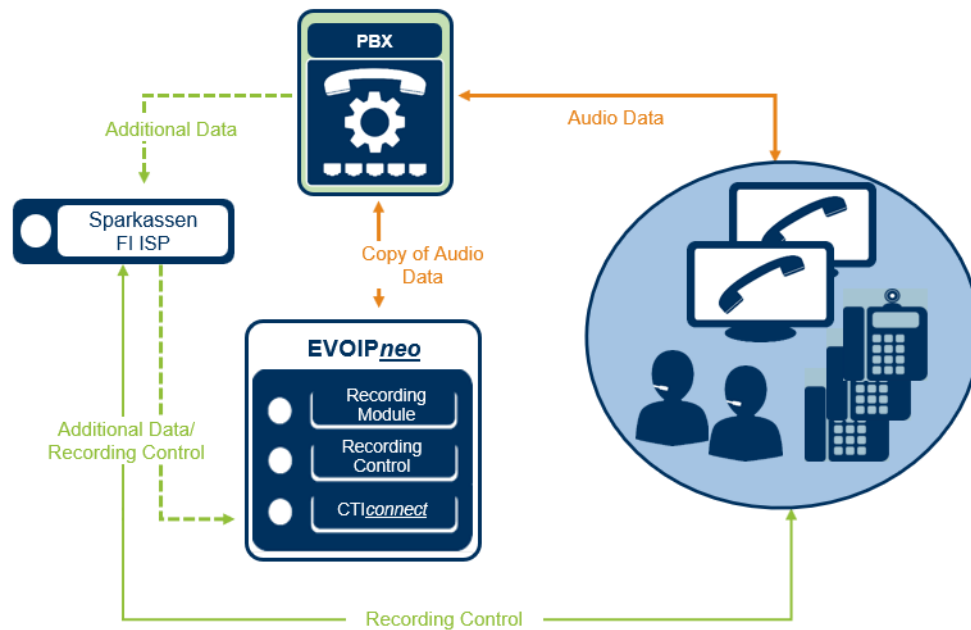



Fig. 270: Overview of Sparkassen FI ISP

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. 271: 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 [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

Parameter	Value/Description
<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 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.

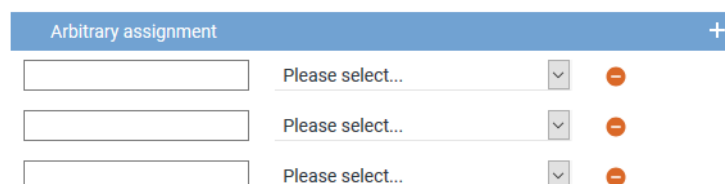



Fig. 272: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)", p. 384](#).

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. 273: 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:

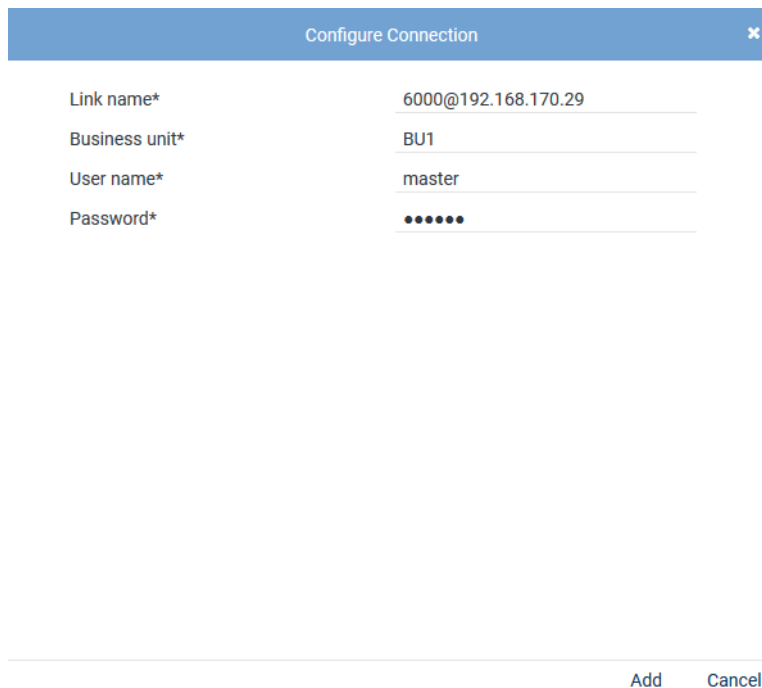


Fig. 274: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<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.

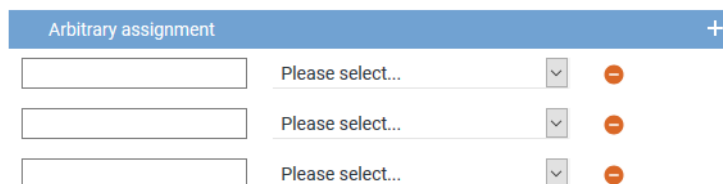




Fig. 275: Arbitrary assignment of the additional data

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 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

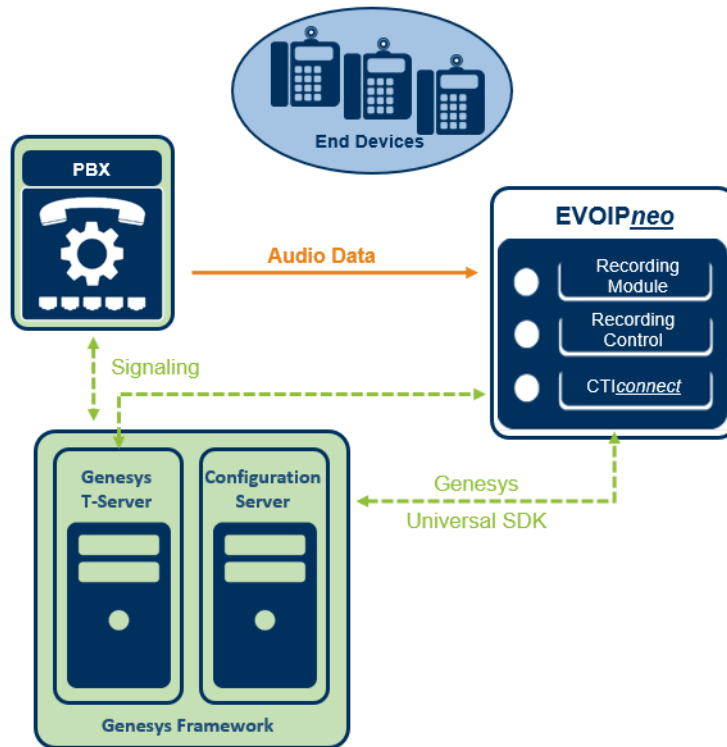


Fig. 276: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

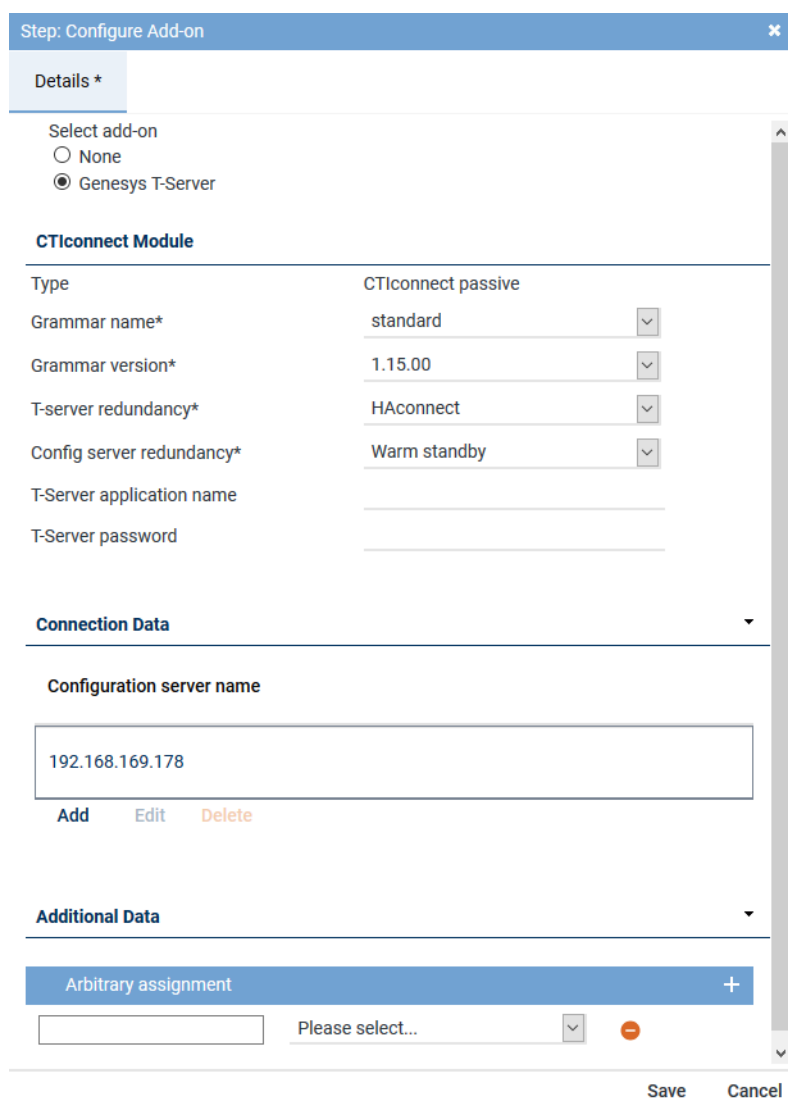
Adjust configuration file for Genesys add-on

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. 277: 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.

Parameter	Value/Description
	<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. 76: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

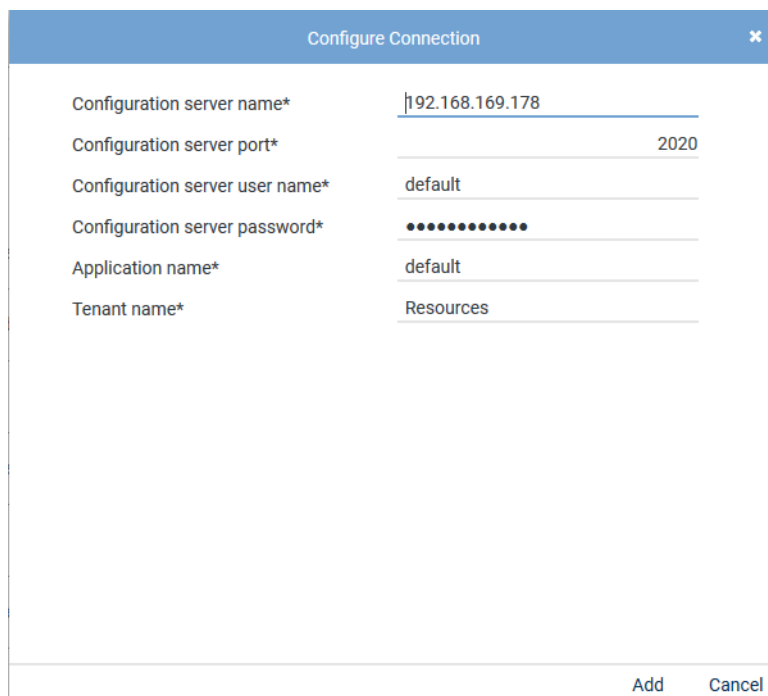


Fig. 278: Configure connection data

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.

Parameter	Value/Description
<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. 77: 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.

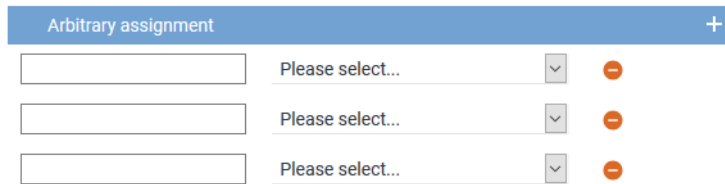



Fig. 279: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

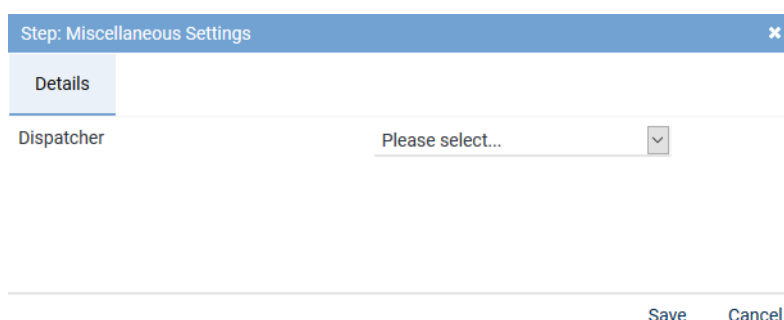


Fig. 280: Configure miscellaneous settings

- 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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 281: 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 active	SIP active		

Fig. 282: 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 active	SIP active		

Fig. 283: 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:

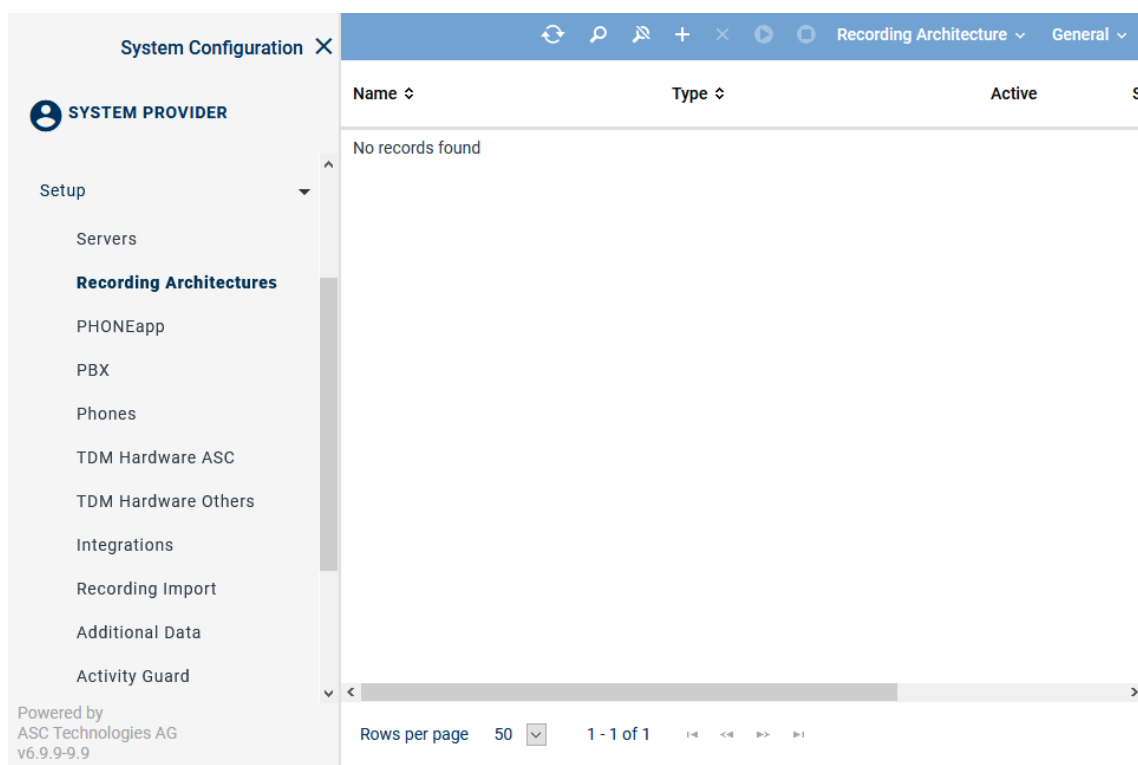




Fig. 284: Recording architectures - main view

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. 285: 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.

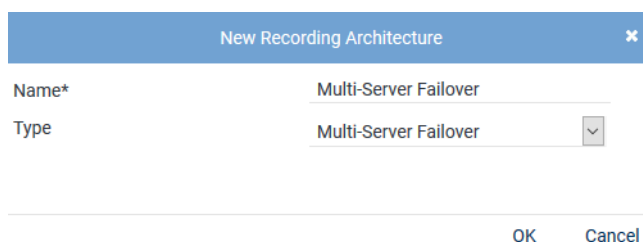


Fig. 286: Create recording architecture - Multi-Server Failover

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

- 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.
- Click on the button *OK*.
⇒ Your entries now appear in the detail view.

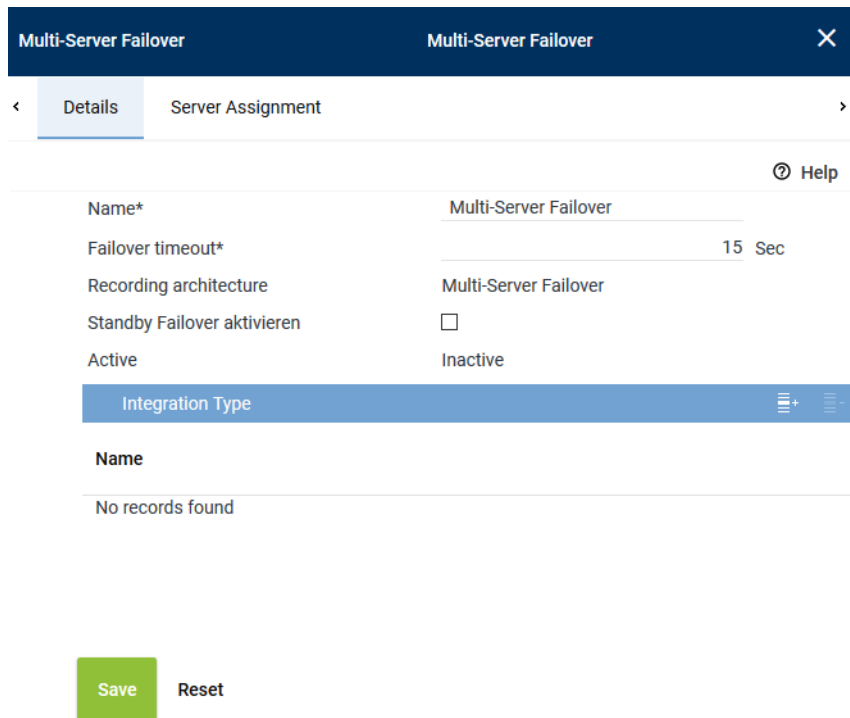


Fig. 287: Recording architecture - tab Details - Multi-Server Failover

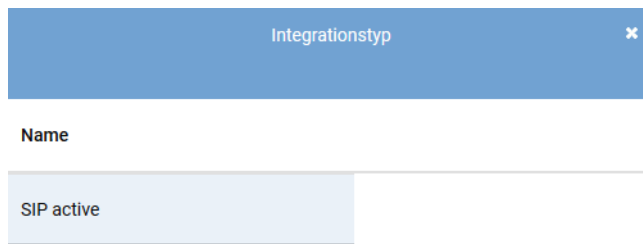
As standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For further information about the configuration of failover architectures, see [chapter "Standby management for failover architectures", p. 374](#).

<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.



Hinzufügen Abbrechen

Fig. 288: Select integration type



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



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

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

Assign server for Multi-Server Failover

1. Click on the tab *Server Assignment* to assign the recording components to the corresponding recording servers for the *Multi-Server Failover* recording architecture.

Group field Recording Control and CTIconnect

In this group field, you can configure recording control. You can configure two different servers 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. 289: 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. 290: 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. 291: Add Recording Server




2. As described in the previous steps, go to the entry field *Primary server* and click on the icon  to select the primary server on which the recording is supposed to run.
3. In the entry field *Standby server*, click on the icon  to select the standby server which is supposed to take over recording in case of an error.
4. Select the recording type you would like to use for these servers by activating the check box.



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



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

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon  (*Activate*) in the 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 Failover	Multi-Server Failover	✓	✗

Fig. 292: 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 [chapter "Standby management for failover architectures", p. 374](#).



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. 293: 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. 294: 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 <i>neo</i> 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. 258 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<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.

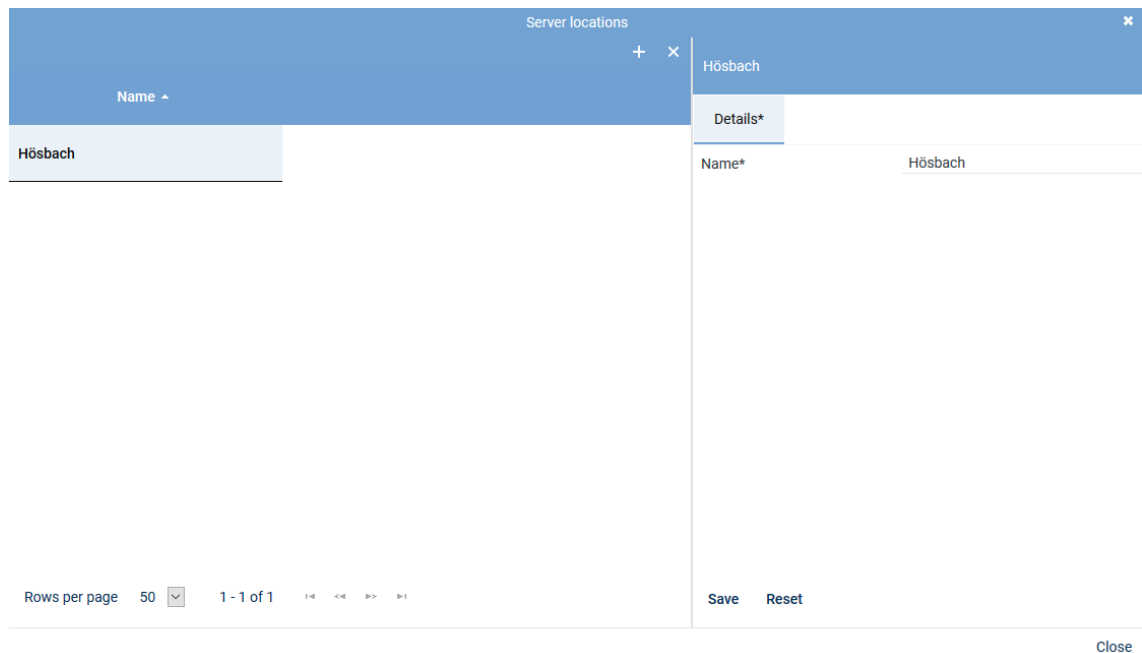



Fig. 295: Add server locations

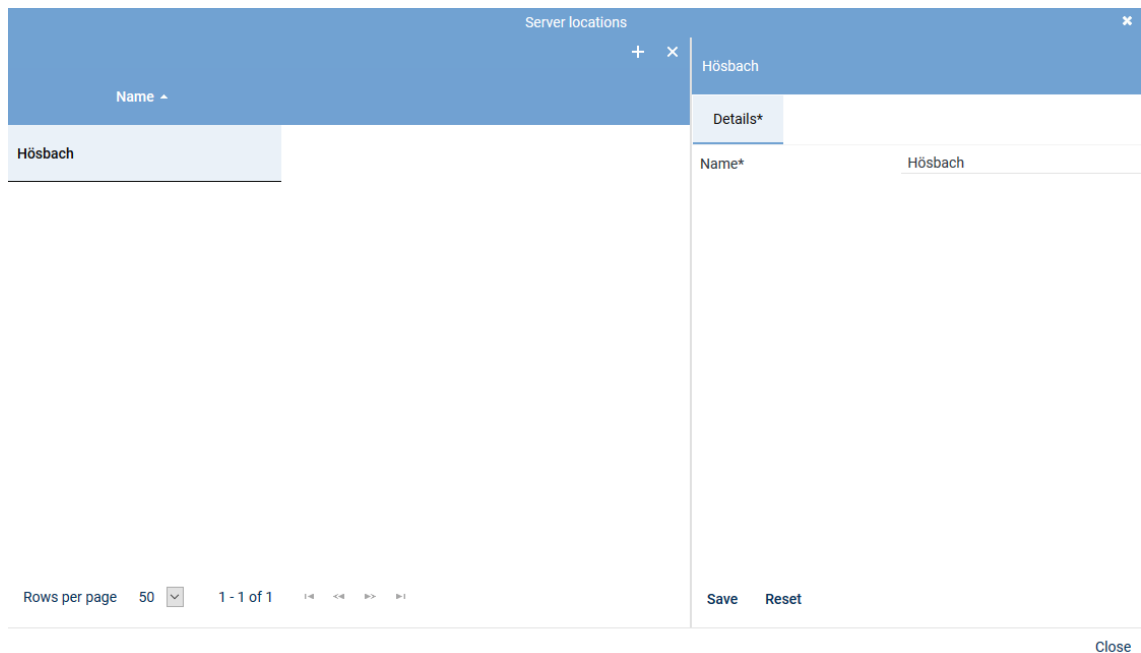
- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.
- To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
- To add further locations, repeat the last 3 steps.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



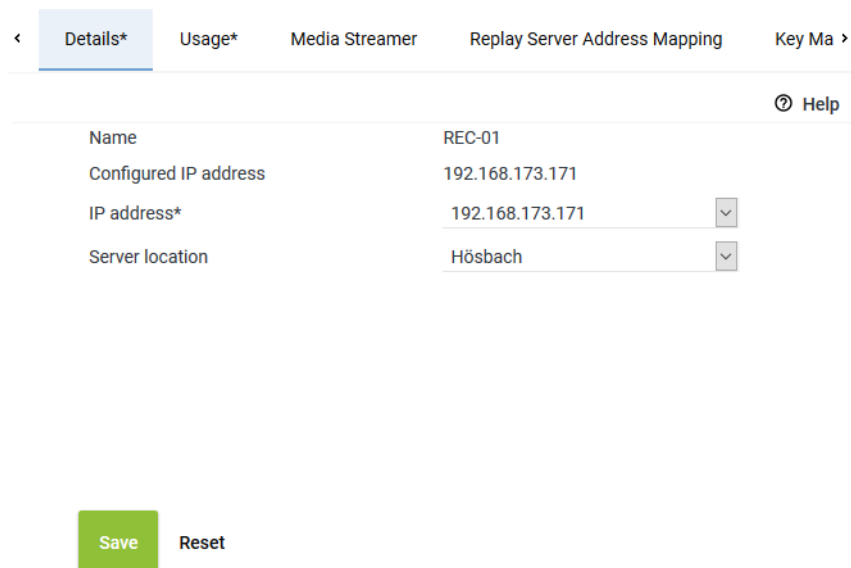
The screenshot shows a window titled "Server locations" with a close button (x) in the top right. Inside, there's a table with one row containing "Hörsbach". To the right of the table is a "Details*" tab. Below the table, there's a pagination bar showing "Rows per page 50" and "1 - 1 of 1". At the bottom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

Fig. 296: 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 area contains a form 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. 297: 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.

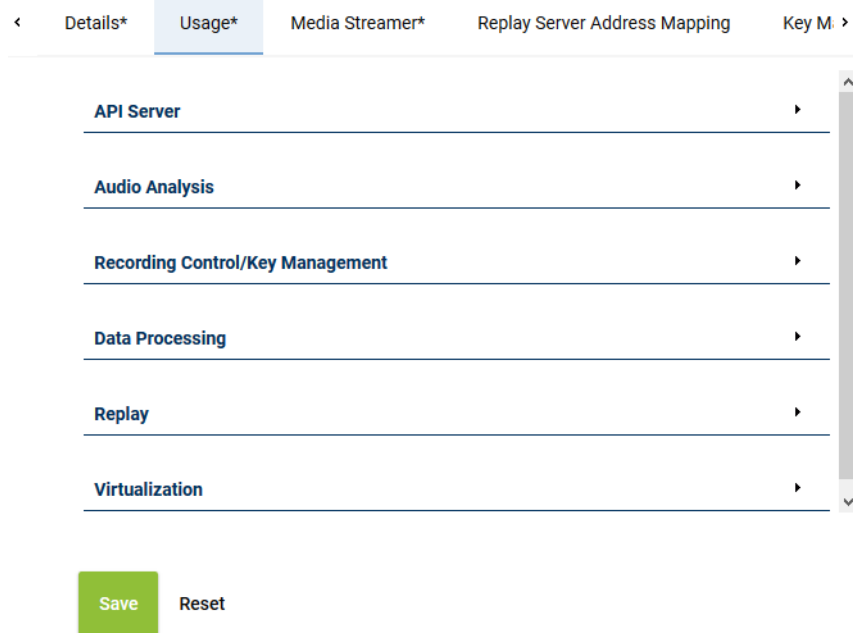


Fig. 298: Servers - tab usage

Group field API Server

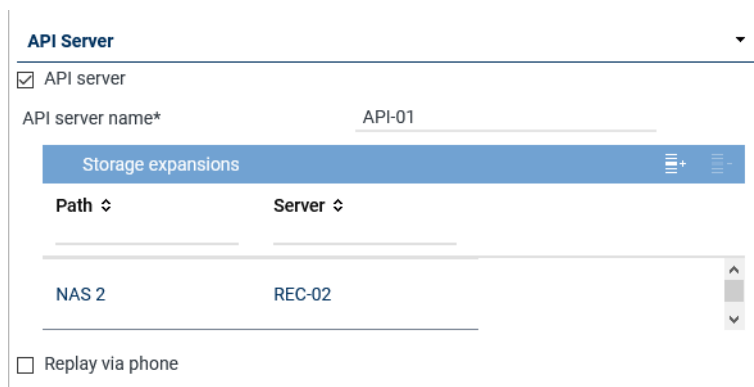




Fig. 299: Group field API Server

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.

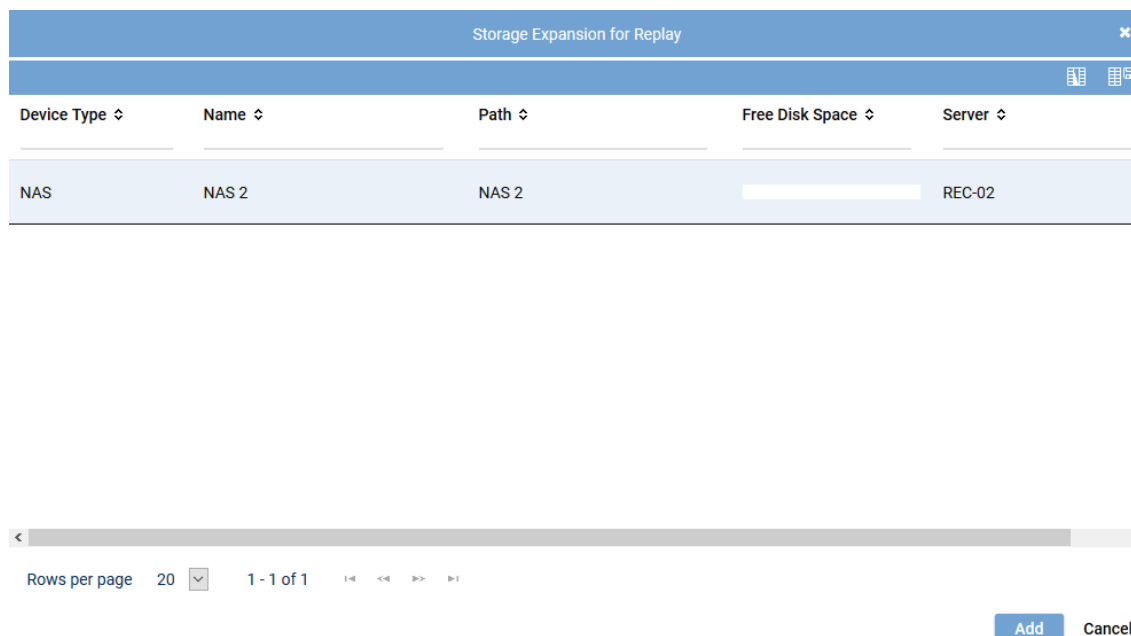
Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

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. 272.</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. 263. • 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 <i>neo</i> 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 <i>PBX</i>, see chapter "Tab Media Streamer", p. 270. To be able to do so, at least 1 <i>PBX</i> 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. 300: 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

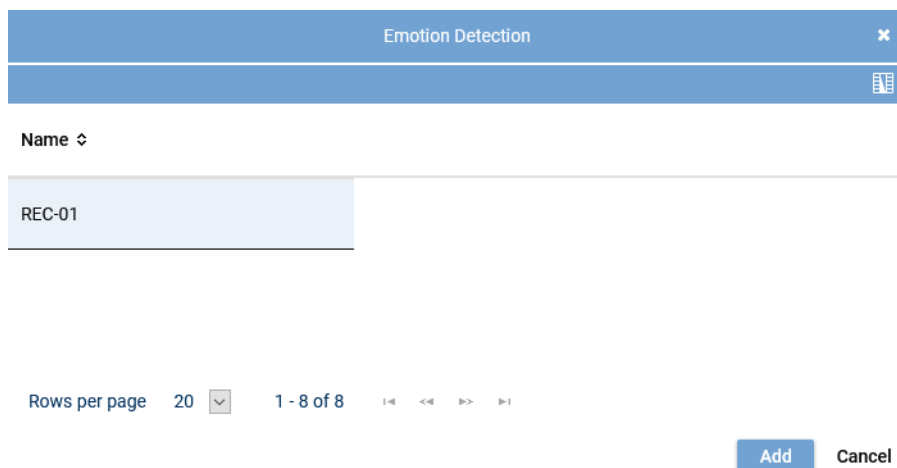
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 301: 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. 78: Configure audio analysis



Emotion Detection

Name ↕

REC-01

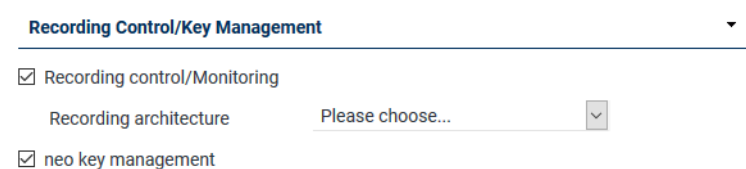
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 302: 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/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 303: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 79: 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	IP Address
No records found	

☐ Archiving



☒ Export





Replay server Please choose... ▼

☒ Import

Recording architecture All-in-one Basic ▼

Fig. 304: 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. 267. 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. 267. 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 <i>neo</i> to <i>neo</i>, 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. 80: 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

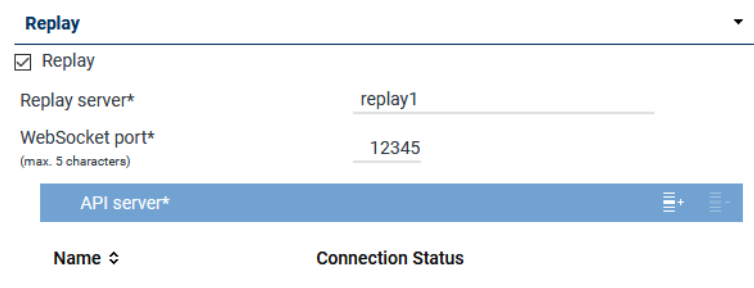
Fig. 305: Select server



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. 306: 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. 268. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 81: 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. 307: Select server



Only those servers are available on which the **API** service has been installed and activated.
See [chapter "Group field API Server", p. 261](#).

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. 308: 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. 82: 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. 309: 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. 276.</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 <i>8000</i>.</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> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</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: <i>5062</i></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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<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 <i>5060</i>.</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. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.



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

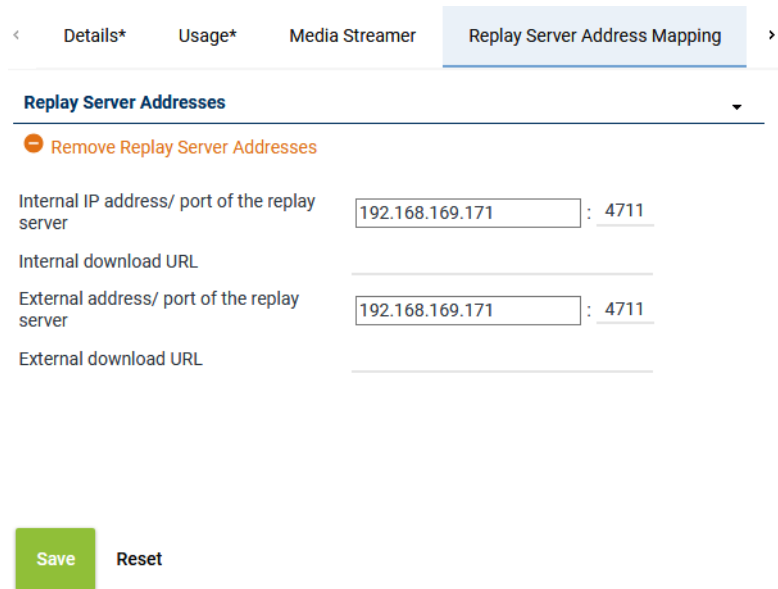


Fig. 310: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

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



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

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



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

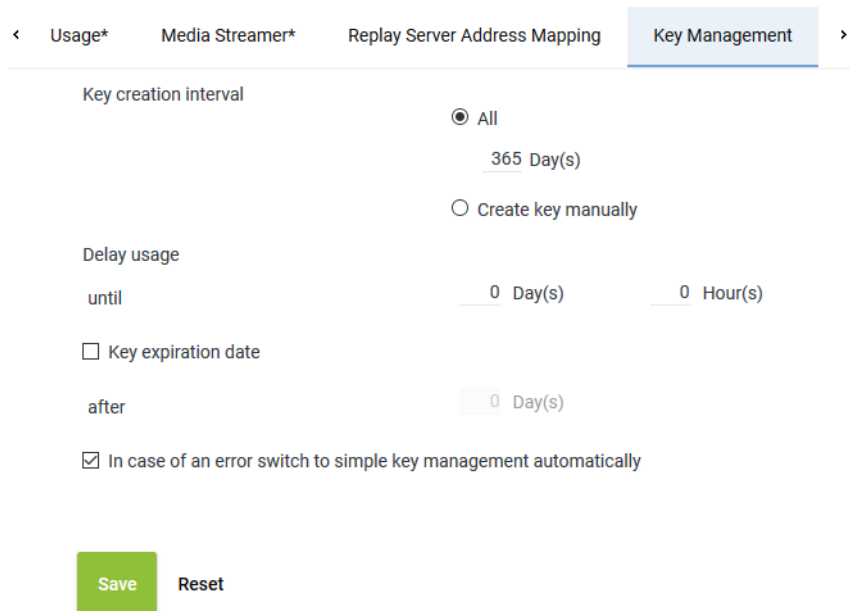


For information about the configuration refer to the administration manual for tenants *User management tenant*.

Tab Key Management

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

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



< 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. 311: 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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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*

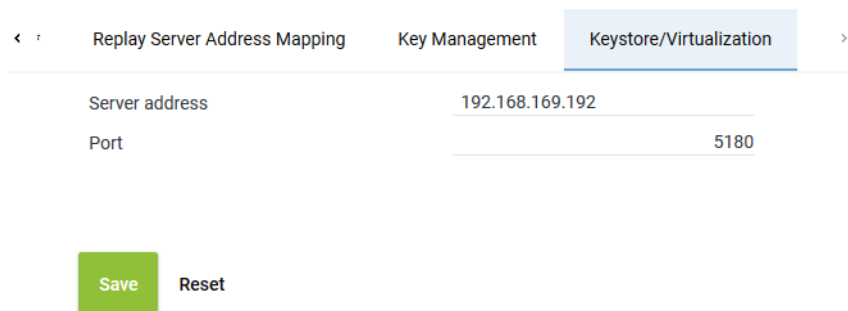
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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. 312: 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:

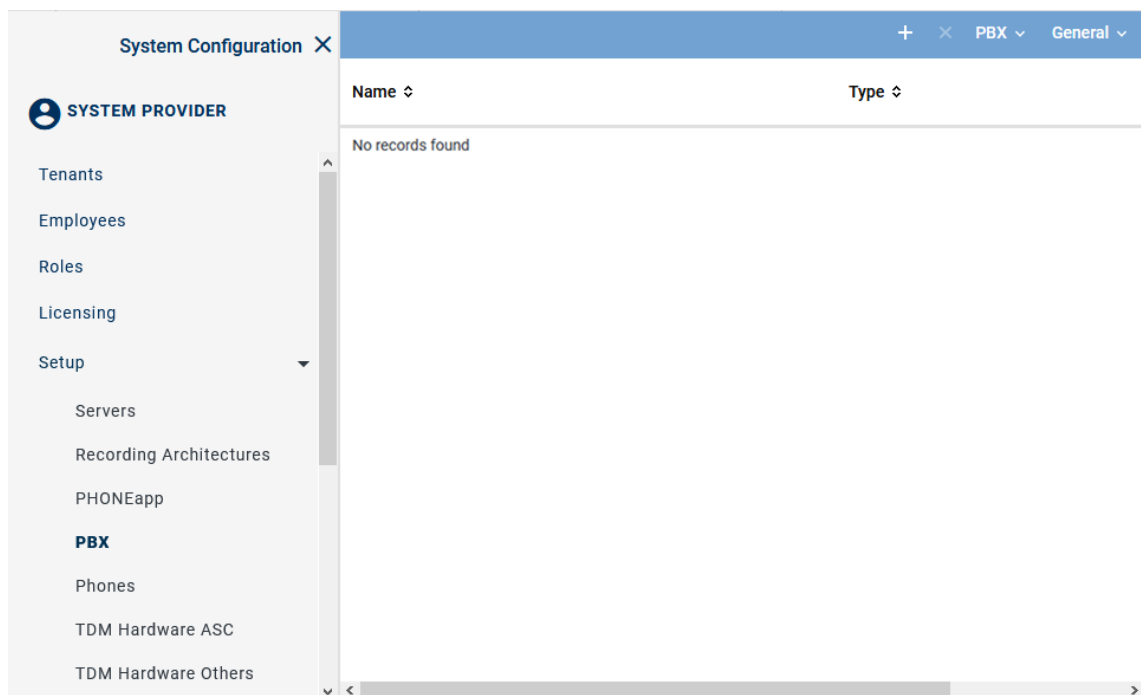


Fig. 313: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

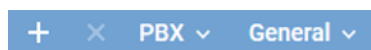




Fig. 314: Toolbar PBX module


	<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. 315: 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. 83: Create PBX

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

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

Tab. 84: PBX parameters with complete phone number

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

7.1.2.5.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

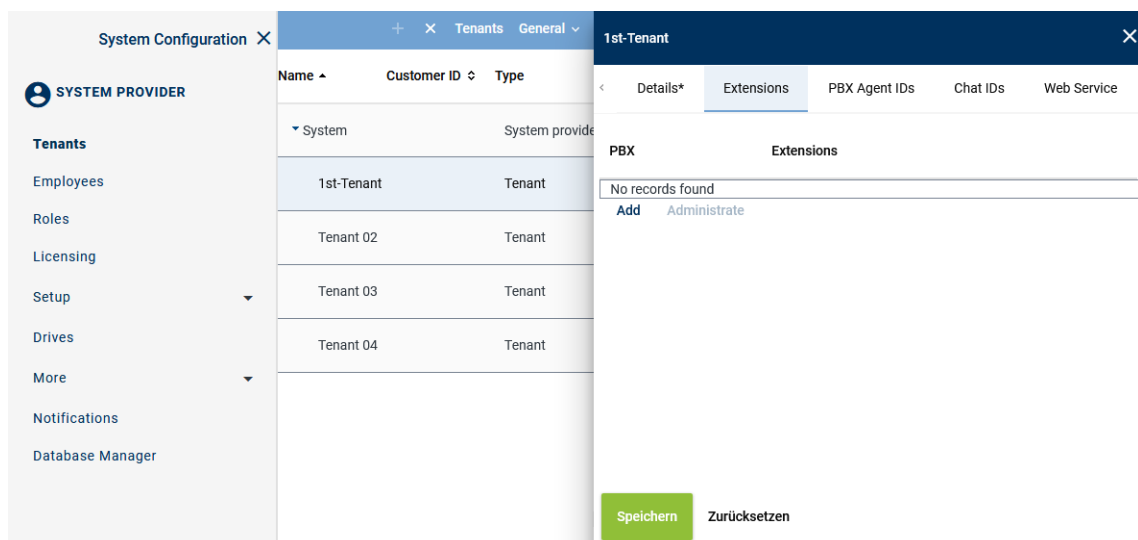


Fig. 316: Tenants - main view - tab Extensions

Add extensions

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

⇒ The following window appears:

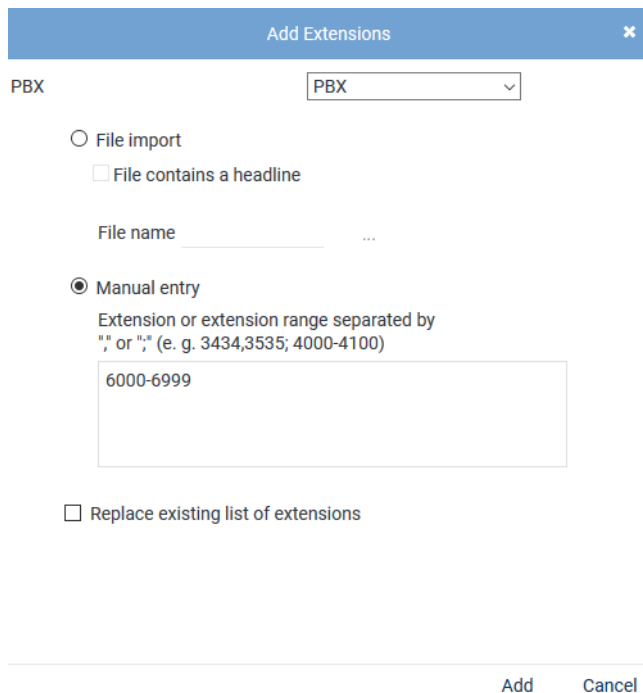




Fig. 317: Assign extensions to tenants

- 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"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <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.

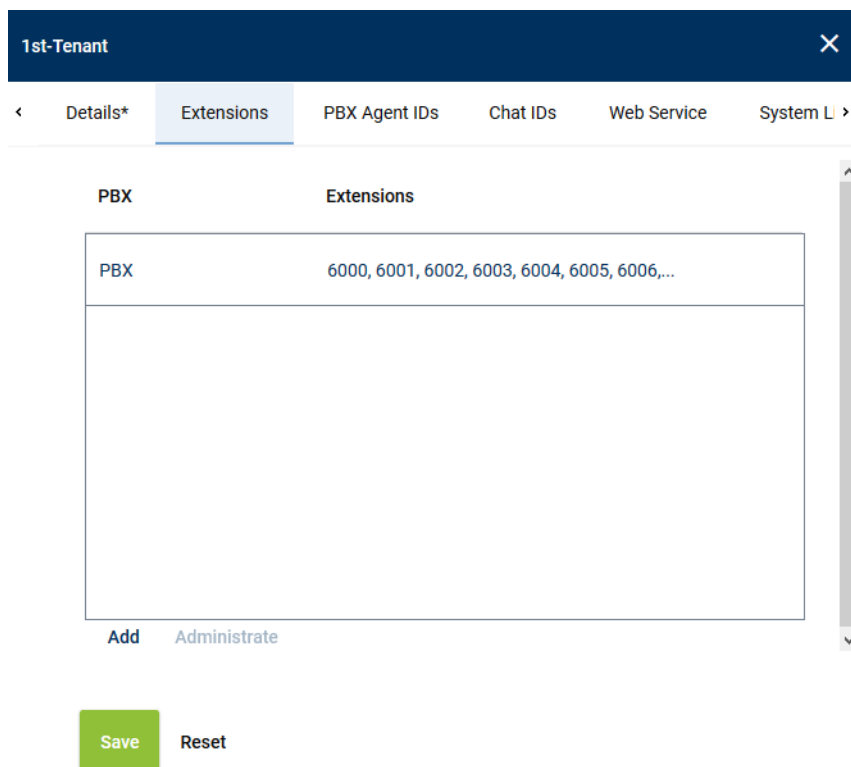
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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.



The screenshot shows a configuration window for '1st-Tenant'. It has a navigation bar with tabs: 'Details*', 'Extensions' (selected), 'PBX Agent IDs', 'Chat IDs', 'Web Service', and 'System L'. Below the tabs is a table with two columns: 'PBX' and 'Extensions'. The 'PBX' column has one entry 'PBX'. The 'Extensions' column has one entry '6000, 6001, 6002, 6003, 6004, 6005, 6006,...'. Below the table are two buttons: 'Add' and 'Administrate'. At the bottom of the window are two buttons: 'Save' and 'Reset'.

Fig. 318: 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. 319: 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.

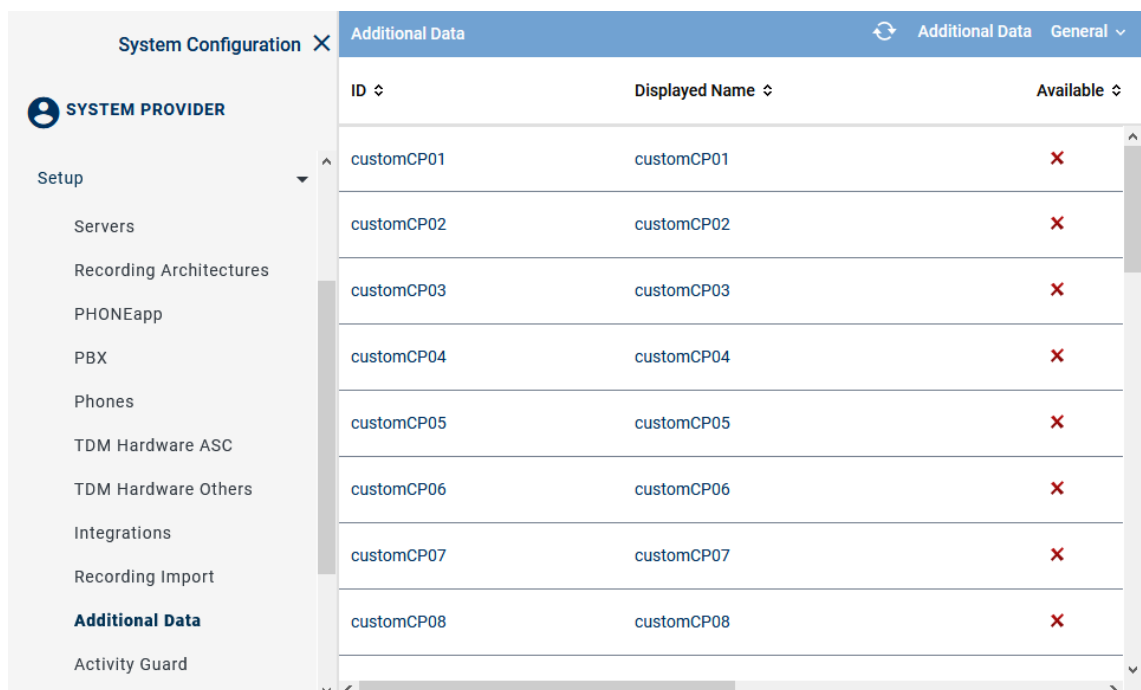


Fig. 320: Additional Data module main view

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. 321: 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. 322: Additional data - configure availability

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



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



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

7.1.2.5.6 Create integration for Multi-Server Failover

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

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

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

1. In the navigation bar, select the menu item *Setup > Integrations*.

⇒ The following window appears:

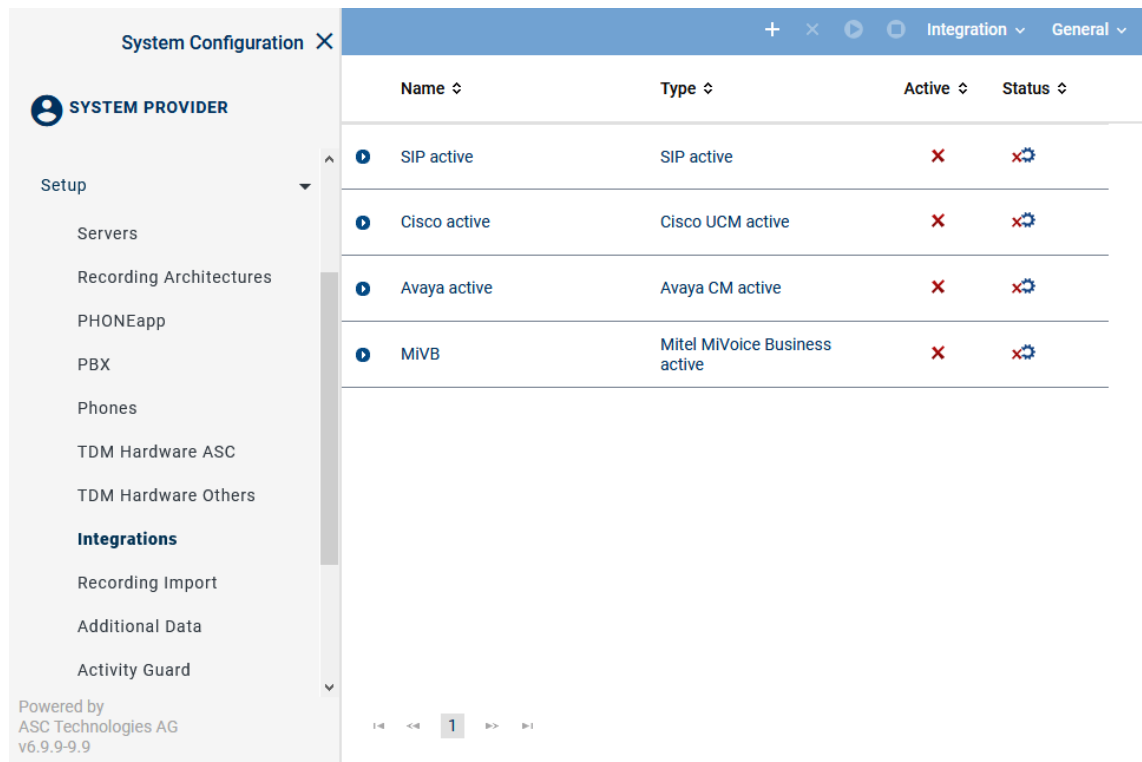




Fig. 323: Integrations - main view

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. 324: 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.

Import grammar

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

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

1. To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.

⇒ The window *Upload File* appears.

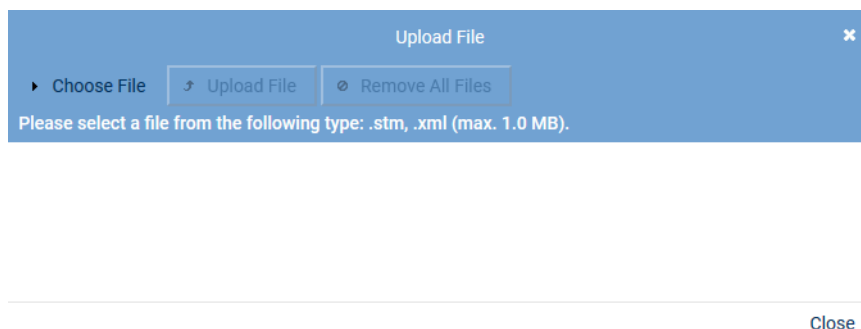


Fig. 325: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.

⇒ The selected file appears in the window *Upload File*.

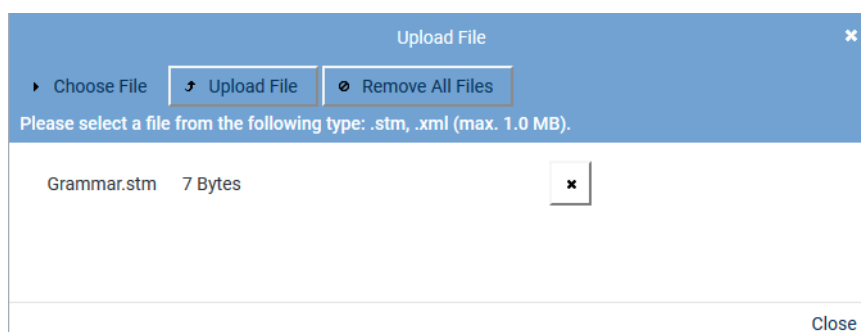




Fig. 326: Upload grammar

5. To remove a selected file from the list, click on the button  (*Remove file*) next to the respective file.
To upload the file, click on the button *Upload File*.
- ⇒ The window closes and a notification appears in the main view that the file has been uploaded successfully.

Assign integration type

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

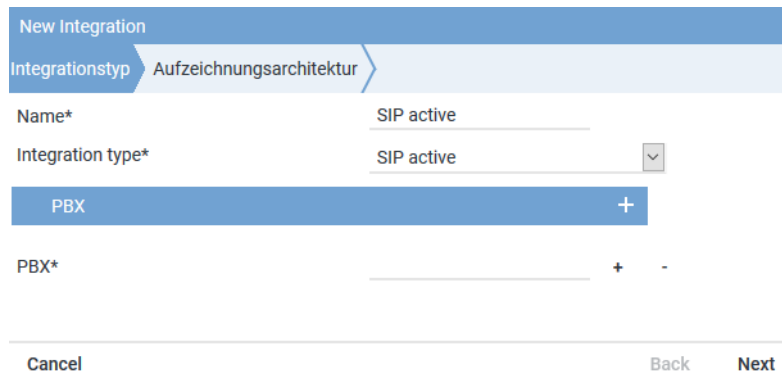



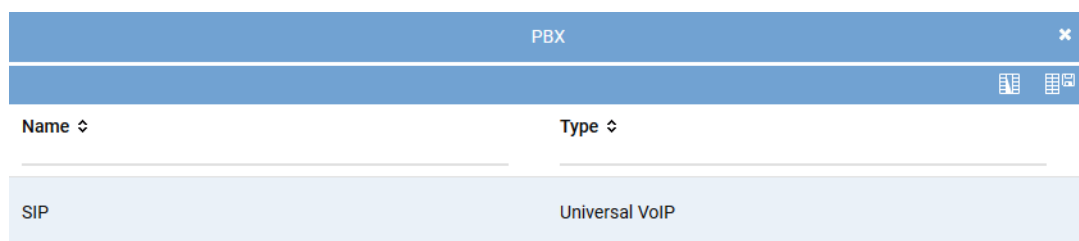
Fig. 327: Create integration type

2. 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 85: Create integration type

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



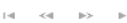
Rows per page 20  1 - 1 of 1 

Fig. 328: Select PBX

4. Select the respective *PBX* from the list of available PBXs.

5. Click on the button *Add*.

Assign recording architecture for Multi-Server Failover

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

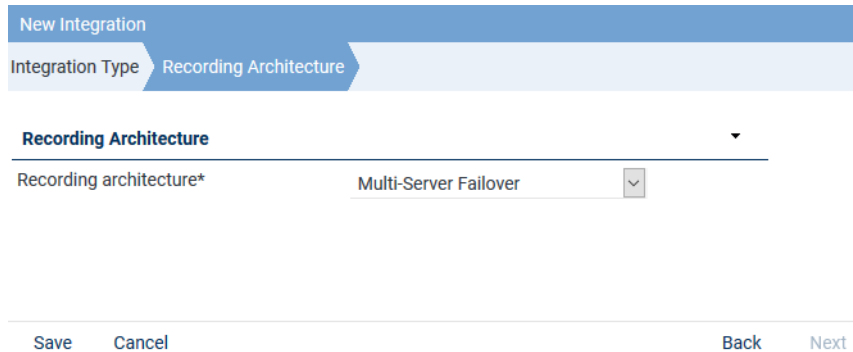


Fig. 329: Assign recording architecture - Multi-Server Failover


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

Fig. 330: Configuration steps of the integration

Configure recording architecture

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

1. Click on the button  (*Edit configuration step*) in the line *Configure recording architecture* in the main view to show the configuration.

- ⇒ In the detail view, the configuration step appears with the information of the assigned recording architecture.

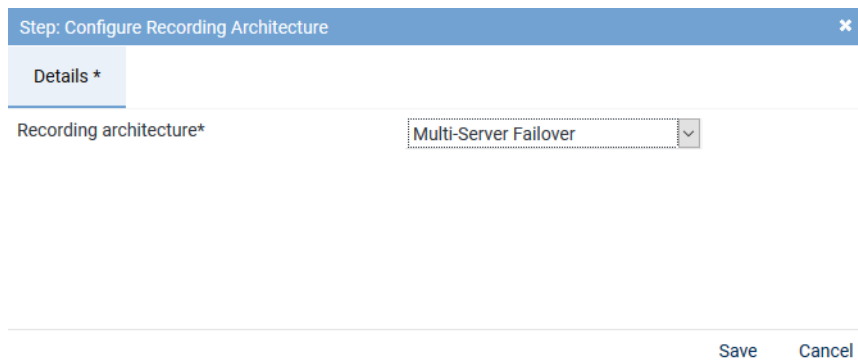


Fig. 331: Configuration step - Configure Recording Architecture

- 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.

Global recording settings for Multi-Server Failover


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



Fig. 332: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted

Parameter	Value/Description
<i>Port SIP signaling</i>	Enter the port for the SIP signaling, where the recording server is expecting the signaling. Default value for UDP and TCP is 5060. Default value with TLS encryption is 5061. NOTICE! If you would like to use several integrations, you have to configure a separate SIP port for each integration. NOTICE! If you would like to use a media streamer for replay, configure another SIP port for it, too. In case of communication issues with the media streamer, this could otherwise affect the recording.
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password of the SIP registration</i>	Enter the password, if an authentication for the SIP registration is used.
<i>Activate PBX connection</i>	Activate this check box if the recording server is supposed to register itself on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration runs out, e. g. 3600.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port on which the SIP signaling is sent to the PBX . The default value is 5060.
<i>Activate SMS recording</i>	Activate the check box if you would like to use SMS recording.

Tab. 86: Global recording settings

Tab SIP Header Tagging

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

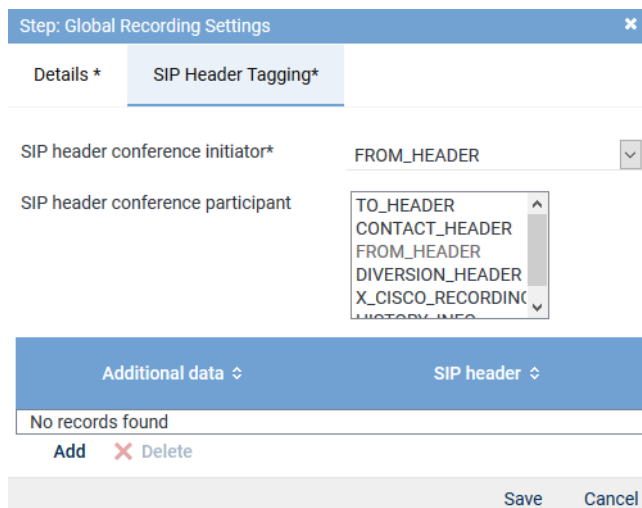


Fig. 333: Tab SIP Header Tagging Configure sources

2. Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.

Parameter	Value/Description
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

Tab. 87: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down. To deselect an entry, click on it again without releasing the [Ctrl] key.

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

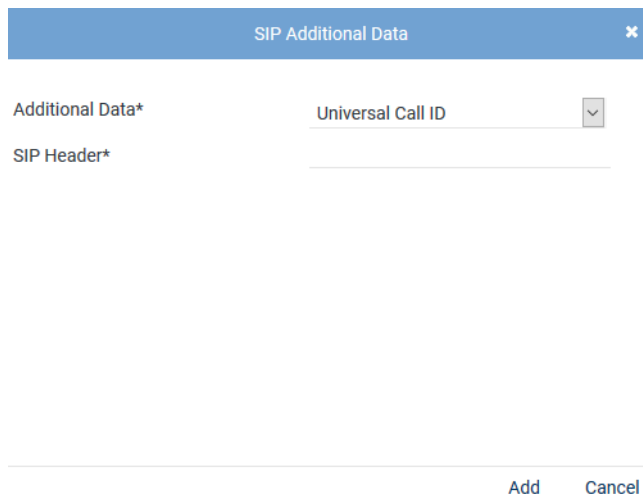


Fig. 334: SIP Additional Data



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

- Enter the following parameters:

Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.


Tab. 88: Configure SIP conversation parameters

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

Configure recording server for Multi-Server Failover

To guarantee that recording works properly when switching servers in case of failover with several servers, you must configure a port range for each recording server. The range may be the same for all recording servers. Make sure, though, that the port range lies within the range of ports activated in the firewall, refer to the installation manual Installation requirements in chapter Communication matrix.

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

1. In the main view in the line *Configure recording servers* click on the button  (*Edit configuration step*).

⇒ The window *Step: Configure Recording Servers* appears.

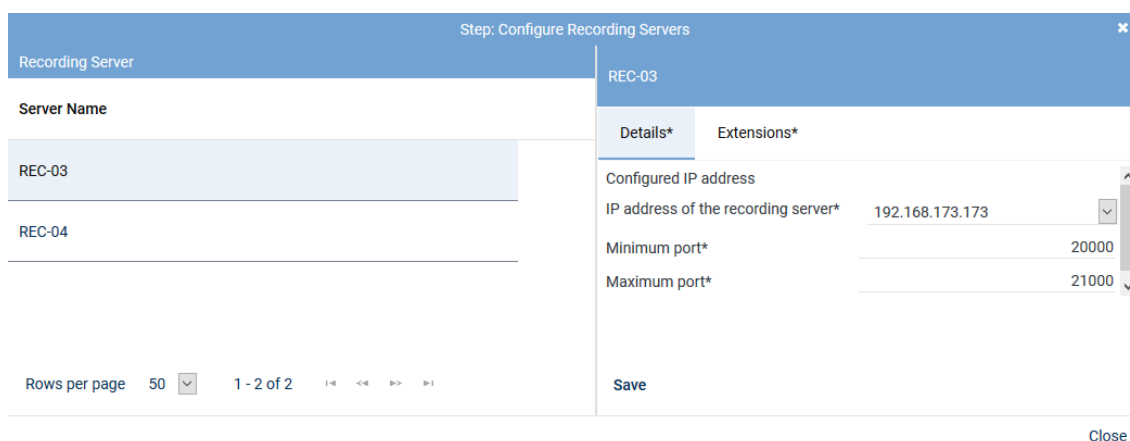


Fig. 335: Configuration step - Configure recording servers

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

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

Tab. 89: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

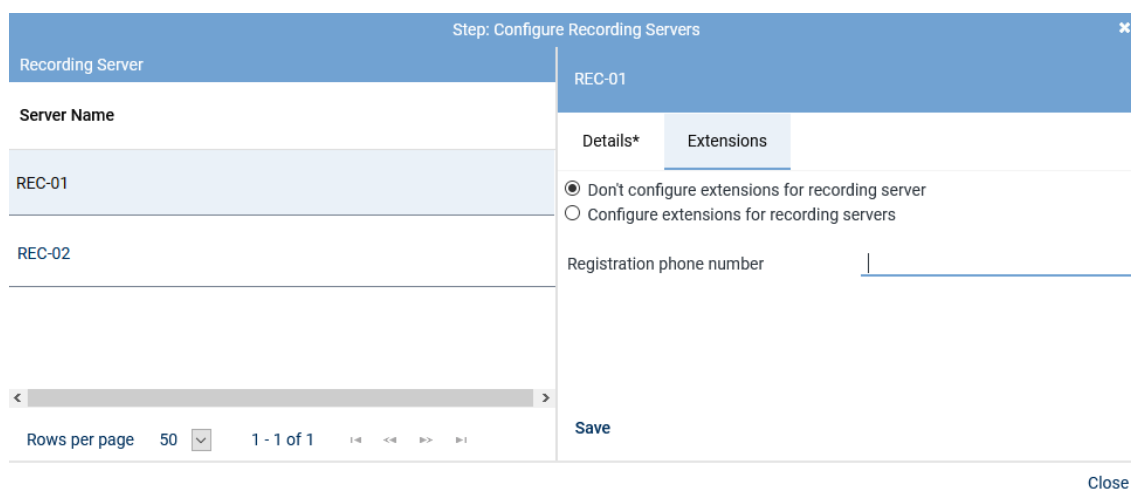


Fig. 336: Recording server - Configure extension for SIP trunk

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a [SIP](#) trunk phone number instead.



If you do not define a phone number for the [SIP](#) trunk of the recording server, all incoming [SIP](#) connections are accepted without being examined.

Registration phone number Enter a registration phone number for the [SIP](#) trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the [SIP](#) trunk, see [chapter "Global recording settings for All-in-one Failover"](#), p. 111.

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

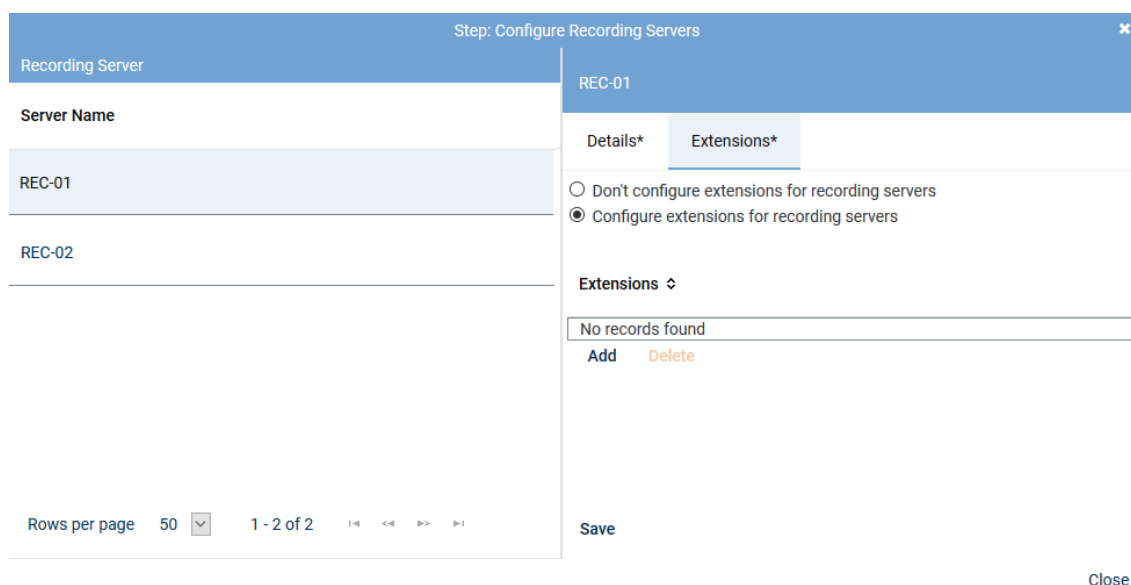


Fig. 337: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

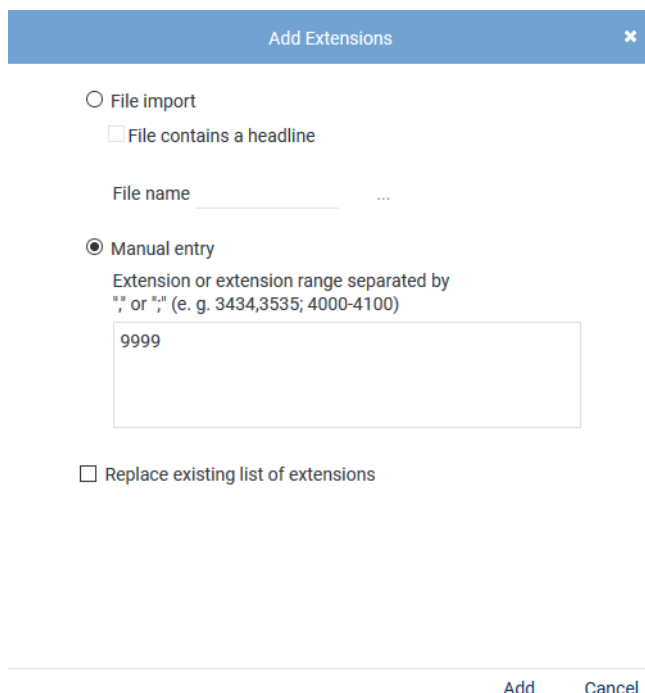


Fig. 338: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
5. If errors have been 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*.
6. The configured extensions now appear in the detail view.

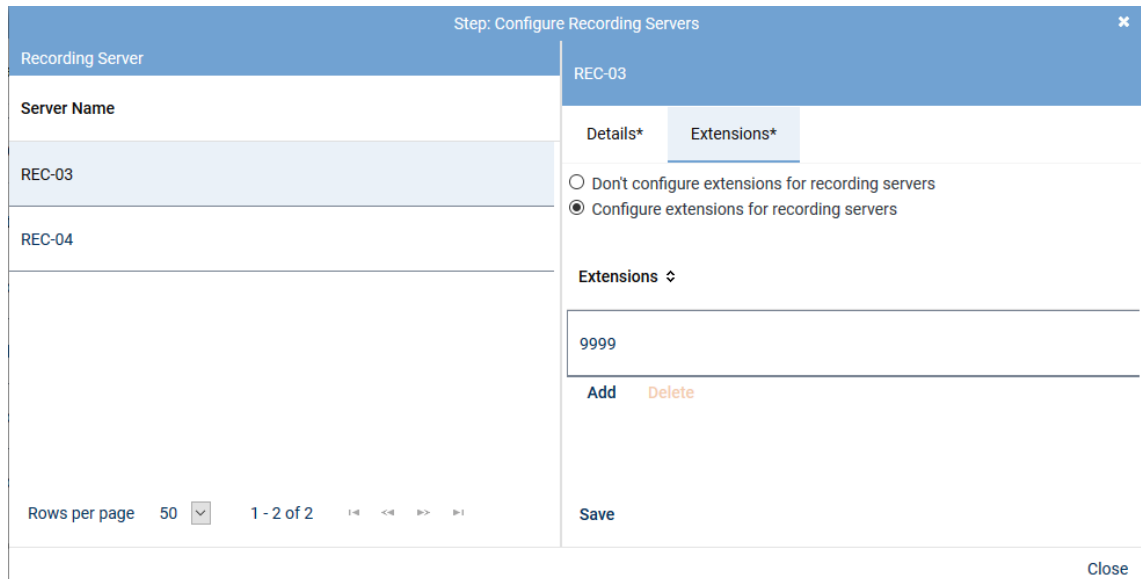


Fig. 339: Added extensions

- Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the **SIP** registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the **SIP** end-points again.

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

Configure add-on



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

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



The additional data delivered by an add-on supplements the additional data which is delivered by the 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 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

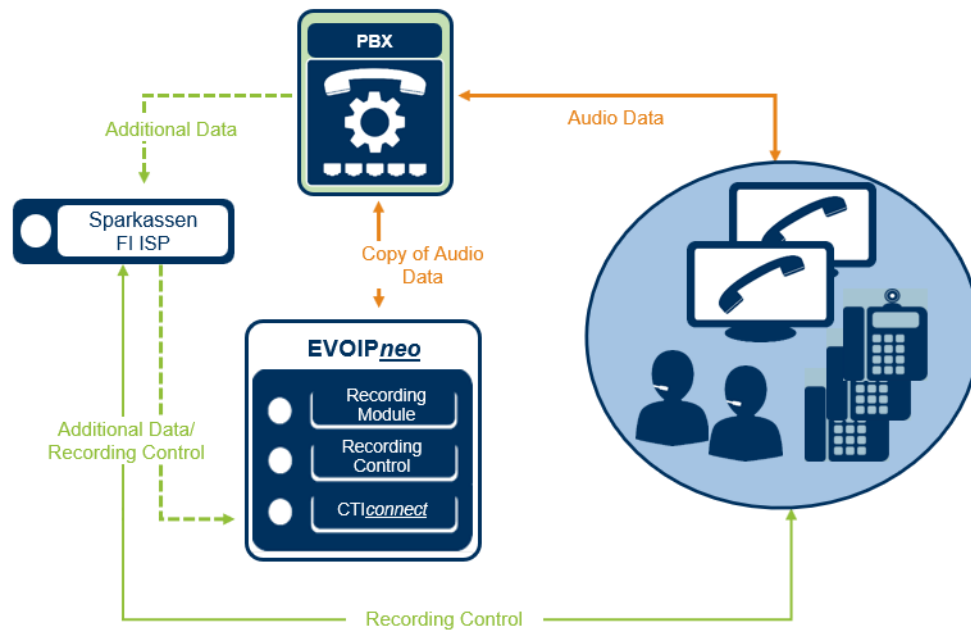



Fig. 340: Overview of Sparkassen FI ISP

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. 341: 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. 90: Configure CTIconnect module



For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

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

Tab. 91: 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.

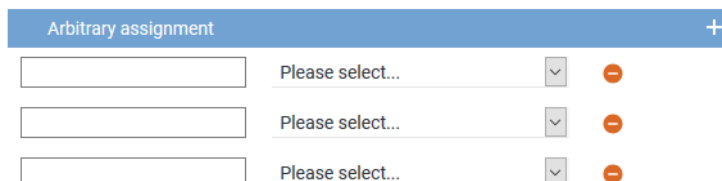



Fig. 342: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)"](#), p. 384.

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. 343: 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. 92: 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:

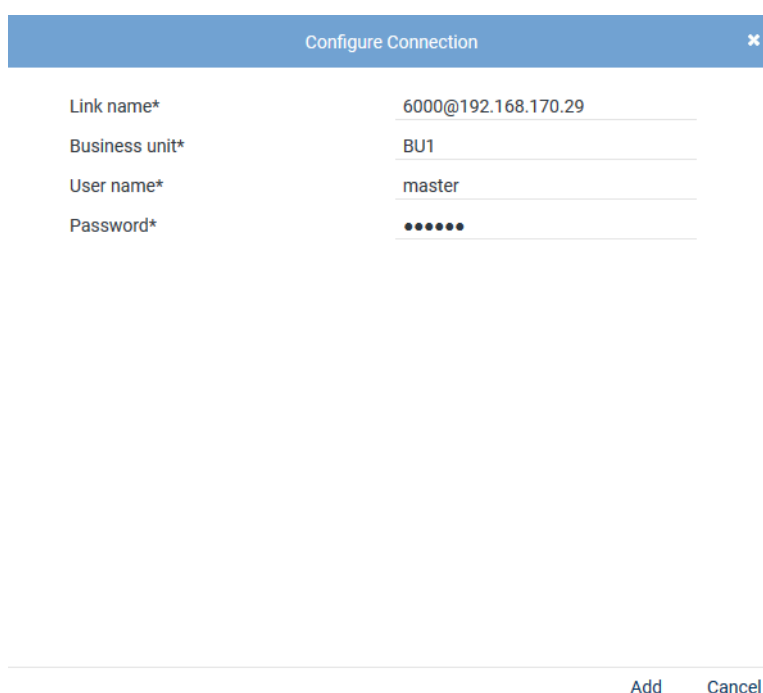


Fig. 344: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 93: 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.

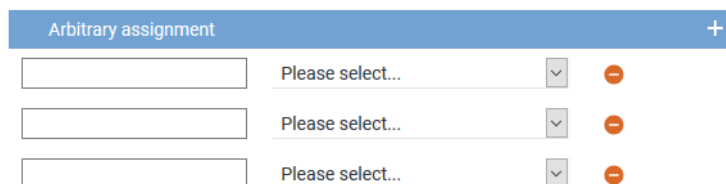




Fig. 345: Arbitrary assignment of the additional data

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 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

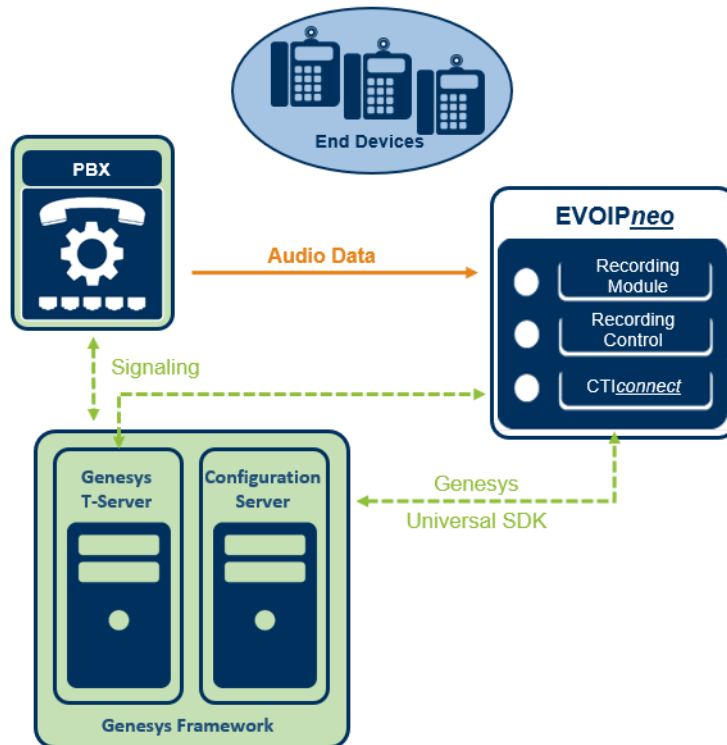


Fig. 346: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

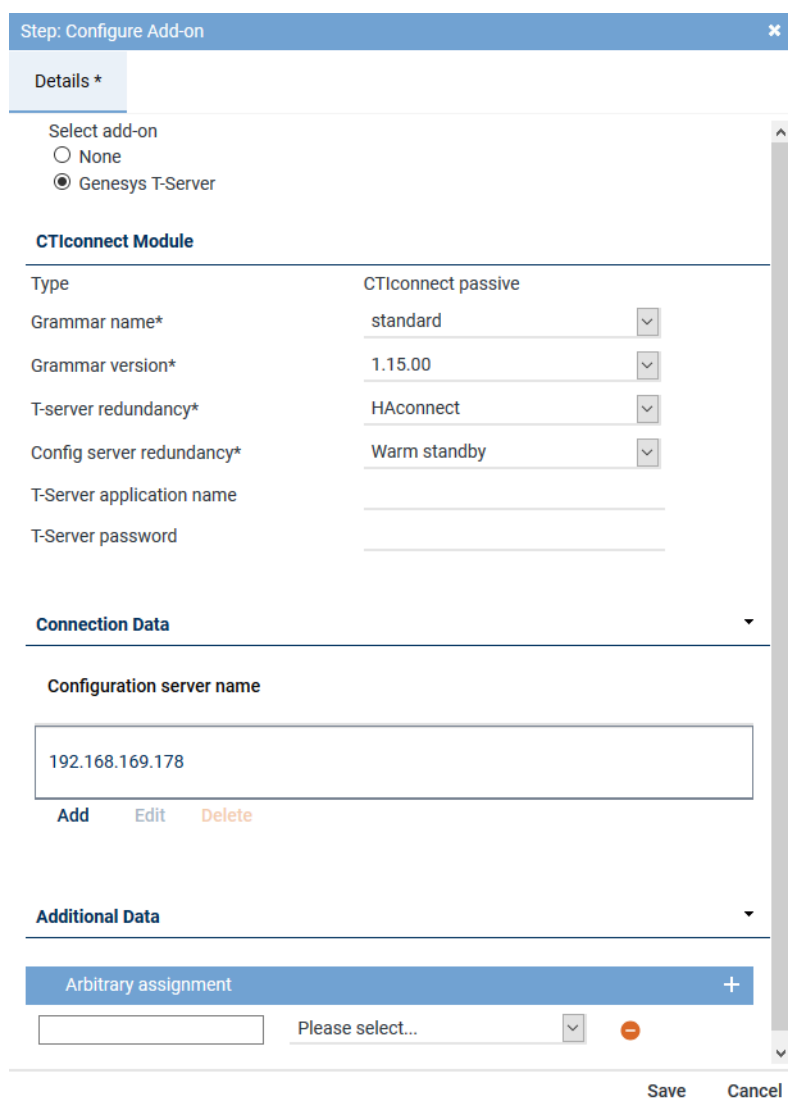


Fig. 347: Configure add-on for Genesys T-Server

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.

Parameter	Value/Description
	<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. 94: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

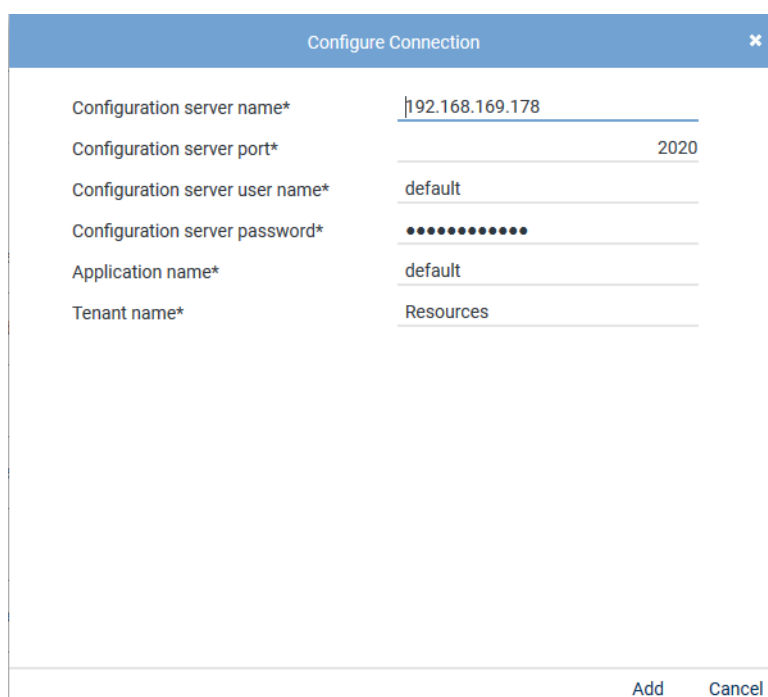


Fig. 348: Configure connection data

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.

Parameter	Value/Description
<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. 95: Configure connection data

Group field Additional Data

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

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



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

Arbitrary assignment

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



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

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



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

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

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

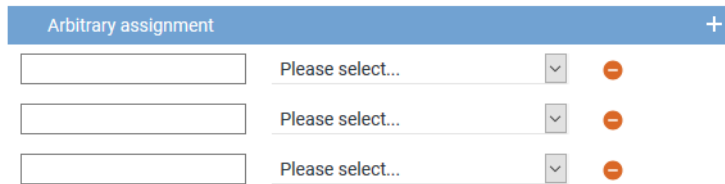



Fig. 349: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

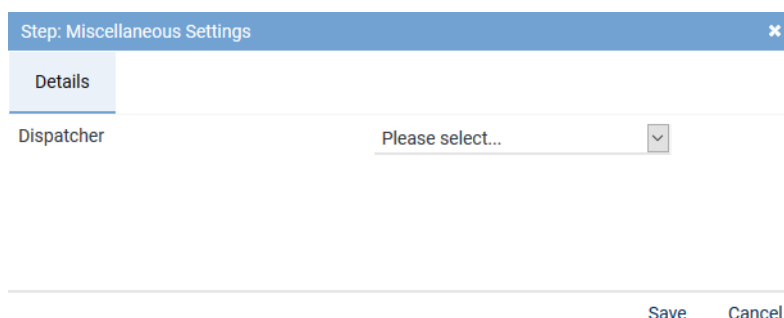


Fig. 350: Configure miscellaneous settings

2. Enter the following parameter:


Parameters	Description
<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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 351: Activate integration

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




+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		

Fig. 352: Activated integration



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



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






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

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

Deactivate/Delete integration

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

- 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 active	SIP active		

Fig. 353: 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:

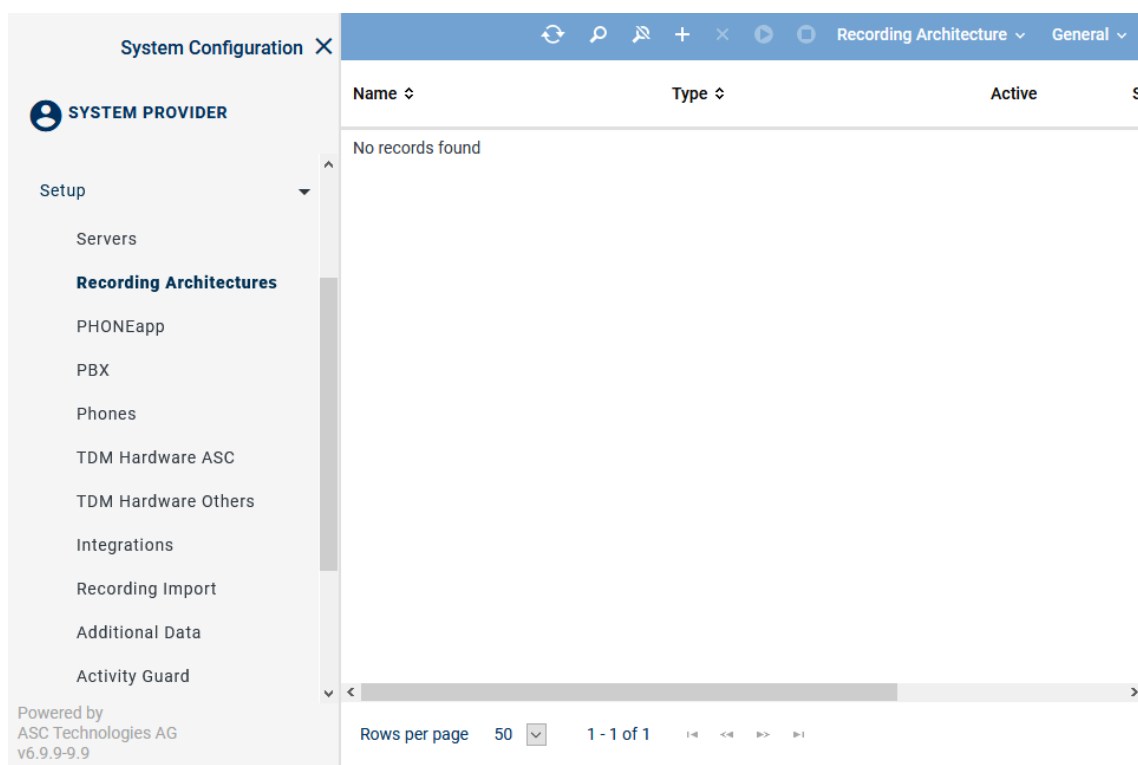




Fig. 354: Recording architectures - main view

Name	Name of the recording architecture
Type	Type of the recording architecture
Active	Shows whether the recording architecture has been activated and is ready to be used for the recording. <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. 355: 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*.

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

⇒ The window *New Recording Architecture* appears.

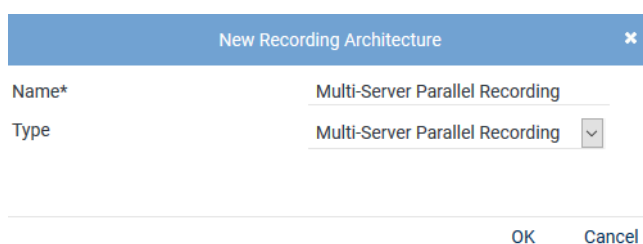
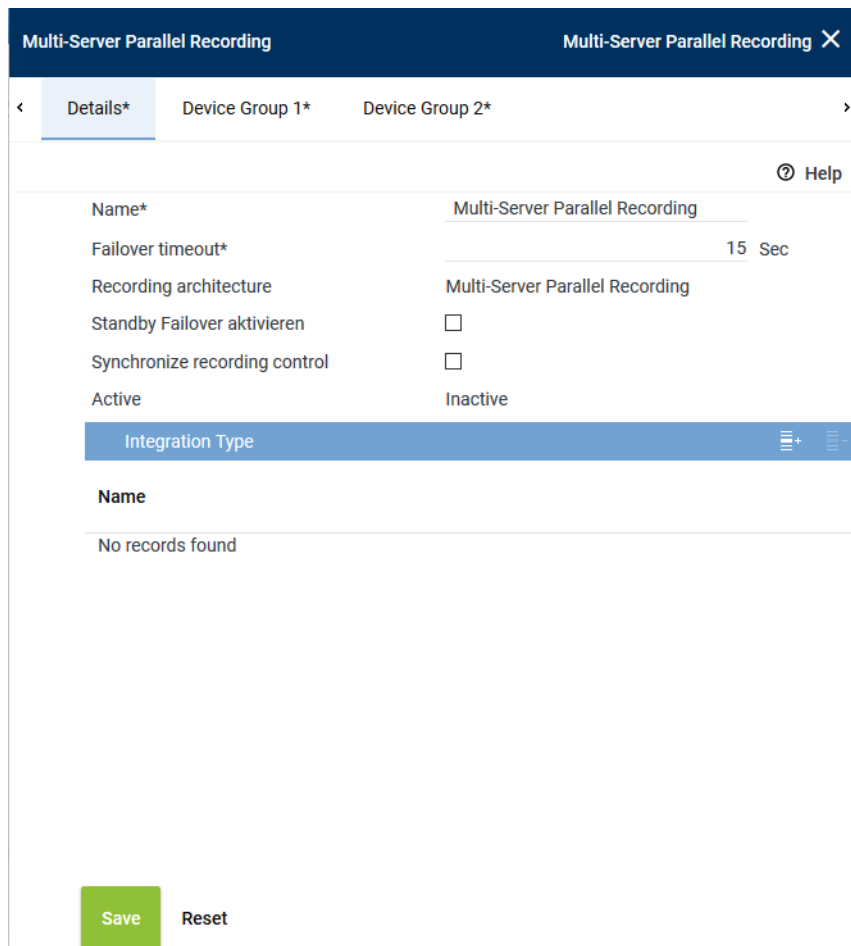


Fig. 356: Create recording architecture - Multi-Server Parallel Recording

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

3. From the drop-down list *Type*, select the recording architecture type *Multi-Server Parallel Recording*.
NOTICE! Only the supported recording architecture types are displayed in the drop-down list.
4. Click on the button *OK*.
 ⇒ The entries now appear in the detail view.



Multi-Server Parallel Recording

Multi-Server Parallel Recording X

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

Help

Name* Multi-Server Parallel Recording

Failover timeout* 15 Sec

Recording architecture Multi-Server Parallel Recording

Standby Failover aktivieren ☐

Synchronize recording control ☐

Active Inactive

Integration Type

Name

No records found

Save Reset

Fig. 357: Recording architecture - tab Details - Multi-Server Parallel Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For more information about the configuration of failover architectures, see [chapter "Standby management for failover architectures", p. 374](#).




Set the failover timeout to a minimum of 15 seconds until the failover process is initiated. Depending on the system architecture it may be useful to set the timeout even higher. The timeout defines how long to wait until the failover process is started. If the state switches back to *OK* within this time, the failover process is not initiated.

5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see [chapter "Synchronization of recording control", p. 366](#).

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

If you do not want to synchronize recording control, you can configure duplicate detection, see [chapter "Duplicates in parallel recording architectures", p. 370](#).

Add integration type

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

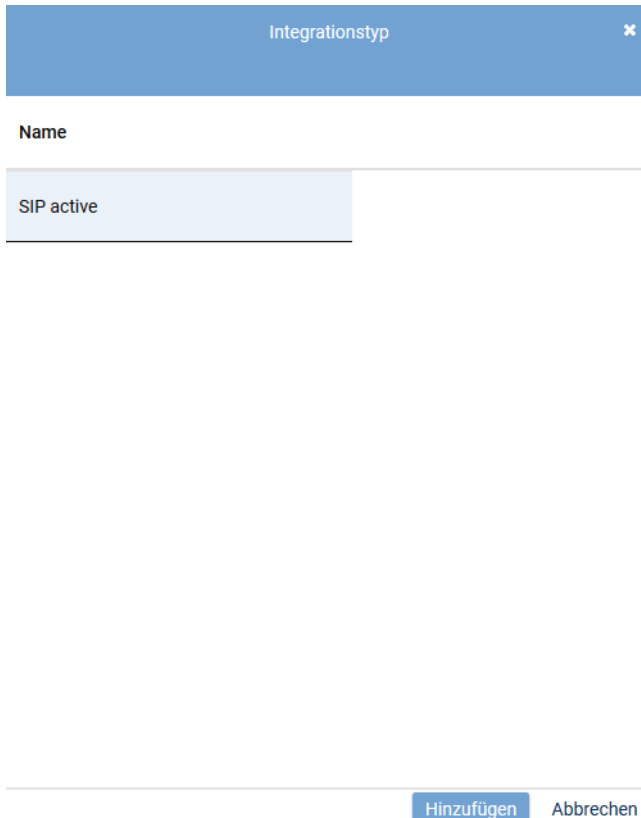


Fig. 358: Select integration type



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



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

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

Assign server for Multi-Server Parallel Recording

In the architecture type *Multi-Server Parallel Recording* a tab for the configuration of the different servers appears for each device group.

Tab Device Group 1

1. Click on the tab *Device Group 1* to configure the distribution of the recording components for the first device group.

Group field Recording Control and 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. 359: 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. 360: Recording architecture - assign server - example

2. Select the server for the *Recording Control module*.
3. Click on the button *Add*.
⇒ The name of the server appears in the detail view.
4. To delete an assignment, click on the icon .




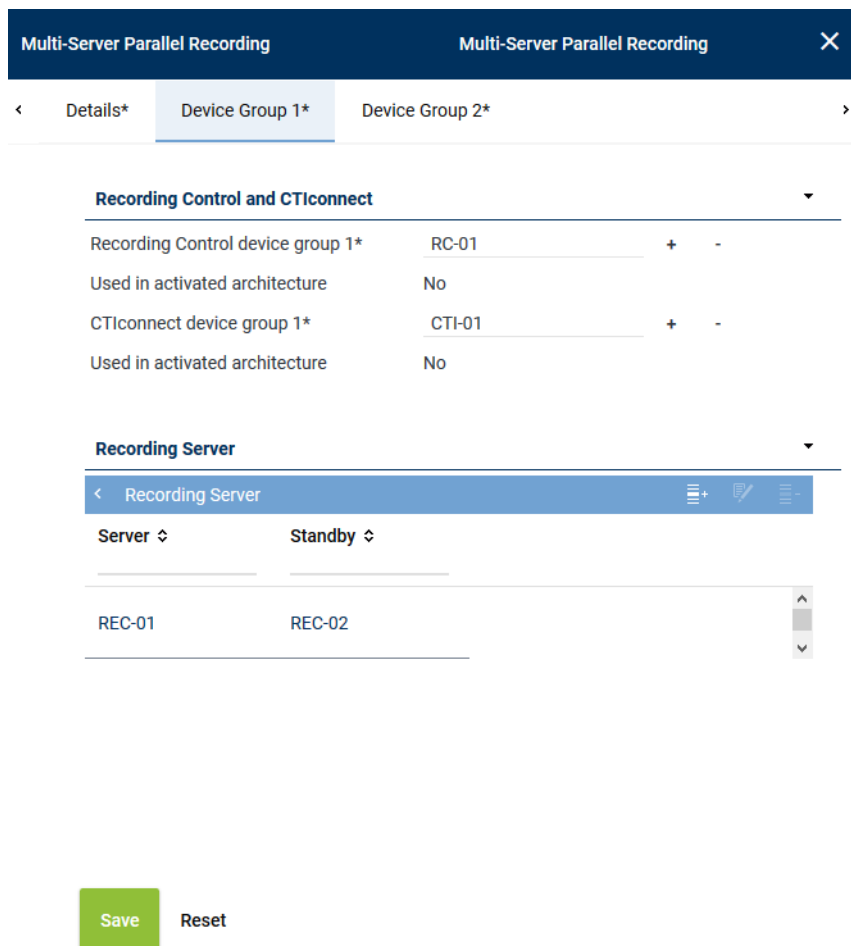
A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.

If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

5. Repeat the steps and select the server for the *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 ×

< 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. 361: Add recording server

2. Following the steps described above, go to the entry field *Primary server* and click on the icon  to select the primary server where recording is supposed to be active.
3. In the entry field *Standby server*, click on the icon  to select the standby server which is supposed to do the recording in case of an error.

4. Tick the check box to activate the recording type you would like to use for this server.
NOTICE! You can activate several recording types if the integration supports them and if the corresponding licenses have been installed.
5. Click on the button *OK* to close the window.
⇒ The name of the server appears in the detail view.
6. To edit the assignment subsequently, click on the icon .
To delete an assignment, click on the icon .
7. If you would like to add additional recording servers repeat the steps described above.




Tab Device Group 2

1. Click on the tab *Device Group 2* to configure the distribution of the recording components for the second device group.
2. Proceed as described in the configuration of tab *Device Group 1*.



In the same device group, you can select the same server for both recording components. For device group 2, you cannot use a server which is already used in device group 1.

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon  (*Activate*) in the 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. 362: Recording architecture - activate recording architecture - example

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



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



Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see [chapter "Configure duplicate detection", p. 370](#).

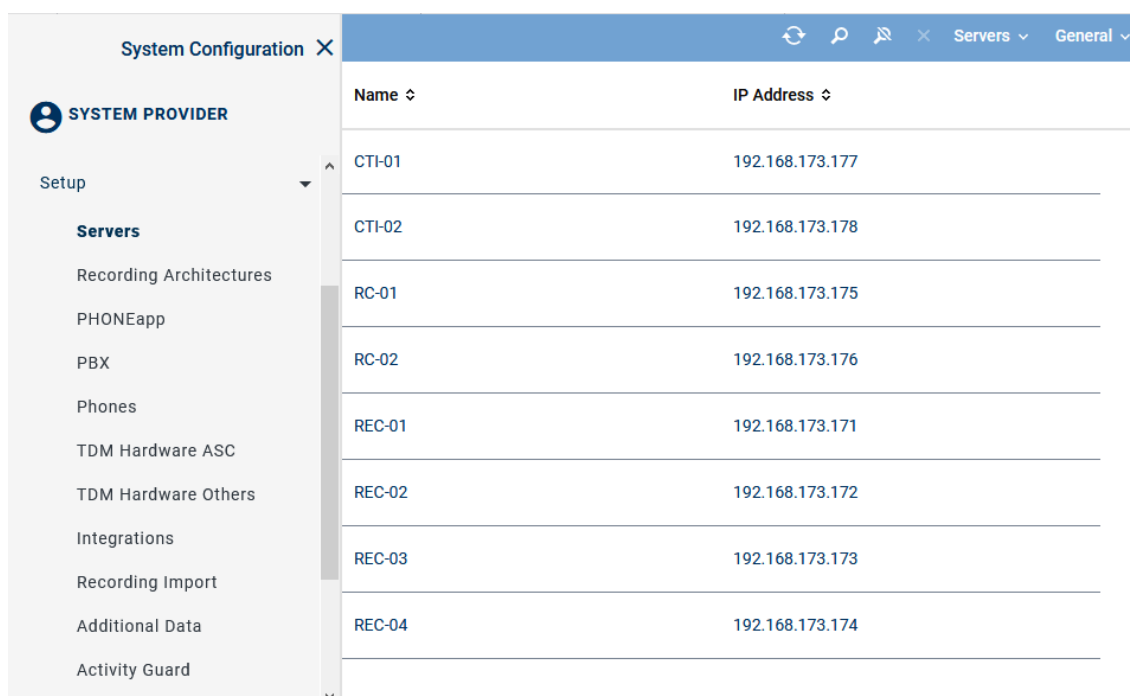


If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

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. 363: 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.

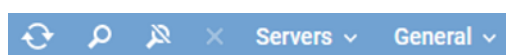







Fig. 364: Toolbar Servers module

	<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. 317 .
	<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.

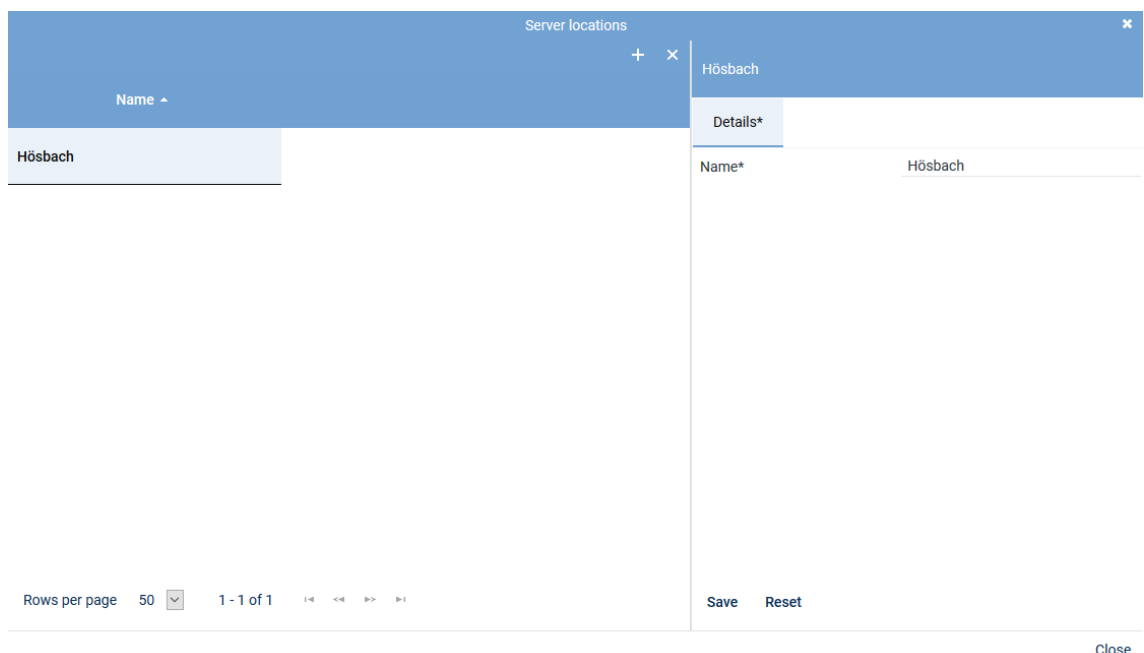



Fig. 365: Add server locations

- 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*.

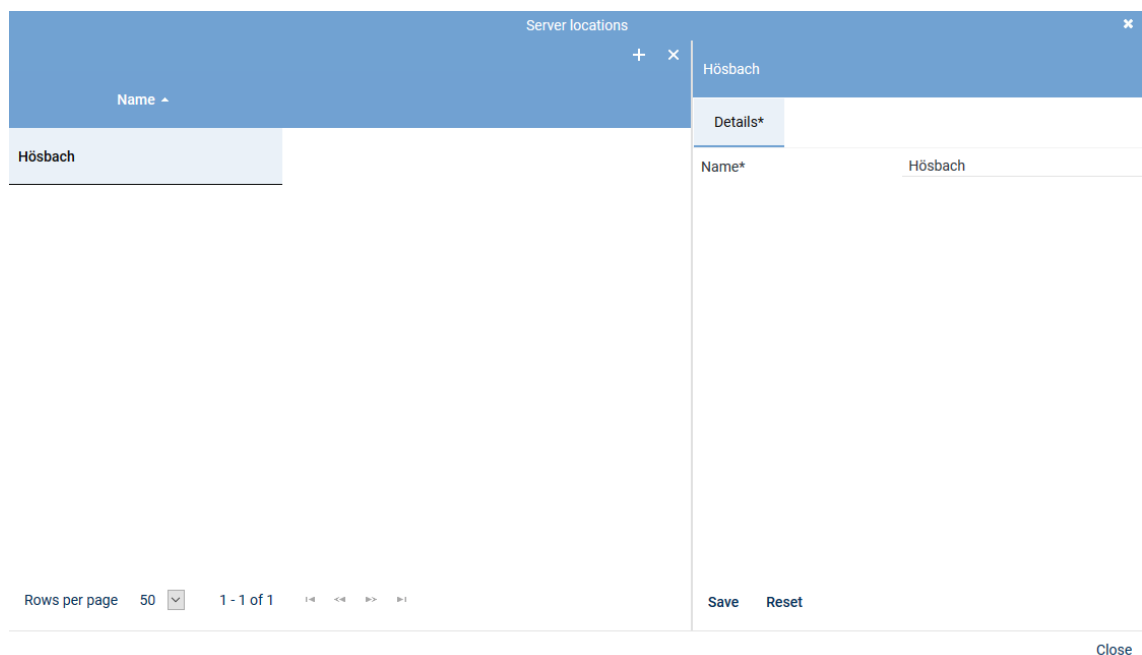
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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 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 at the very bottom right.

Fig. 366: Delete server location

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

Tab Details

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

<
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"/>

Save
Reset

Fig. 367: 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	▶

Save
Reset

Fig. 368: Servers - tab usage

Group field API Server

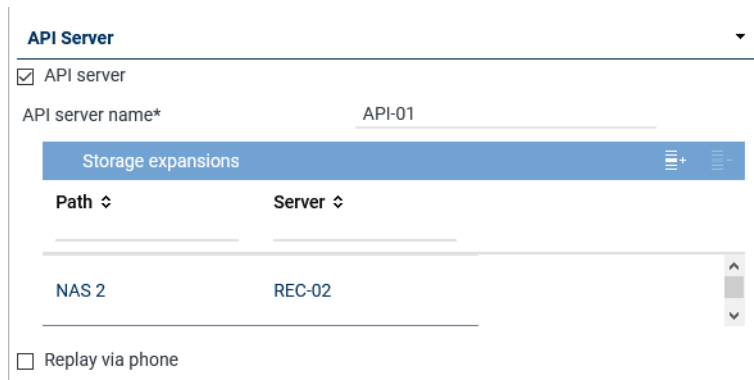




Fig. 369: Group field API Server

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


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

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

Parameter	Value/Description
<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. 330.</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. 321. 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 <i>neo</i> 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. 328. 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. 370: 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. 371: 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. 96: Configure audio analysis

Emotion Detection ×

📋

Name ↕

REC-01

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

Add Cancel

Fig. 372: 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/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 373: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use CLIENT <i>command</i> or API recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.
<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 <code>ASC_KEY_MANAGEMENT</code> 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. 97: 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

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 374: Group field Data Processing

EVOIP_{neo} active for SIP - _{neo} 6.x Rev. 17


323 / 406

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<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  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 325. 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. 325. 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!</p> <p>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>

Parameter	Value/Description
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<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 <i>neo</i> to <i>neo</i>, 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. 98: 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
Rows per page 20 1 - 6 of 6	
<div>Add Cancel</div>	

Fig. 375: Select server



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

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

Group field *Replay*

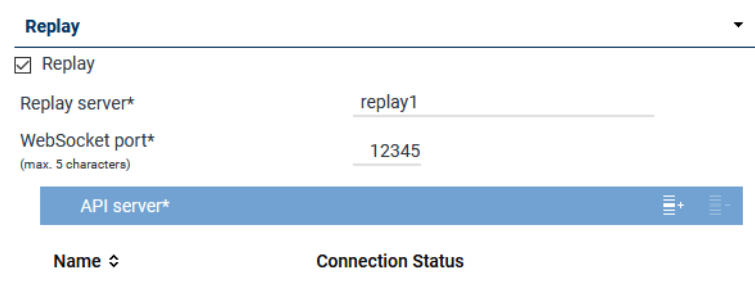




Fig. 376: Group field *Replay*

Parameter	Value/Description
<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>

Parameter	Value/Description
	<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. 327. By clicking on the icon  (Remove), you can remove selected API servers from the list.

Tab. 99: 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.

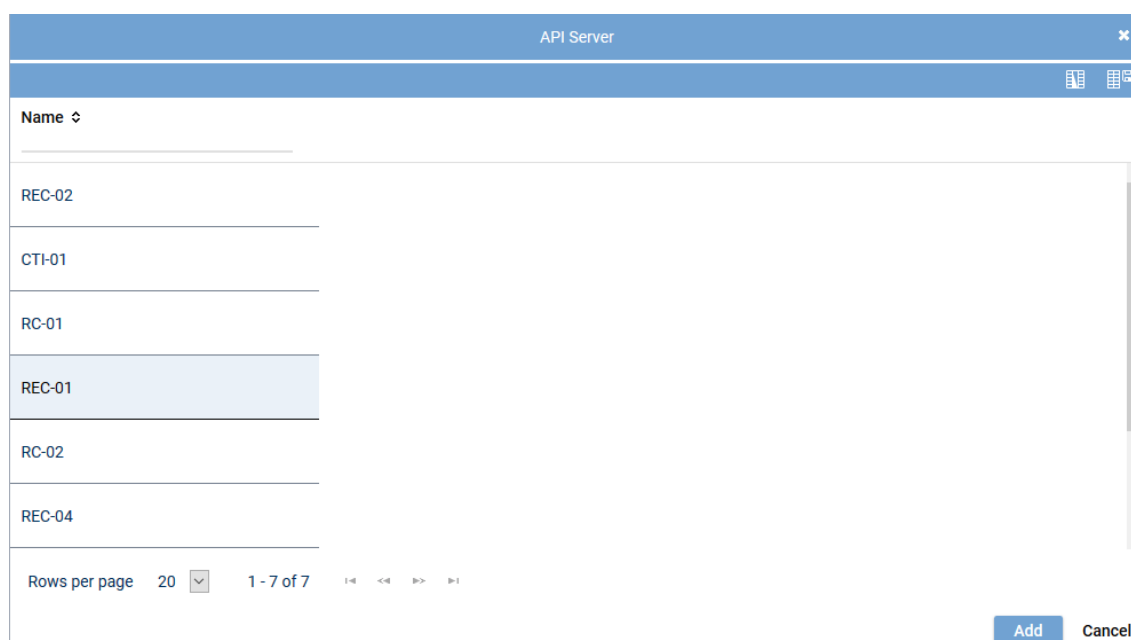


Fig. 377: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 320.

- 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. 378: 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. 100: 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. 379: 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. 335.</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> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</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 UDP = unencrypted 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>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address 169.254.254.101.</p>
<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 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. Servers which have been activated for replay require this address mapping so that they can be reached from a public network and with configured port forwarding.



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




Fig. 380: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters

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



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

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



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



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

Tab Key Management

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

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

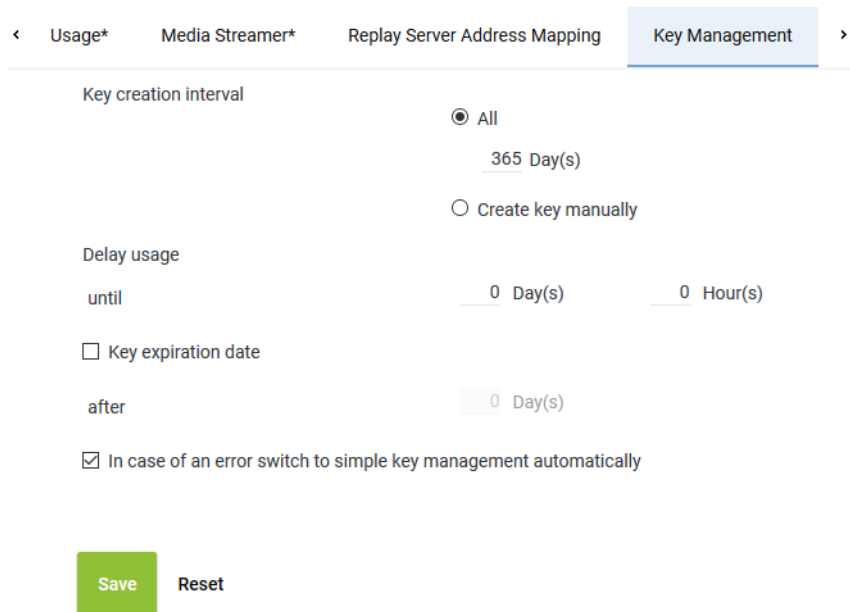


Fig. 381: Servers module - tab Key Management

Key creation interval	<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>
Delay usage	<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>
Key expiration date	<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 <u>neo</u> 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 <u>neo</u> 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 <u>neo</u> 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.

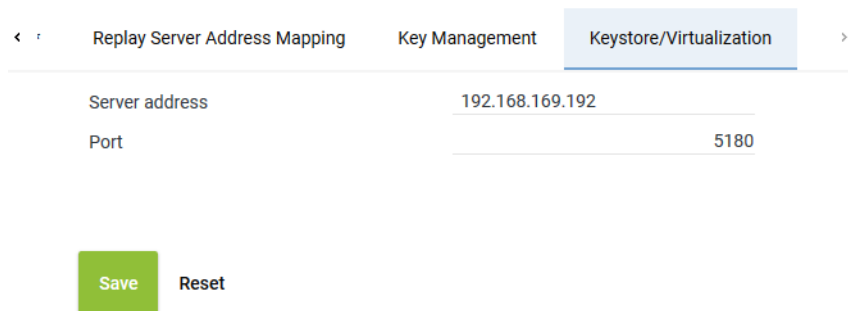
- *Trusted Virtualization License*

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' (grey).

Fig. 382: 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*.

7.1.2.6.3 Create PBX

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

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

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

⇒ The following window appears:

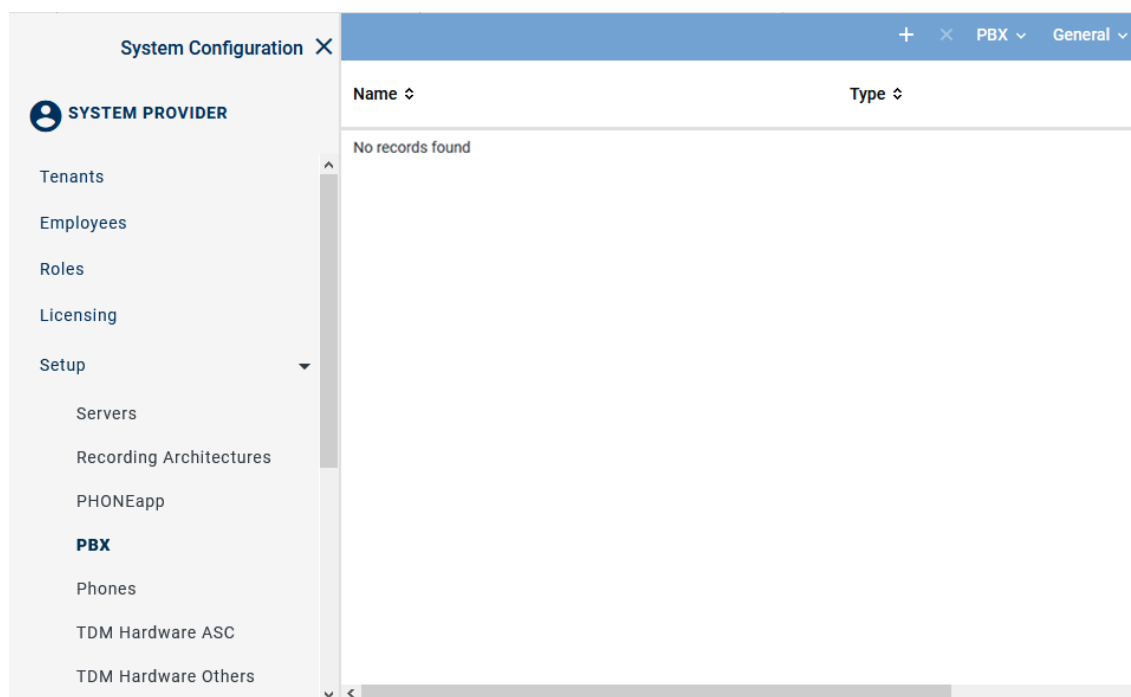


Fig. 383: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

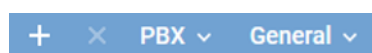




Fig. 384: Toolbar PBX module


	<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.

Module Help Opens the module-specific online help.



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

Create new PBX

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

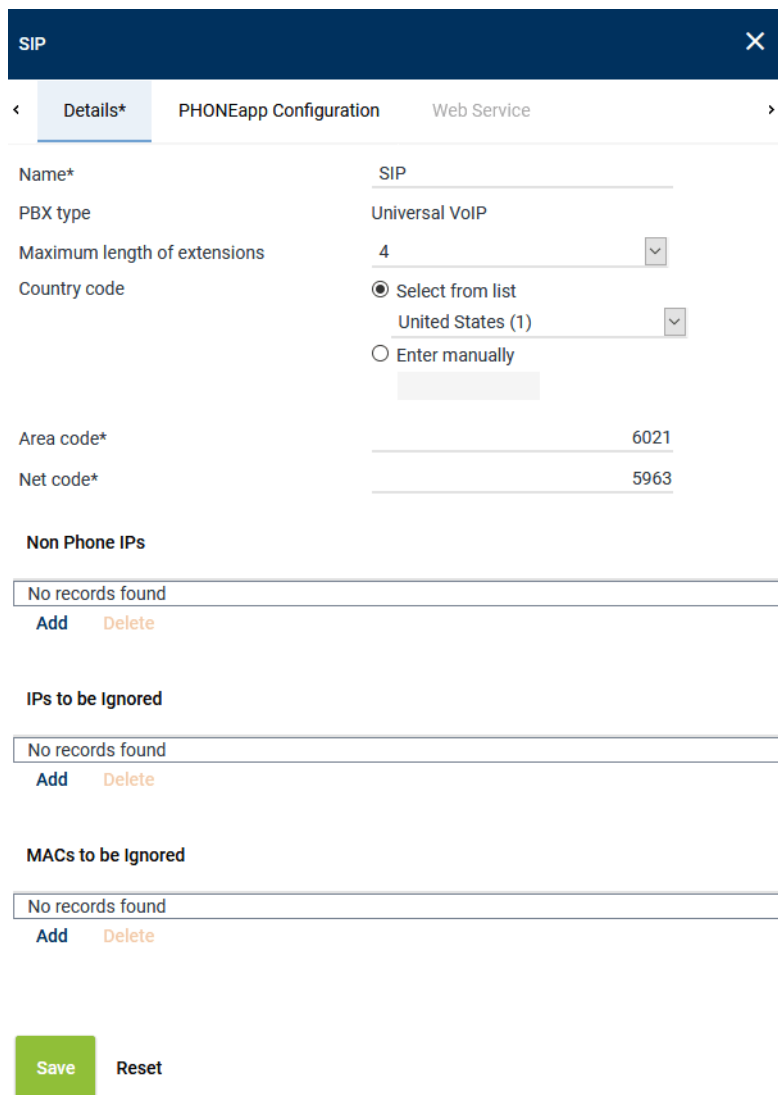


Fig. 385: Create new PBX - tab Details

- 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.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Enter manually</i> <p>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>.</p>
<i>Area code</i>	Enter the area code without the preceding <i>0</i> , e. g. <i>6021</i> .
<i>Net code</i>	Enter the net code, e. g. <i>5963</i> . Do not enter an extension here.

Tab. 101: Create PBX

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

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

Tab. 102: PBX parameters with complete phone number

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

7.1.2.6.4 Assign recording resources

Resources for tenants

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

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

Assign extensions to tenants

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

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

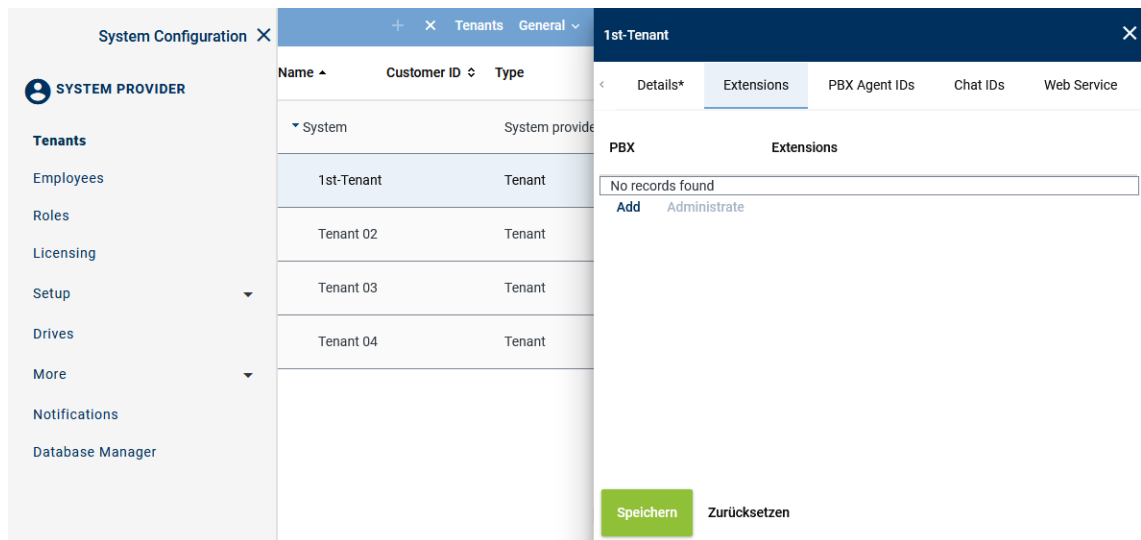
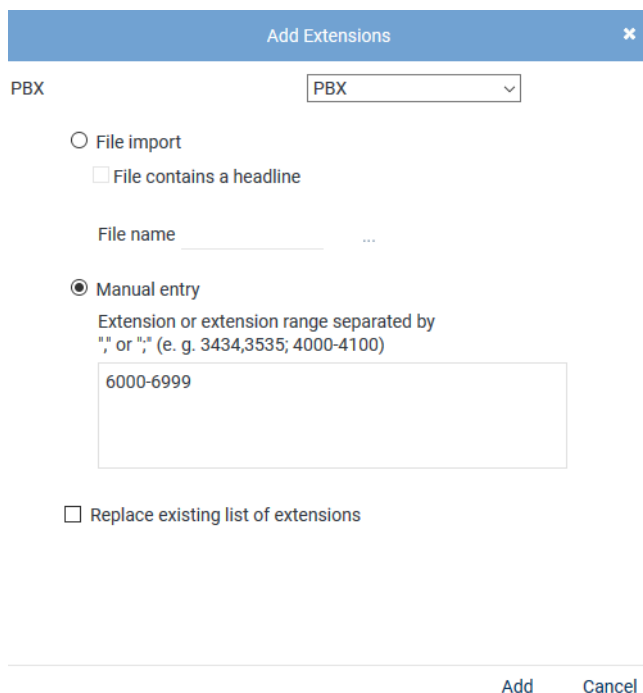


Fig. 386: Tenants - main view - tab Extensions

Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.
 - ⇒ The following window appears:



The 'Add Extensions' dialog box has a 'PBX' dropdown menu set to 'PBX'. It contains two radio buttons: 'File import' (unselected) and 'Manual entry' (selected). Under 'File import', there is a checkbox for 'File contains a headline' and a 'File name' field. Under 'Manual entry', there is a text area containing '6000-6999' and a checkbox for 'Replace existing list of extensions'. At the bottom are 'Add' and 'Cancel' buttons.

Fig. 387: Assign extensions to tenants

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

File import	<p>Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported:</p> <ul style="list-style-type: none"> • ZIP • TXT
--------------------	---

- CSV

NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.



File contains a headline

Activate this option so that this structured is recognized correctly when importing the file.

The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.

File name

To import the file, proceed as follows:

- Click on the button  behind the field *File name*.
- Click on the button *Choose File*.
- Select the respective file in the Explorer and click on the button *Open*.
- Click on the button  *Upload File*.

Manual entry

Select this option to enter extensions or extension ranges manually.

To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100.

Enter country codes as number ranges as follows:

+4984496800--+4984496810

NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

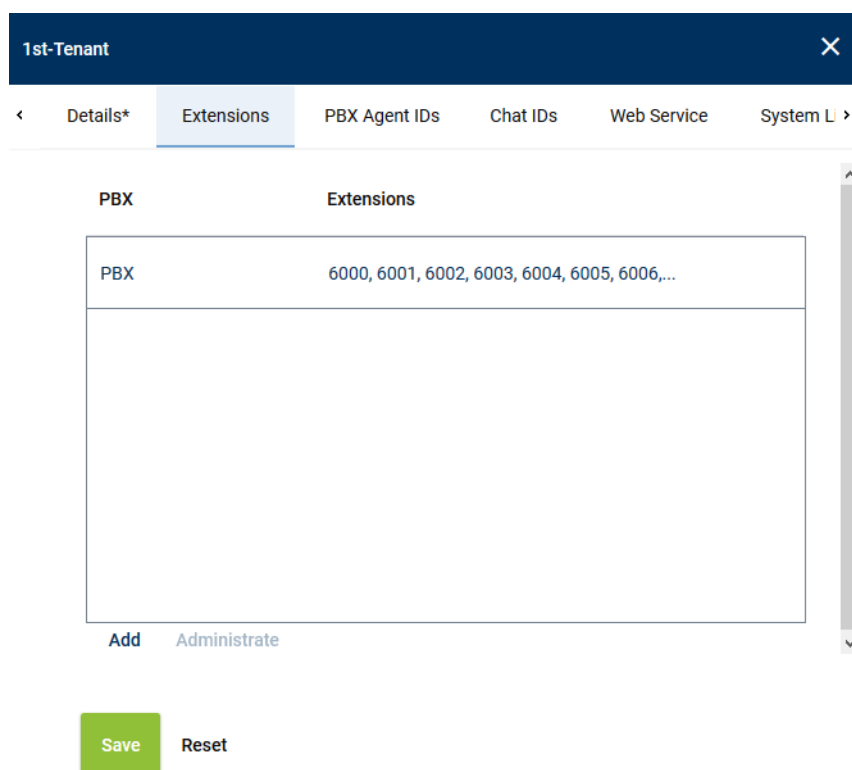
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

- Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
- 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*.
- The configured extensions now appear in the detail view.
- Click on the button *Save* in the detail view to save the entries.

Remove extensions

- 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. 388: Remove extensions

- 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.



Administrate Extensions

6993
6994
6995
6996
6997
6998
6999

Remove Cancel

Fig. 389: Select extensions

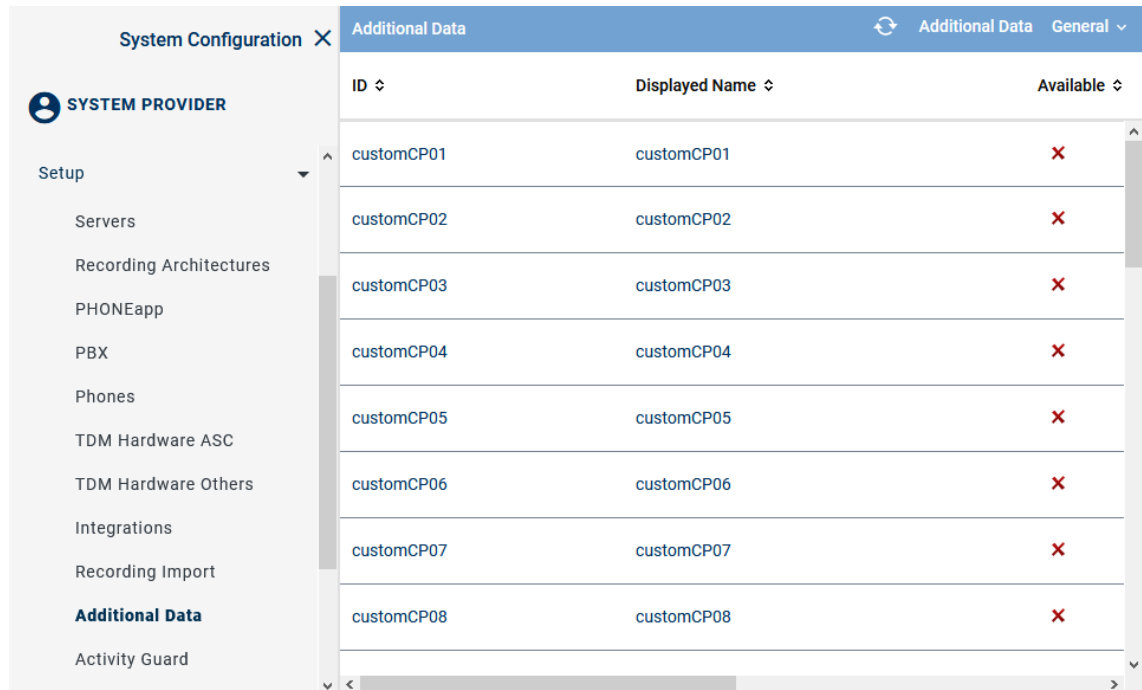
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

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.

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



ID	Displayed Name	Available
customCP01	customCP01	X
customCP02	customCP02	X
customCP03	customCP03	X
customCP04	customCP04	X
customCP05	customCP05	X
customCP06	customCP06	X
customCP07	customCP07	X
customCP08	customCP08	X

Fig. 390: 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. 391: 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"/>

Save
Reset

Fig. 392: Additional data - configure availability

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



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



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

7.1.2.6.6 Create integration for Multi-Server Parallel Recording

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

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

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

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

System Configuration

SYSTEM PROVIDER

Setup

Servers

Recording Architectures

PHONEapp

PBX

Phones

TDM Hardware ASC

TDM Hardware Others

Integrations

Recording Import

Additional Data

Activity Guard

Powered by
ASC Technologies AG
v6.9.9-9.9

+

×

▶

⏸

Integration

General

Name

Type

Active

Status

1

SIP active

SIP active

✗

⚙

1

Cisco active

Cisco UCM active

✗

⚙

1

Avaya active

Avaya CM active

✗

⚙

1

MiVB

Mitel MiVoice Business active

✗

⚙

1



<<

1

>>

Fig. 393: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.


+ × ⏮ ⏭	Integration ▾	General ▾
---------	---------------	-----------

Fig. 394: Toolbar Integrations module

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

<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.

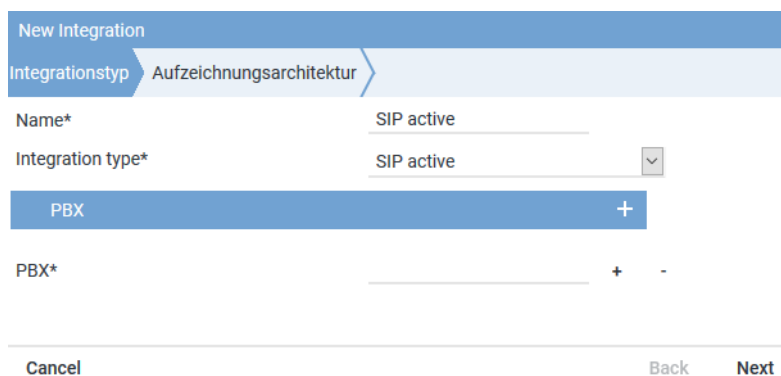



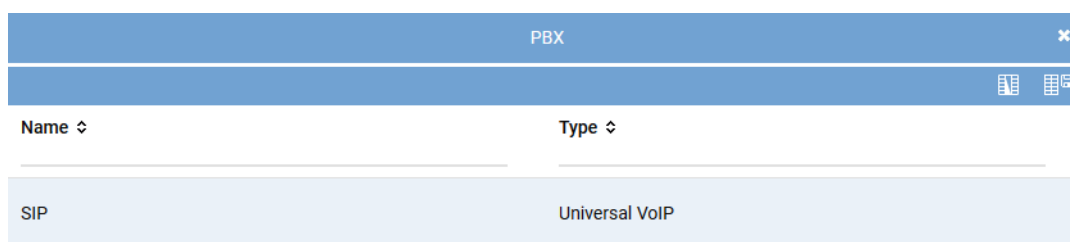
Fig. 395: Create integration type

- 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 active</i> from the drop-down list <i>Integration type</i> .

Tab. 103: Create integration type

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





Rows per page 20  1 - 1 of 1 

Fig. 396: Select PBX

- Select the respective *PBX* from the list of available PBXs.

5. Click on the button *Add*.

Assign recording architecture for Multi-Server Parallel Recording

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

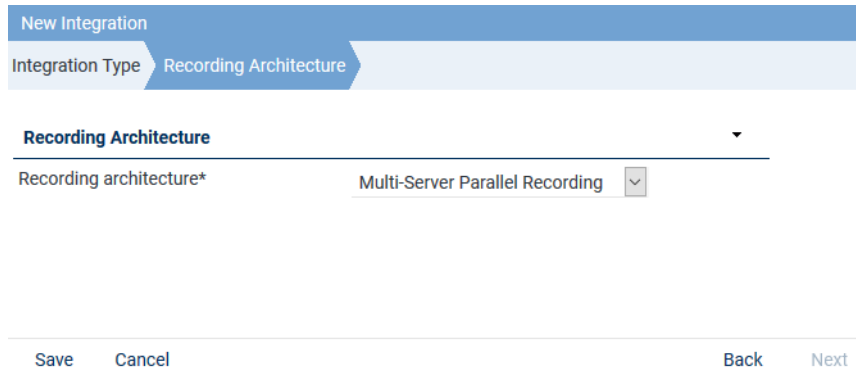


Fig. 397: Assign recording architecture - Multi-Server Parallel

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




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

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



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see [chapter "Duplicates in parallel recording architectures", p. 370](#).

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 active		SIP active		X		x	
Step				Configuration			
Configure recording architecture				✓			
Global recording settings				X			
Configure recording servers				X			
Configure add-on				✓			
Configure miscellaneous settings				✓			

Fig. 398: 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.

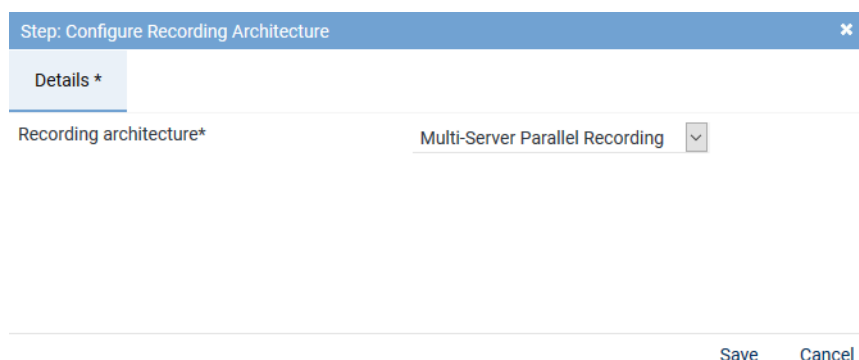



Fig. 399: Configuration step - Configure Recording Architecture

- 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.

Global recording settings for Multi-Server Parallel Recording

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

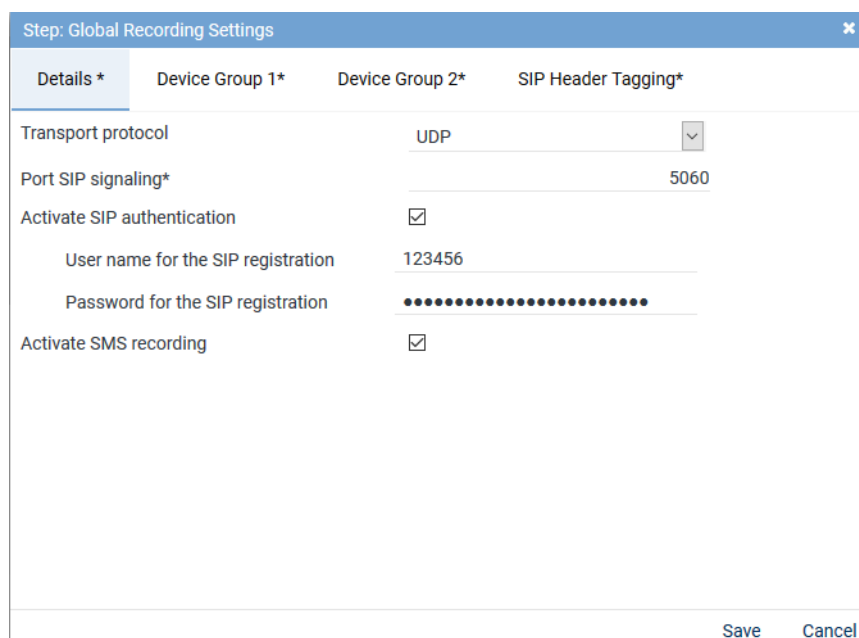


Fig. 400: Configuration step - Global Recording Settings - Multi-Server Parallel Recording

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

Parameter	Value/Description
<i>Transport protocol</i>	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling, where the recording server is expecting the signaling. The default value is 5060.
<i>Activate SIP authentication</i>	Activate this option if you would like to use the SIP digest authentication.
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password of the SIP registration</i>	Enter the password, if an authentication for the SIP registration is used.
<i>Activate SMS recording</i>	Activate the check box if you would like to use SMS recording.

Tab. 104: Global recording settings

- Click on the button Save.

Tab SIP Header Tagging

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

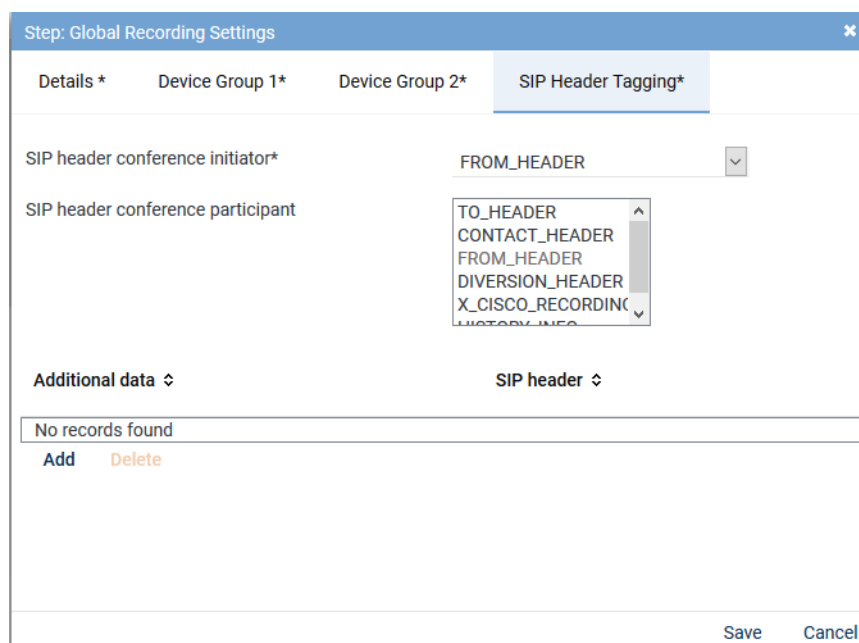


Fig. 401: Tab SIP Header Tagging Configure sources

- Enter the following parameters:

Parameter	Value/Description
<i>SIP header conference initiator</i>	Select the SIP header which contains the extension of the conference initiator.
<i>SIP header conference participant</i>	Select the SIP header which contains the extension of the additional conference participants.

Parameter	Value/Description
-----------	-------------------

Tab. 105: Configure SIP header tagging



It is possible to select several entries; the information is then displayed one after the other in the respective replay application.

To select several entries, highlight the respective entries while holding the [Ctrl] key down. To deselect an entry, click on it again without releasing the [Ctrl] key.

- If you would like to configure individual additional data that you have defined previously in the Additional Data module, click on the button *Add* in the section *Additional data*.

⇒ The window *SIP Additional Data* appears.

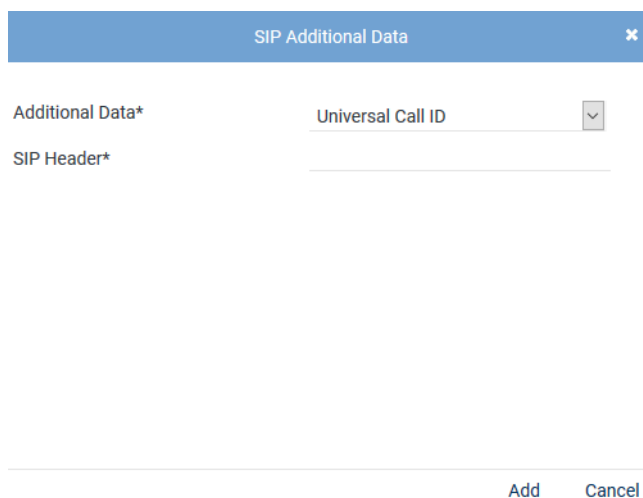


Fig. 402: SIP Additional Data



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

- Enter the following parameters:

Parameter	Value/Description
<i>Additional Data</i>	In the drop-down list, select the display name of the field in which the information of the SIP header is supposed to be released.
<i>SIP Header</i>	Enter the source from the SIP header from where the information is to be extracted. Observe the correct spelling.


Tab. 106: Configure SIP conversation parameters

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

Configure recording server for Multi-Server Parallel Recording

When using several recording servers, you must configure the port range for each recording server separately. The range may be the same for all recording servers. Make sure, though, that the port range is within the port range open in the Firewall. For more information refer to the Communication matrix in the installation requirements.

These settings are configured in the configuration step *Configure recording server*.

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

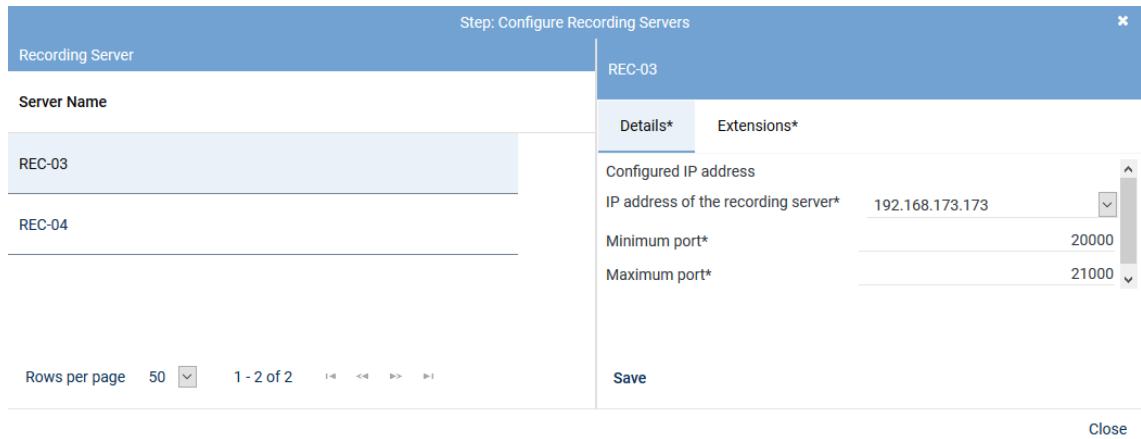


Fig. 403: Configuration step - Configure recording servers

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

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

Tab. 107: Configure recording servers



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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

Tab Extensions

Configure extensions for SIP trunk

To register the **SIP** trunk, you can enter a registration phone number in the tab *Extensions*.

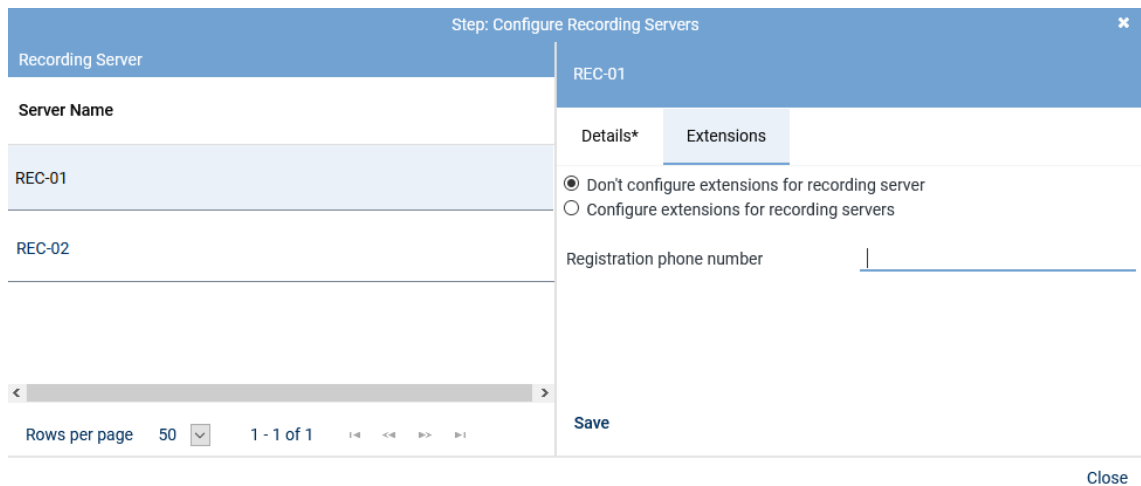


Fig. 404: Recording server - Configure extension for SIP trunk



Ask your provider whether registering 2 servers in parallel mode is supported. To do so, it must be possible to assign a [SIP](#) trunk phone number to 2 different IP addresses at the same time.

Don't configure extensions for recording server - Activate this option if you do not have configured extensions for the recording server in the PBX and would like to configure a [SIP](#) trunk phone number instead.



If you do not define a phone number for the [SIP](#) trunk of the recording server, all incoming [SIP](#) connections are accepted without being examined.

Registration phone number Enter a registration phone number for the [SIP](#) trunk.

For a successful registration, registration must have been activated in the section *Global recording settings*. The user name and password entered there are used to register the [SIP](#) trunk, see [chapter "Global recording settings for All-in-one Parallel Recording", p. 169](#).

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

Configure extensions for the recording server

1. If you have defined extensions for the recording servers in the PBX, you can configure these extensions in the tab *Extensions*.

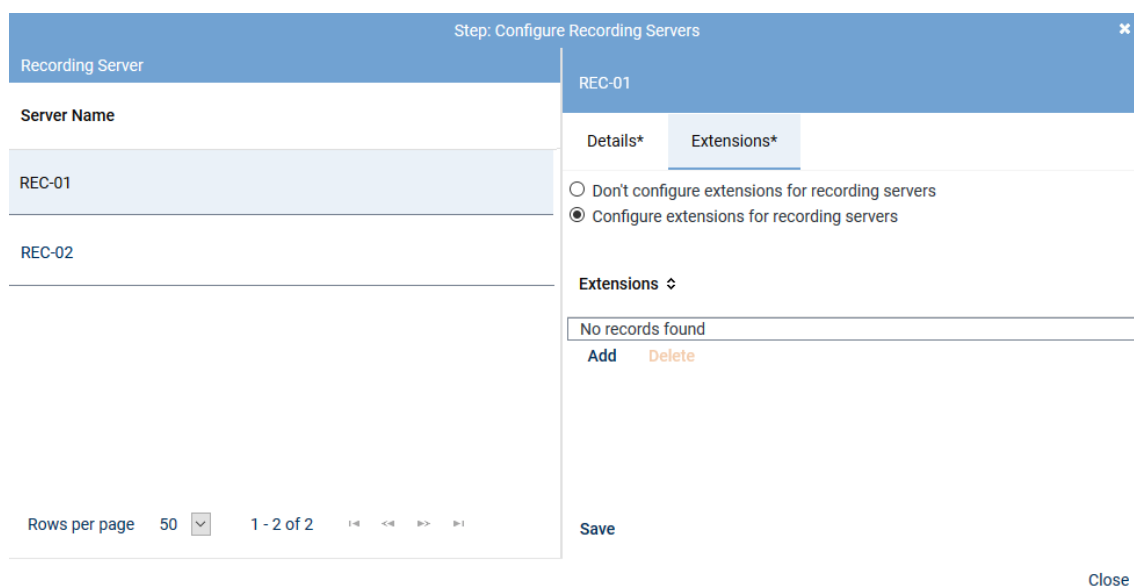


Fig. 405: Tab Extensions

Configure extensions of the recording server Activate this option if you have configured extensions for the recording server in the PBX and add the extensions.

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

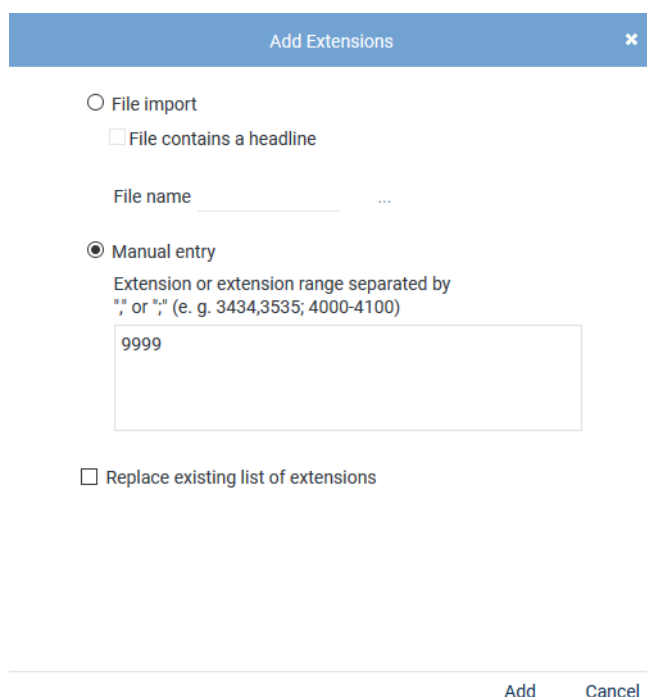


Fig. 406: Add extensions

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

6. The configured extensions now appear in the detail view.

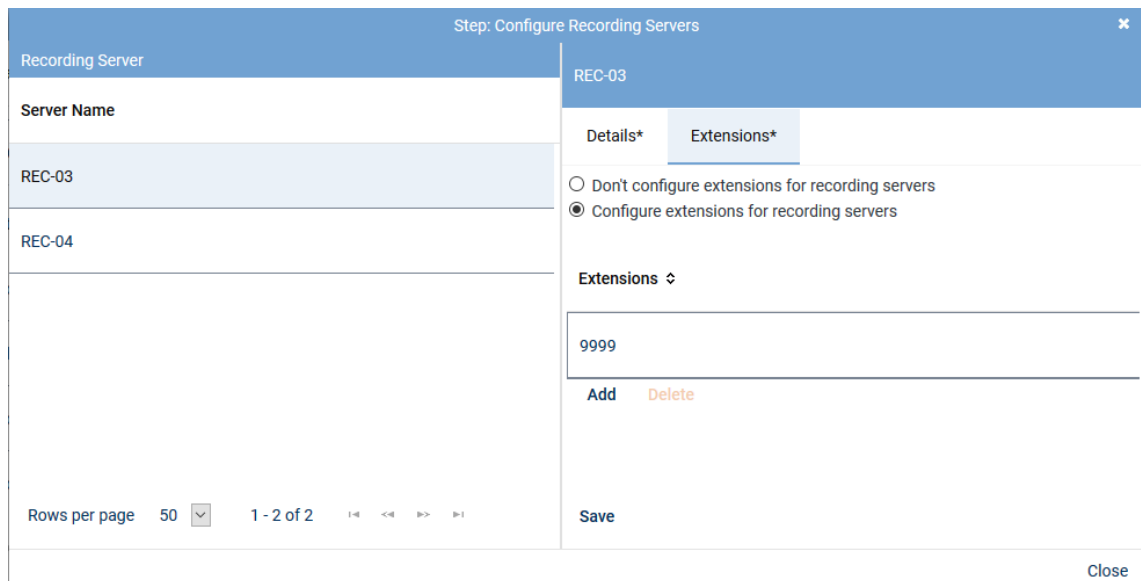


Fig. 407: Added extensions

7. Repeat the steps for additional servers. For each server, configure its own extension or extension range depending on how it can be reached.



In failover architectures, it is recommended to set up a separate extension or extension range for each recording server. If the [SIP](#) registration timer has expired for the extension for the recording server, problems may occur when switching back to the primary recording server. If the primary recording server displays an error, it is not yet possible to register the [SIP](#) end-points again.

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

Configure add-on



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

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



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



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

Configure add-on for Sparkassen FI ISP (optional)

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



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

The integration runs in combination with a PBX and the recording server. The service **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

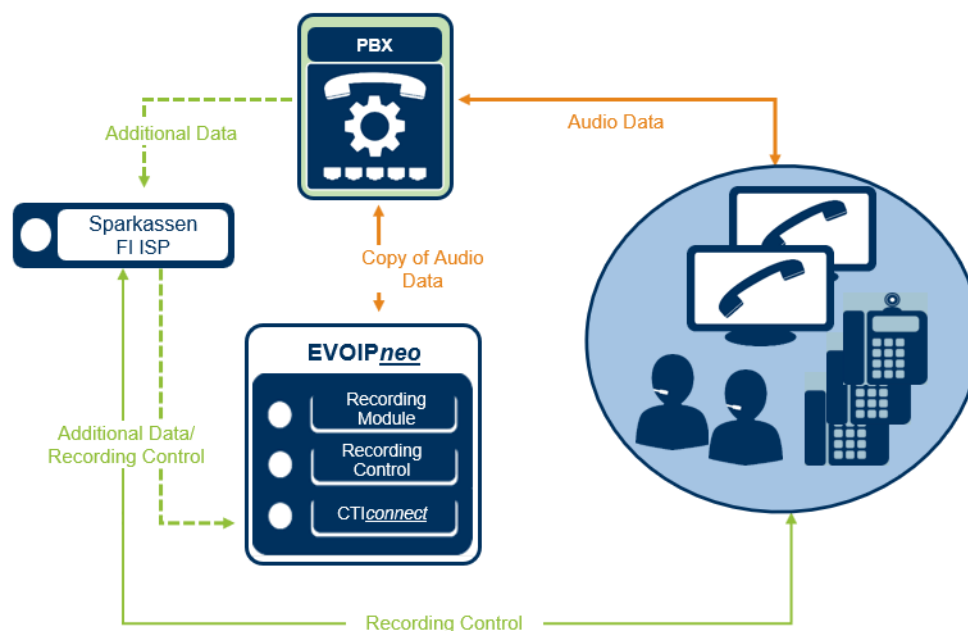



Fig. 408: Overview of Sparkassen FI ISP

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. 409: 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. 108: Configure CTIconnect module



For recording control via the add-on of the Sparkassen FI ISP, grammar version 1.00.05 or higher is required. If the grammar in the respective version is not available yet, you can import it. See [chapter "Import grammar", p. 285](#).

Group field Connection Data

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

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

Tab. 109: 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.

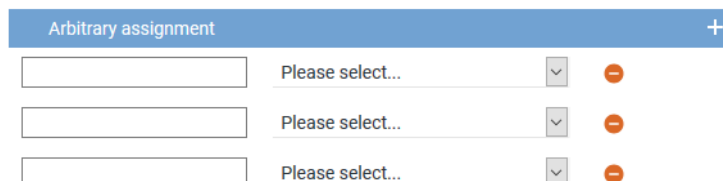



Fig. 410: Arbitrary assignment of the additional data

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 [chapter "Configure OpenScape Contact Center \(optional\)"](#), p. 384.

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. 411: 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. 110: 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:

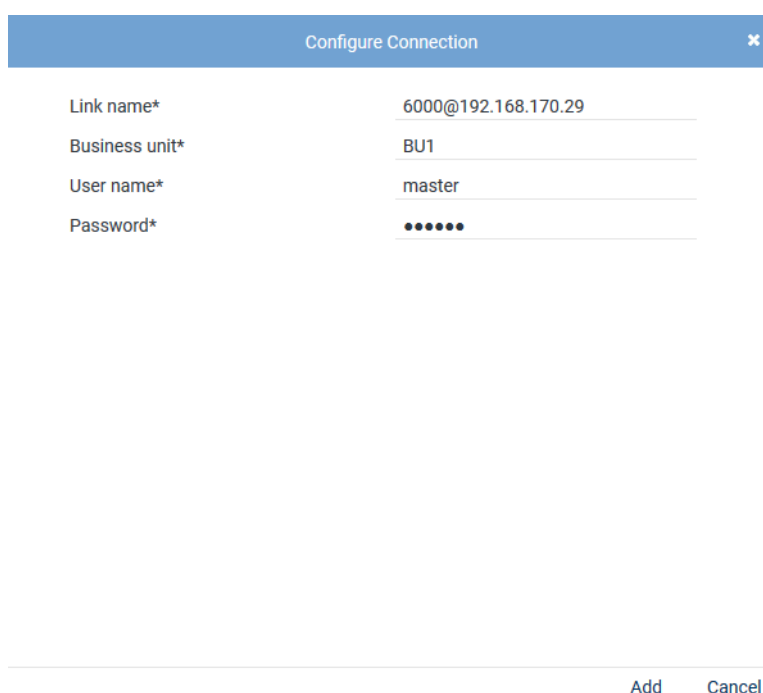


Fig. 412: Configure connection data

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 chapter "Create user for CTIconnect", p. 384 .
<i>Password</i>	Enter the password for the user of the business unit.

Tab. 111: 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.

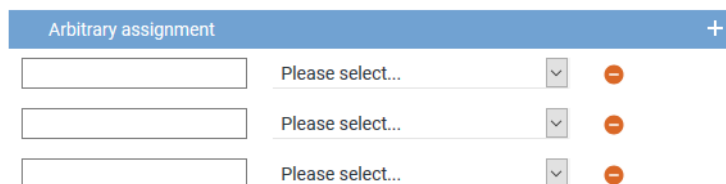




Fig. 413: Arbitrary assignment of the additional data

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 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

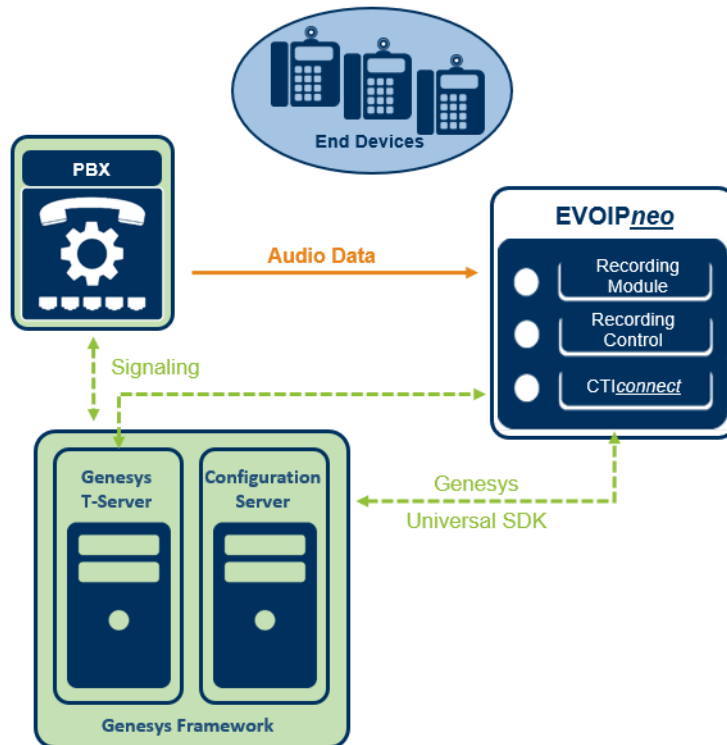


Fig. 414: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 384](#).

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*.

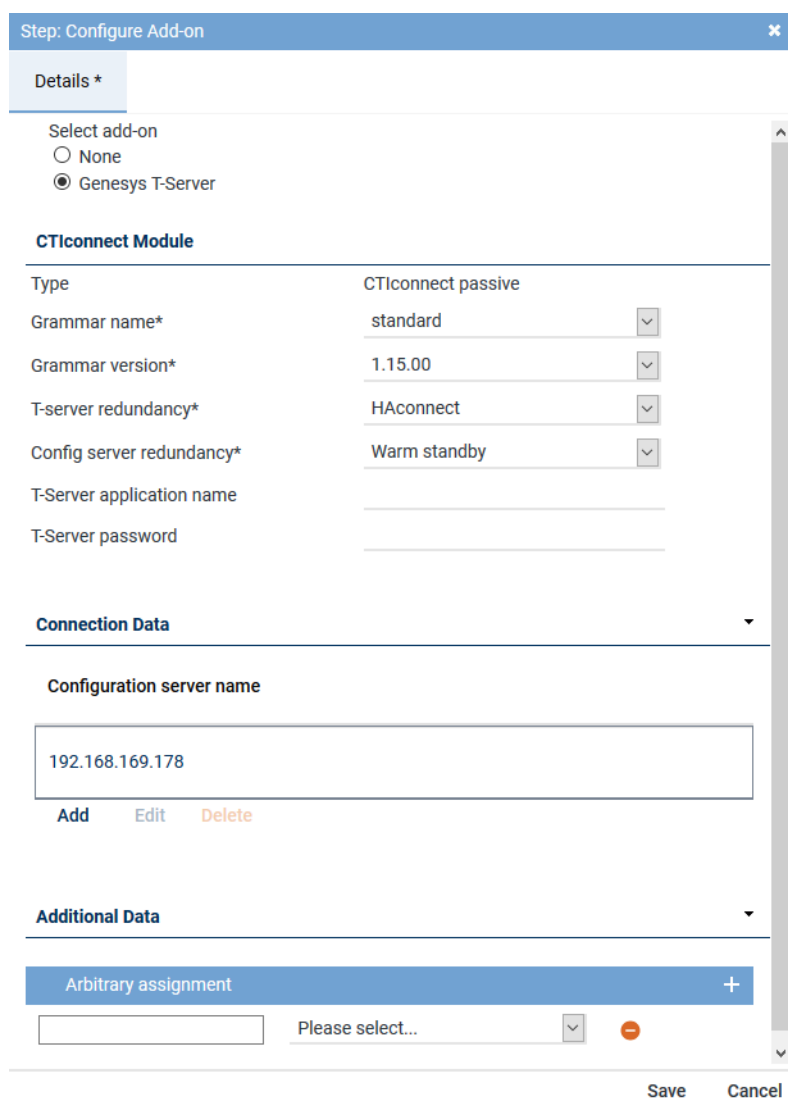


Fig. 415: Configure add-on for Genesys T-Server

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.

Parameter	Value/Description
	<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. 112: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

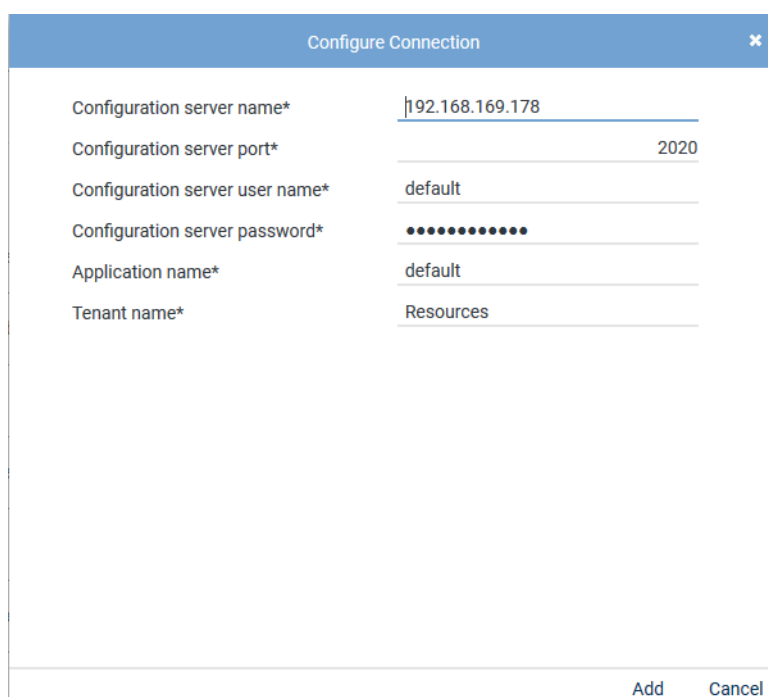


Fig. 416: Configure connection data

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.

Parameter	Value/Description
<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. 113: 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.

Arbitrary assignment			+
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖
<input type="text"/>	Please select...	▼	⊖

Fig. 417: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

▼

Save

Cancel

Fig. 418: Configure miscellaneous settings

2. 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*.

















+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		
Step		Configuration	
Configure recording architecture			
Global recording settings			
Configure recording servers			
Configure add-on			
Configure miscellaneous settings			

Fig. 419: Activate integration

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




+ × ⏮ ⏭ Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP active	SIP active		

Fig. 420: 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 active	SIP active		

Fig. 421: Deactivate integration

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

7.1.3 Synchronization options

There are 2 different types of synchronization:

- Synchronization of the Recording Control Service for recording control
- Synchronization of the system storage to compare recording data

7.1.3.1 Synchronization of recording control

Recording Control Services

For parallel recording servers installed in the same system architecture, you can configure synchronization of recording control.

ATTENTION!

Before the configuration, contact your ASC support to ensure that this function is suitable for your recording solution and to avoid a possible loss of recordings!

For information about which recording solutions support this function refer to the file [neo](#) Integration Overview.

If recording is supposed to be controlled manually by means of applications such as CLIENT-[command](#), PHONE[app](#), SCREEN[rec](#) scan Editor, or by external control, synchronization of the Recording Control Services of the parallel recording servers must be created.

Initially, the 1st Recording Control Service is responsible for recording control. The Recording Control Service ensures that the conversations of both recording servers are recorded.

If the 1st Recording Control Service fails, the 2nd Recording Control Service takes over recording control for both recording servers each of which then records the conversations.

Synchronization of recording control is configured in the Recording Architectures module. In parallel recording architectures, the check box *Synchronize recording control* appears in the tab *Details*.

1. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers.

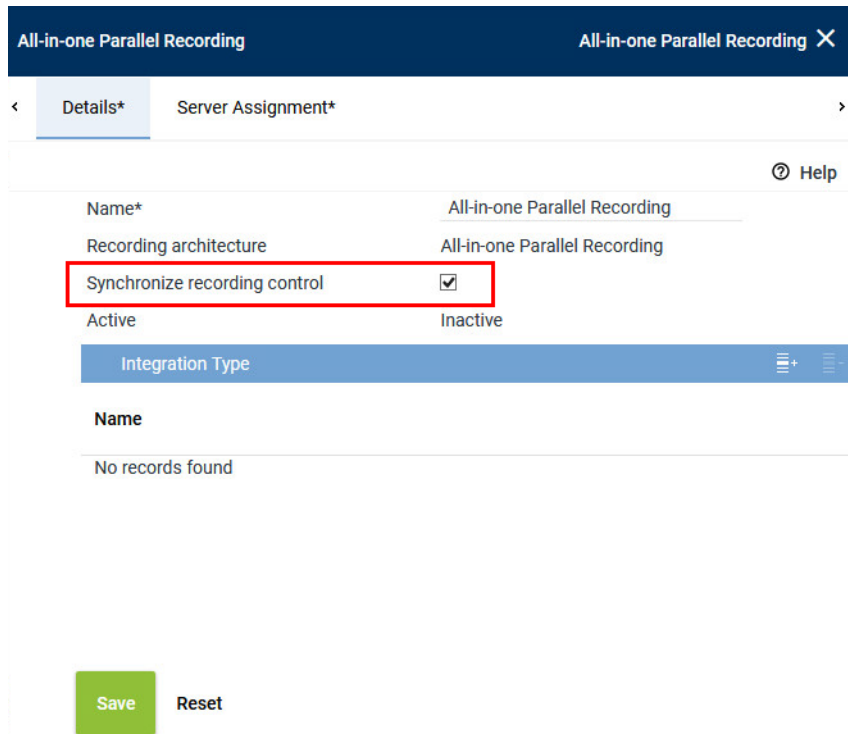


Fig. 422: Synchronize recording control

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



Synchronization of recording control brings stricter timeouts between the components. Observe the increased hardware and network requirements. Latency must be < 100 ms.

If you activate or deactivate this synchronization option subsequently, you must repeat the following configuration steps for the changes to take effect:

1. Select the required state of recording control:
 - ☒ = *Recording control is synchronized*
 - ☐ = *Recording control is not synchronized*
2. Deactivate the integration.
3. Deactivate the recording architecture.
4. Ensure that the following services have been stopped:
 - *ASC RecordingControl*
 - *ASC RecordingModule*
 - *ASC CTIconnect(integration name)*
5. Activate the recording architecture.

WARNING! In this status, all services have received the updated configuration but states may be conflicting.

Therefore, repeat the following steps:

6. Deactivate the recording architecture again.

7. Ensure that the services have been stopped.
 8. Activate the recording architecture again.
 9. Activate the integration.
- ⇒ The changes are now active.

7.1.3.2 Synchronization of system storage

In recording architectures with 2 system storages, you can configure synchronization to compare recordings.

A synchronization configuration is always created for 2 system storages. All recordings which are saved on one system storage are also copied to the other one and vice versa. That way, all recordings always exist on both system storages.



In a multi-core architecture, the system storage must not be synchronized between the Enterprise Cores.

Synchronization of the system storages is configured in the Servers module.

1. To create a synchronization configuration, click on the menu item *Servers > Manage Synchronization Configuration* in the toolbar of the main view.



Fig. 423: Menu item Manage Synchronization Configurations

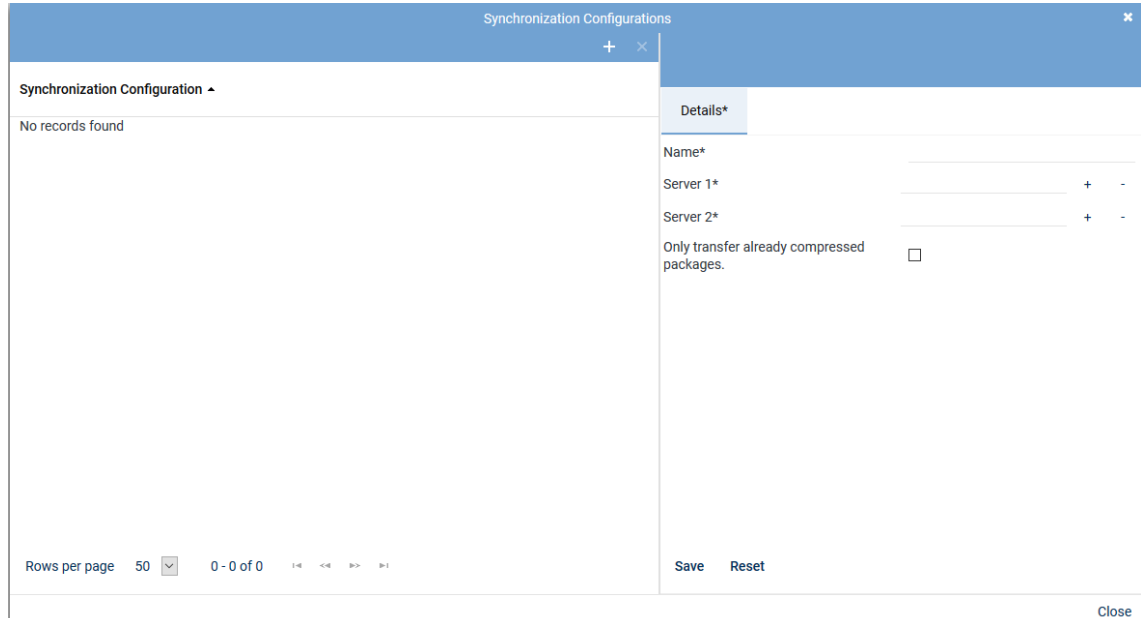




Fig. 424: Configure synchronization configurations

The following options are available:


	Create	Creates a new synchronization configuration, see chapter "Create synchronization configuration", p. 369 .
	Delete	Deletes the selected synchronization configuration, see chapter "Delete synchronization configuration", p. 369 .

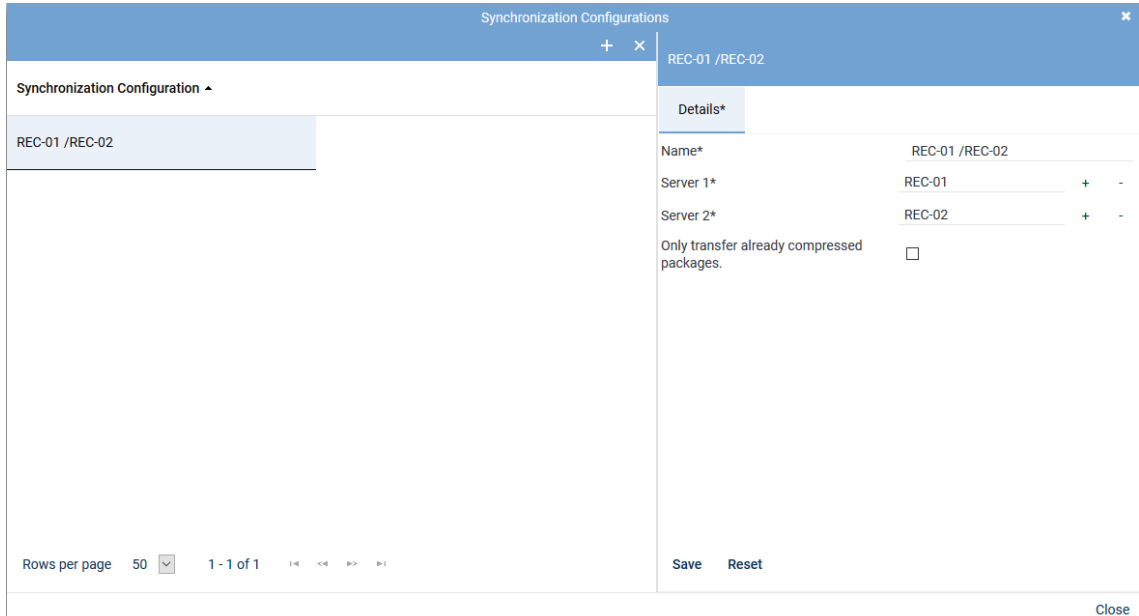
A synchronization configuration becomes active upon saving it and remains active until deleted. During this time, both system storages are regularly checked for new content and synchronized.



A server which is already used in a synchronization configuration cannot be used in another synchronization configuration.

7.1.3.2.1 Create synchronization configuration

- In the window *Administrate Synchronization Configuration*, click on the icon  (*Create*).
⇒ The tab *Details* becomes active.





The screenshot shows a window titled 'Synchronization Configurations'. On the left, a list shows 'REC-01 / REC-02' selected. The main area on the right is the 'Details*' tab for this configuration. It contains the following fields:

- Name***: REC-01 / REC-02
- Server 1***: REC-01 (with '+' and '-' buttons)
- Server 2***: REC-02 (with '+' and '-' buttons)
- Only transfer already compressed packages.**: ☐

At the bottom, there are 'Save' and 'Reset' buttons. A 'Close' button is located at the bottom right of the window.


Fig. 425: Create synchronization configuration

- Complete all fields for the new synchronization configuration:

Name	Enter a name for the synchronization configuration.
Server 1 / Server 2	<p>Click on the button  next to the entry field to select the respective server for the synchronization of the system storage from the list of available servers.</p> <p>If you would like to delete an entry in one of the entry fields, click on the button  next to the respective entry field.</p>
Only transfer already compressed packages	<p>Select whether data which has not yet been compressed is supposed to be transferred, too.</p> <p><input checked="" type="checkbox"/> = Uncompressed data is transferred, too.</p> <p><input type="checkbox"/> = Only compressed data is transferred.</p> <p>NOTICE! This option is not available until you have entered and saved the two servers.</p>

- Click on the button *Save* to apply the configuration.
- Click on the button *Close* to finish this configuration step and close the window.

7.1.3.2.2 Delete synchronization configuration

- In the window *Administrate synchronization configurations*, select the synchronization configuration you would like to delete.
- Click on the icon  (*Delete*) in the toolbar of the window.
⇒ The synchronization of the two entered system storages is finished.
⇒ The selected synchronization configuration is deleted.

7.1.4 Duplicates in parallel recording architectures



In parallel recording architectures in which recording control is synchronized, no duplicates are created which could be deleted. Both recordings are merged in one package and thus cannot be deleted separately. Keep in mind that more storage space must thus be available for the recordings.

A parallel recording without synchronization results in redundant recording data in the system. To avoid that conversations are displayed twice in the replay applications (e. g. *POWERplay Web*) because the database contains them twice, you can delete duplicates so that only one of the double recordings remains.

Conversations with the following characteristics are considered identical:

- Identical start and end times

You can define an allowed difference for the start and end times so that the conversations are still considered duplicates despite a differing start or end time, see [chapter "Configure duplicate detection", p. 370](#).

The start and end times of complete conversations as well as the start and end times of the individual recordings belonging to a conversation are checked.

- Identical call participants
- Identical additional data

Duplicate detection is configured in the Integrations module. There, you can configure for each integration individually under which circumstances conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings, see [chapter "Configure duplicate detection", p. 370](#).

The shorter one of the two identical recordings is deleted. To calculate the total recording length, the recording lengths of all sections of a conversation are added. The additional data as well as the audio data of the duplicate are deleted. On which of the two recording servers a duplicate is deleted thus depends on the location where the shorter recording has been saved. If the recording length is the same, the recording which has been checked second is considered a duplicate and deleted.

Duplicate detection is executed regularly for all new recordings from the moment on it has been activated but not for past recordings. This means Recordings which already exist when duplicate detection is activated are not checked for duplicates.



For information about the status of a job refer to the Jobs module in the application System Monitoring, see user manual *Usage System Monitoring*.



If you would like to delete duplicates but nevertheless want that all conversations exist on both recording servers, you can create a synchronization configuration in the Servers module which synchronizes the system storages of the two recording servers.

7.1.4.1 Configure duplicate detection

In the Integrations module, you can configure for each integration separately under which circumstances 2 conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings.

1. In the main view of the Integrations module, select the integration for which you would like to configure duplicate detection.
2. Select the tab *Parallel Recording* in the detail view and adjust the following settings:

Details*
Recording Content Validation
Parallel Recording

☒ Delete duplicates if the participants of the conversations are identical and the following criteria are met:
The start times differ in a maximum of Milliseconds
*
The end times differ in a maximum of Milliseconds
*
Additional settings
Time after which conversations are to be checked at the earliest * minutes
Interval in which the check is to take place * minutes

Additional Data

ID ↕
Displayed Name

No records found



Criteria to be Ignored

Available attributes	Ignored attributes
CHATIDENTIFIER	
DISPLAYNAME	
EMAILADDRESS	
EMPLOYEEID	
EXTENSION	
IPADDRESS	
MACADDRESS	
PBXAGENTID	
PBXID	

Save
Reset

Fig. 426: Tab Parallel Recording (integration)

<i>Delete duplicates,....</i>	<p>When activating this option, you can define by means of the displayed criteria when 2 recordings are supposed to be identified as identical.</p> <p><input checked="" type="checkbox"/> = Duplicate detection has been activated. Duplicates are deleted according to the defined criteria.</p> <p><input type="checkbox"/> = Duplicate detection has been deactivated.</p>
<i>The start times differ in a maximum of</i>	<p>Enter the maximum difference with regards to the start time. The start times of complete conversations as well as the start times of the individual recordings belonging to a conversation are checked.</p> <p>Example: <i>1000 milliseconds</i></p> <p>If one conversation started at 2:20:15 PM and a second conversation started at 2:20:16 PM, and if the start times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their start time.</p>
<i>The end times differ in a maximum of</i>	<p>Enter the maximum difference with regards to the end time. The end times of complete conversations as well as the end times of the individual recording sections belonging to a conversation are checked.</p> <p>Example: <i>1000 milliseconds</i></p> <p>If one conversation ended at 2:20:15 PM and a second conversation ended at 2:20:16 PM, and if the end times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their end time.</p>

<i>Time after which conversations are to be checked at the earliest</i>	<p>Enter the time interval which is supposed to pass before a recording is checked for duplicates.</p> <p>Example: <i>3 minutes</i></p> <p>If one conversation ended at 2:20 PM, i. e. the recording has been saved at 2:20 PM, then the recording is not check for duplicates before 2:23 PM.</p>
<i>Interval in which the check is to take place</i>	<p>Select the intervals in which the job for duplicate detection is supposed to be executed.</p> <p>Example: <i>2 minutes</i></p> <p>The job for duplicate detection is started over again every 2 minutes to search for new recordings and possible duplicates and to delete duplicates.</p>
<i>List Additional Data</i>	<p>Add all additional data to the list which are supposed to be used as criteria. When searching for duplicates, only those recordings are considered which contain an additional data type from the list. If an additional data type is empty in both conversations, this is considered identical, too, and one of the conversations is deleted.</p> <p> = Add additional data to the list, see chapter "Map additional data", p. 372.</p> <p> = Remove additional data from the list, see chapter "Delete additional data assignment", p. 373.</p>

- To save the settings, click on the button **Save**.
- ⇒ Upon activating the option *Delete duplicates...* the recordings are checked for duplicates and the detected duplicates are deleted.

7.1.4.2 Additional data

7.1.4.2.1 Map additional data

In addition to the start time and the end time, you can configure more additional data which is supposed to be used for checking for duplicates.

- In the list *Additional data*, click on the icon  (*Add*) to configure more additional data.

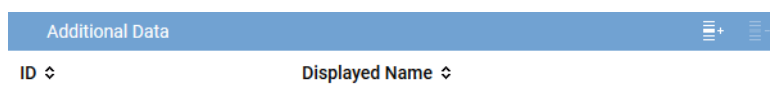


Fig. 427: Map additional data

- Select the respective additional data from the list which are supposed to be used additionally to check for duplicates.
To select several entries or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Additional Data ✕			
Displayed Name ↕	Available ↕	Editable ↕	External Recording Control ↕
Kommentar	✓	✓	✗
Universal Call ID	✓	✓	✗
<div> Rows per page 20 ▼ 1 - 2 of 2 ◀ << >> ▶ </div>			
			<div>Add Cancel</div>

Fig. 428: Select additional data


NOTICE! The list contains only additional data which have been configured in the Additional Data module previously.



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

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

7.1.4.2.2 Delete additional data assignment

- Select the tab *Parallel Recording*.
- Select the additional data that you would like to remove in the list *Additional Data*.
- Click on the icon  (*Delete*).

Additional Data ⋮ ⋮	
ID ↕	Displayed Name ↕
customCP01	Kommentar
customCP02	Universal Call ID

Fig. 429: Delete additional data assignment

7.1.4.3 Criteria to be ignored

In this group field, you can exclude certain criteria for duplicate detection which may prevent conversations to be detected as duplicates.

If conversations differ in just one attribute, they are not considered as duplicates. This holds true for conversations with different PBX IDs, for example.

To exclude this criterion during duplicate detection, add the respective attribute to the list of attributes which are supposed to be ignored.

In the list of available attributes, you can select which attributes are supposed to be excluded during duplicate detection. Click on the respective attributes and drag and drop them in the list of attributes to be ignored.

7.1.5 Standby management for failover architectures

For architectures with failover concepts, you can go to the standby management to manually select which server with which components is supposed to be active.

For architectures of the type *Parallel Recording*, you can also use the standby management if you have provided for the respective resources.

Using the standby management makes sense in the following cases:

- You would like to switch back to the primary server, e. g. when the standby server has automatically taken over and the primary server is now available again.
- You would like to switch to the standby server manually, e. g. during maintenance of the primary server.



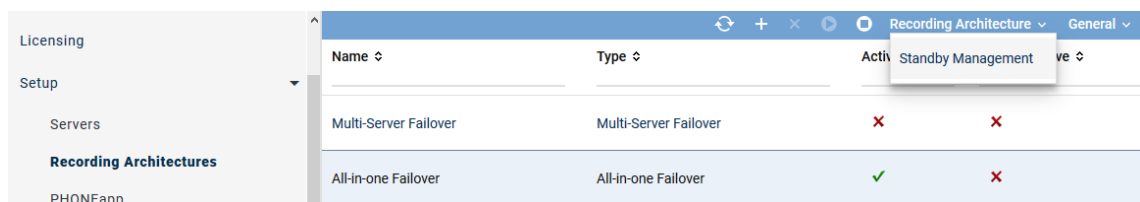
You can only edit the standby management if the corresponding architecture has been activated.

7.1.5.1 Standby management for All-in-one Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
 - ⇒ If the selected recording architecture has been activated, the menu item *Standby Management* is active.



			Recording Architecture ▾		General ▾	
Name ↕	Type ↕	Active	Standby Management	ve ↕		
Multi-Server Failover	Multi-Server Failover	✗	✗			
All-in-one Failover	All-in-one Failover	✓	✗			

Fig. 430: Configure standby management


3. Click on the menu item *Standby Management*.
 - ⇒ The window *Standby Management* appears.

Standby Management				
Server Name	Status	Oldest Running Activity	Running Activities	Version
RC - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.01.00
REC-02	In Standby		Activities: 0	
RIA - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.01.00
REC-02	In Standby		Activities: 0	
RM - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.00.00
REC-02	In Standby		Activities: 0	

Fig. 431: Switch server

Here, you see the assignment of the deployed components.

In the column *Status*, you can see which component is currently active.



- To activate a standby server, select the respective server in the list.
 - Click on the icon  (*Activate*) in the toolbar.
- ⇒ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server



This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

- To activate shutdown mode for a server, select the respective server in the list.
 - Click on the icon  (*Activate shutdown mode*) in the toolbar.
- ⇒ The status of the server changes from *Active* to *Shutdown Mode*.
- To deactivate shutdown mode again, click on the icon  in the toolbar again.
- ⇒ The status of the server changes from *Shutdown Mode* to *Active*.




In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

- To activate a standby server, select the respective server in the list.

2. Click on the icon  (*Activate*) in the toolbar.
- ⇒ The status of the standby server changes from *In Standby* to *Active*.
Only now can this server record new conversations.

7.1.5.2 Standby management for Multi-Server Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
 - ⇒ If the selected recording architecture has been activated, the menu item *Standby Management* is active.

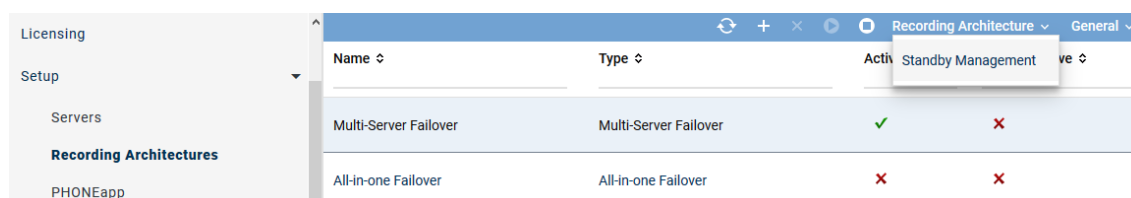


Fig. 432: Menu of the standby management

3. Click on the menu item *Standby Management*.
 - ⇒ The window *Standby Management* appears.

Standby Management				
Server Name	Status	Oldest Running Activity	Running Activities	Version
RC - RC-01 / RC-02				
RC-01	Active		Activities: 0	60.01.00
RC-02	In Standby		Activities: 0	60.00.00
RM - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.00.00
REC-02	In Standby		Activities: 0	
RIA - CTI-01 / CTI-02				
CTI-01	Active		Activities: 0	60.01.00
CTI-02	In Standby		Activities: 0	60.00.00

Fig. 433: Switch server

If you have installed the required redundancy options on different servers, you can use standby management for the following components:

- **RC** (*Recording Control Standby Management*) to secure recording control

- **RM** (*Recorder Standby Management*) to secure recording
- **RIA** (*CTIconnect Standby Management*) to secure the additional data of the recordings

Here, you see the assignment of the deployed components.

In the column *Status*, you can see which component is currently active.

4. To activate a standby server, select the respective server in the list.

5. Click on the icon  (*Activate*) in the toolbar.

⇒ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server




This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

1. To activate shutdown mode for a server, select the respective server in the list.

2. Click on the icon  (*Activate shutdown mode*) in the toolbar.

⇒ The status of the server changes from *Active* to *Shutdown Mode*.

3. To deactivate shutdown mode again, click on the icon  in the toolbar again.

⇒ The status of the server changes from *Shutdown Mode* to *Active*.



In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

1. To activate a standby server, select the respective server in the list.

2. Click on the icon  (*Activate*) in the toolbar.

⇒ The status of the standby server changes from *In Standby* to *Active*.

Only now can this server record new conversations.

7.1.6 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*.

- Open the group field *Audio Analysis*.

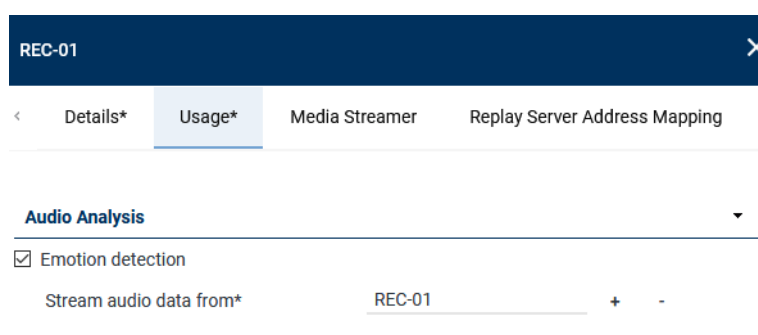


Fig. 434: Servers module - Activate emotion detection

- Activate the function *Emotion detection*.
- 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

- In the main view, select the integration for which you would like to check the validity of recording.
- Select the tab *Recording Content Validation*.

The following criteria are available to check proper recording:

- *Packet loss detection*
- *Decryption error detection*
- *Silence detection*

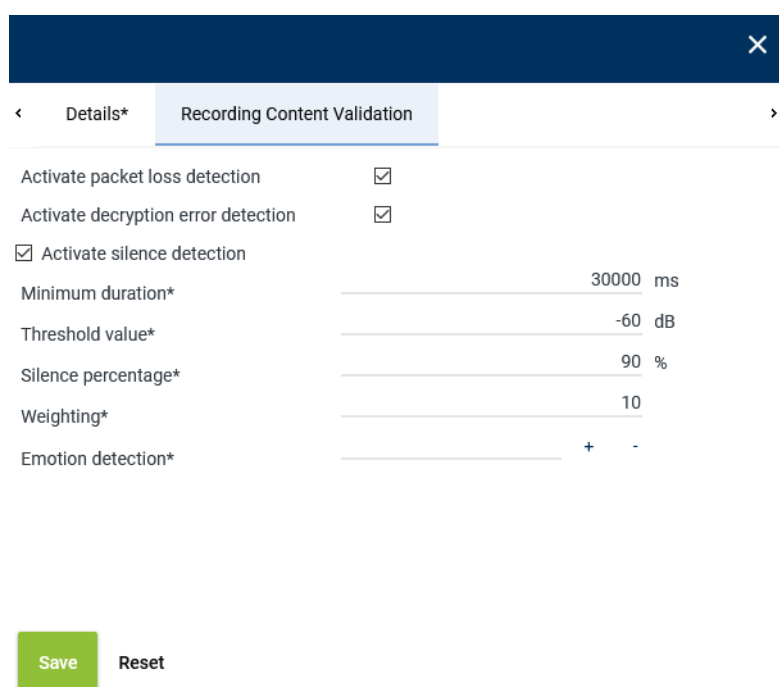



Fig. 435: Create integration - tab Recording Content Validation

Activate packet loss detection ☒ Activate the check box to check whether packets of a recording have been lost.

	NOTICE! Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	<input checked="" type="checkbox"/> Activate the check box to check whether errors occurred during decryption. NOTICE! Decryption errors result in noise which may corrupt the audio file.
Activate silence detection	<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! Detection is useful in case the PBX sends RTP packages which contain silence instead of an audio signal.
<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 smoothing factor defining to which extent the audio curves (samples) are supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 0-10000 can be recommended.
<i>Emotion detection server</i>	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.

- 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. 436: Select server for emotion detection

- 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.

7.1.7 Adjust neo configuration file

Some parameters cannot be configured via the graphic interface but have to be adjusted in the configuration files.

7.1.7.1 Adjust Recording Module for RTCP

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*.

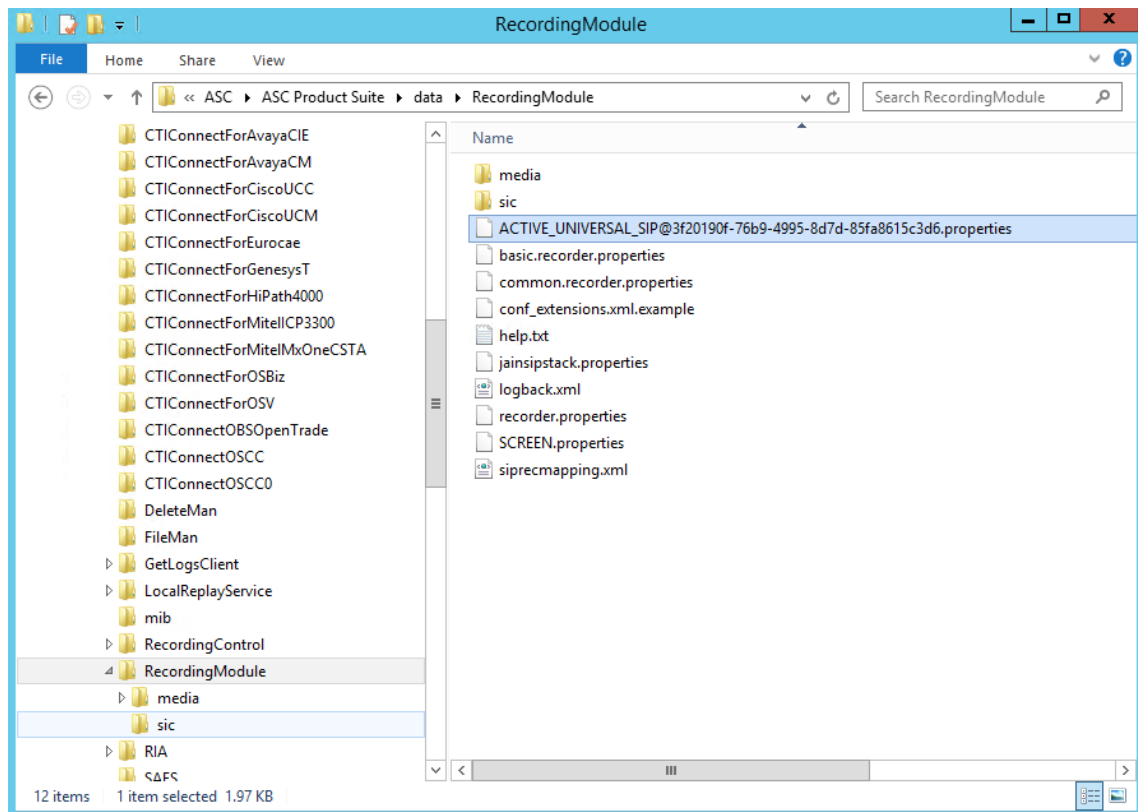


Fig. 437: Path to the configuration file

2. Open the file `ACTIVE_UNIVERSAL_SIP@<UUID>.properties` in the Editor.
3. Search for the entry `universalSip.rtpreceiver.portMode=`.
4. To enable the PBX to process **RTCP** data, you must supplement the parameter with the value `RTP_RTCP_PORTS`.
 - `universalSip.rtpreceiver.portMode=RTP_RTCP_PORTS`
5. Save the changes in the configuration file.
6. Restart the service *ASC RecordingModule* to apply the changes.

7.1.7.2 Configure recording announcement

If you would like to issue recording announcements, you have to adjust the configuration files of the Recording module.

1. Open the Windows Explorer.
2. Change to the installation directory `C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingModule`.

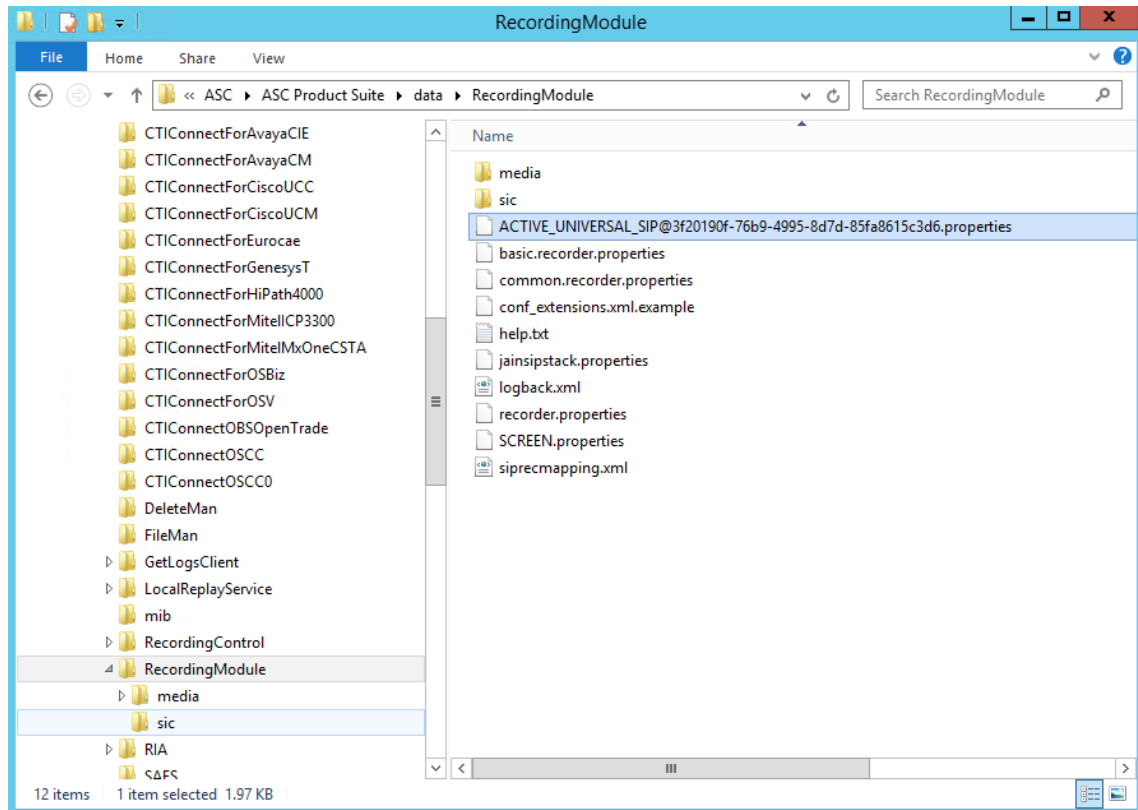


Fig. 438: Path to the configuration file

3. Open the file `ACTIVE_UNIVERSAL_SIP@<UUID>.properties` in the Editor.
4. Search for the section `# recording announcement`.

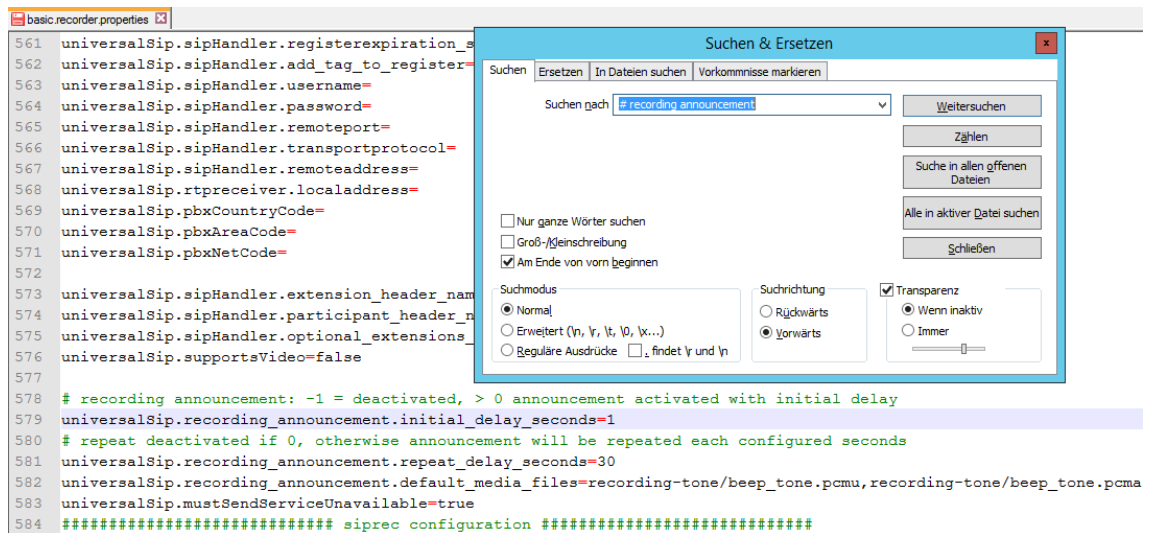


Fig. 439: Configure recording announcements

5. Configure the following parameters:

<code>universalSip.recording_announcement.initial_delay_seconds=</code>	-1 Deactivated; no announcements are issued. > 0 Activated; the announcement is issued with the configured delay.
<code>universalSip.recording_announcement.repeat_delay_seconds=</code>	0 Deactivated; the announcements are not repeated.

	> 0
	Activated; the announcement is repeated with the configured delay in seconds.
<i>universalSip.recording_announcement.default_media_files=</i>	<p>A list of default files which are issued in an announcement. The file extension indicated the codec that the file has been encoded with.</p> <p>The beep tone files in the directory <i>/recording-tone</i> have been pre-configured by default.</p> <ul style="list-style-type: none"> • beep_tone.g722 • beep_tone.g729 • beep_tone.pcma • beep_tone.pcmu

6. Save the changes in the configuration file and restart the service *ASC RecordingModule* so that the changes are applied.

Adjust announcement texts

Instead of the beep tones configured by default you can use announcement texts in different languages, too.

1. The default files of the announcement texts in different languages and the beep tones can be found in the following path:
C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingModule\media\default\.

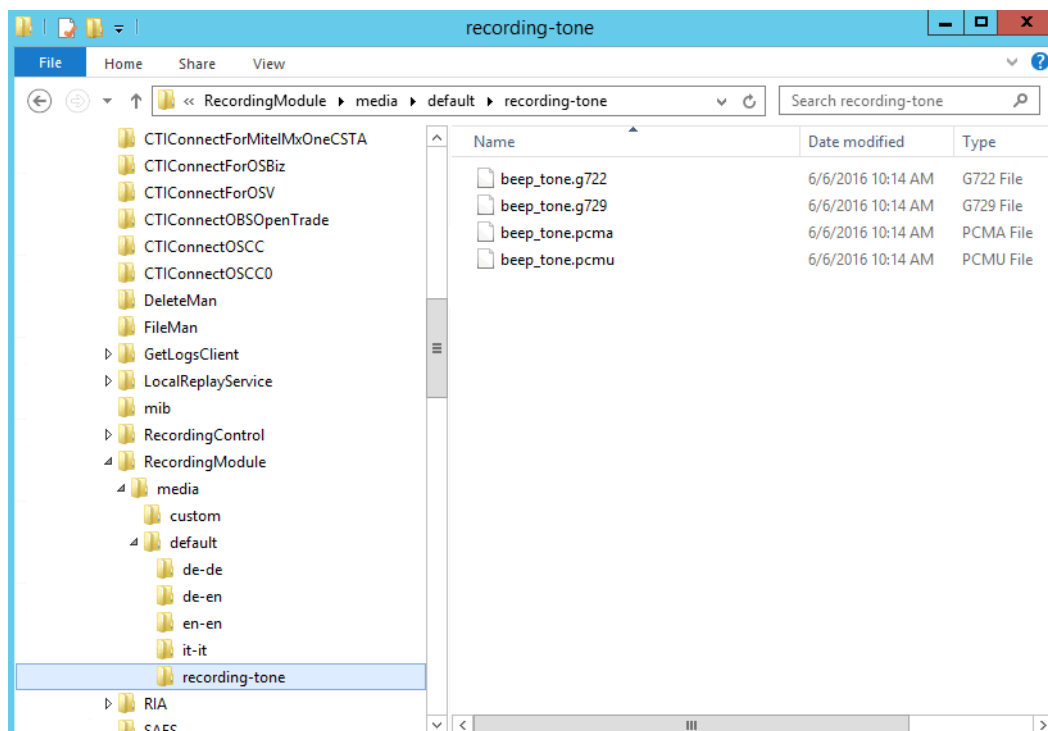


Fig. 440: Path of the default files

2. If you would like to use default texts in other languages, copy the files from the language-specific directory (e. g. */default/en-us*) directly into the directory */custom*. Do not use sub-directories. The files in the directory */custom* are preferred to the files in directory */default* and will not be overwritten in case of an update.
3. If you are using individual media files, deposit them in the directory */custom* as well. Observe that the file extension has to indicate the codec that the file has been encoded with.



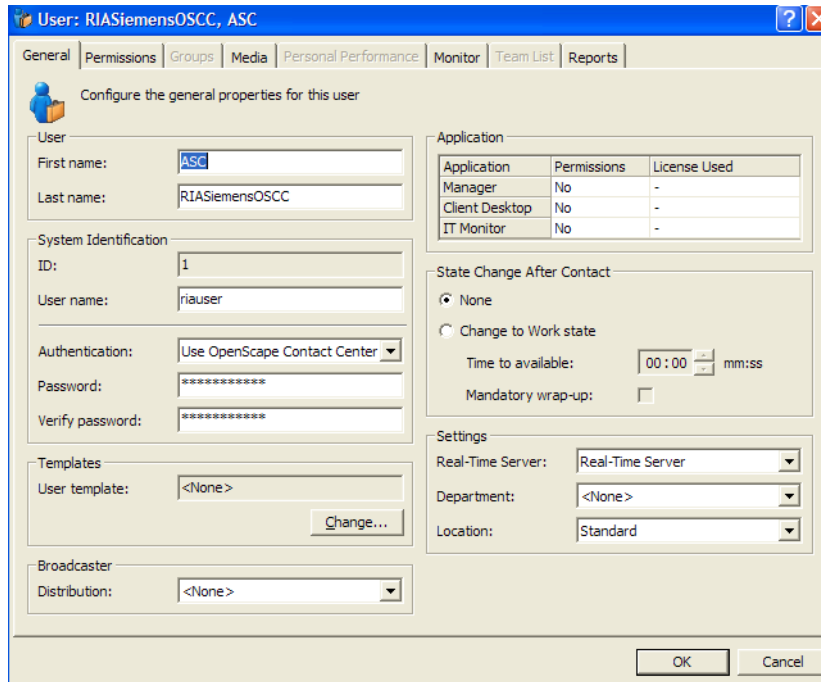
For further information about how to adjust the configuration files contact your local ASC support or call ASC support at +49 700 27278776.

7.2 Configure CTIconnect add-on

7.2.1 Configure OpenScope Contact Center (optional)

7.2.1.1 Create user for CTIconnect

Create a user in **OSCC** server administration.



Application	Permissions	License Used
Manager	No	-
Client Desktop	No	-
IT Monitor	No	-

Fig. 441: Create a user for CTIconnect service

This user does not need other special authorizations. All other settings can remain on default values.

7.2.2 Configure Genesys T-Server (optional)

7.2.2.1 Configure IP address and port of the Genesys T-Server

1. Log in to the Genesys Administrator.
2. Click on the menu item *Environment > Applications* in the navigation bar.

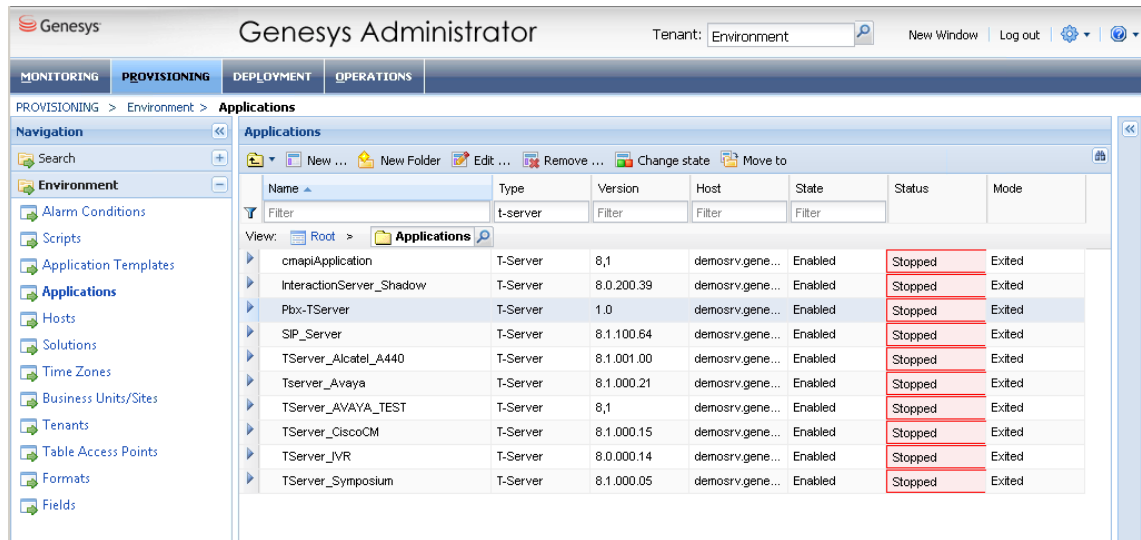


Fig. 442: Genesys Administrator - select T-Server

- 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*.

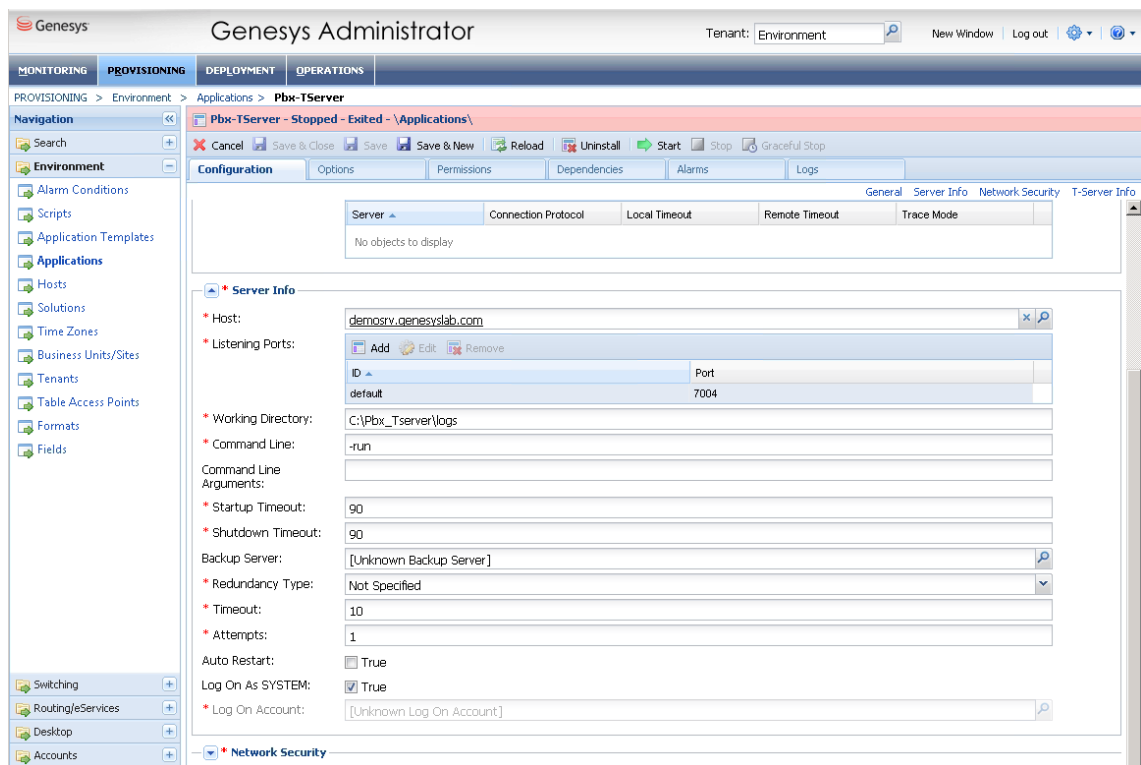


Fig. 443: Genesys Administrator - configure T-Server

- 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.

7.2.2.2 Configure IP address and port of the Genesys Configuration Server

- Click on the menu item *Environment > Applications* in the navigation bar.

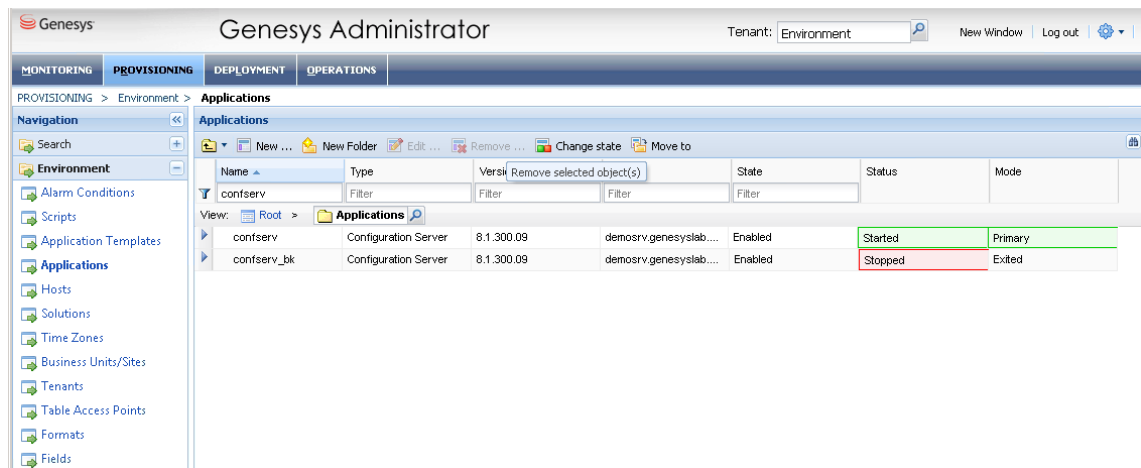


Fig. 444: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.
⇒ The window *Configuration* appears.
3. Expand the area *Server Info*.

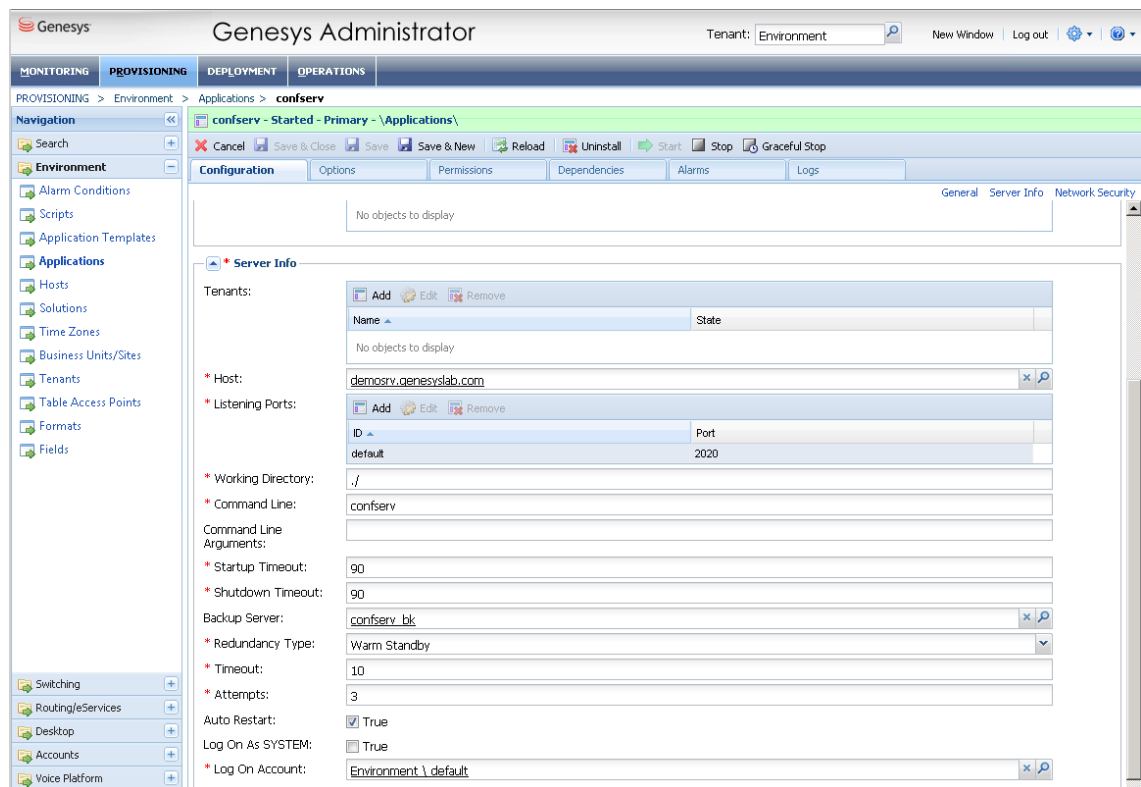


Fig. 445: Genesys Administrator - configure configuration server

4. In the field *Host*, enter the IP address or the computer name of the configuration server, e. g. *demosrv8.genesyslab.com*.
5. In the field *Listening Port*, enter the port of the configuration server, e. g. *2020*.

7.2.2.3 Configure switch instance in the Genesys Configuration Server

1. Click on the menu item *Switching > Switches* in the navigation bar.

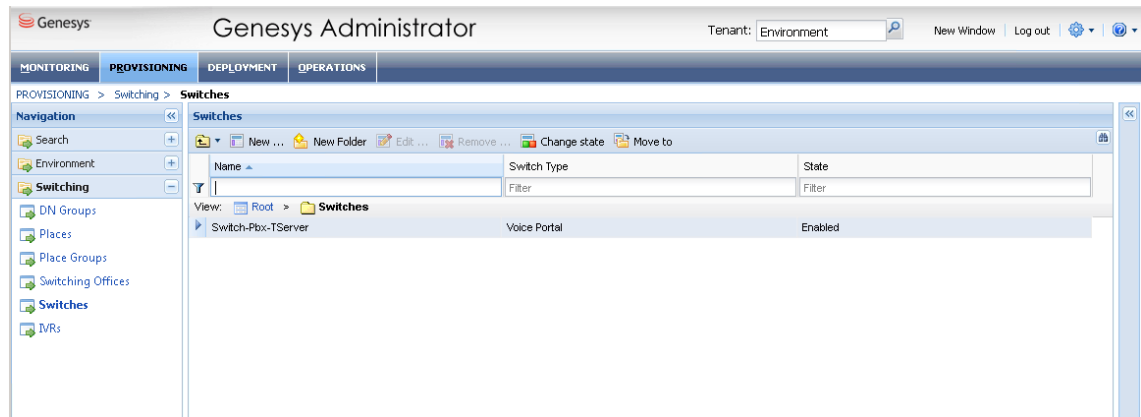


Fig. 446: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.
⇒ The window *Configuration > General* appears.

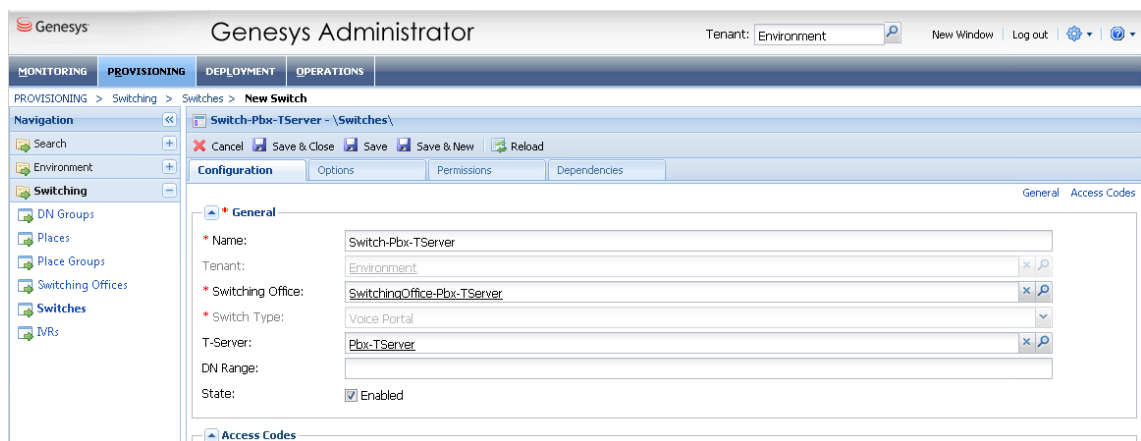


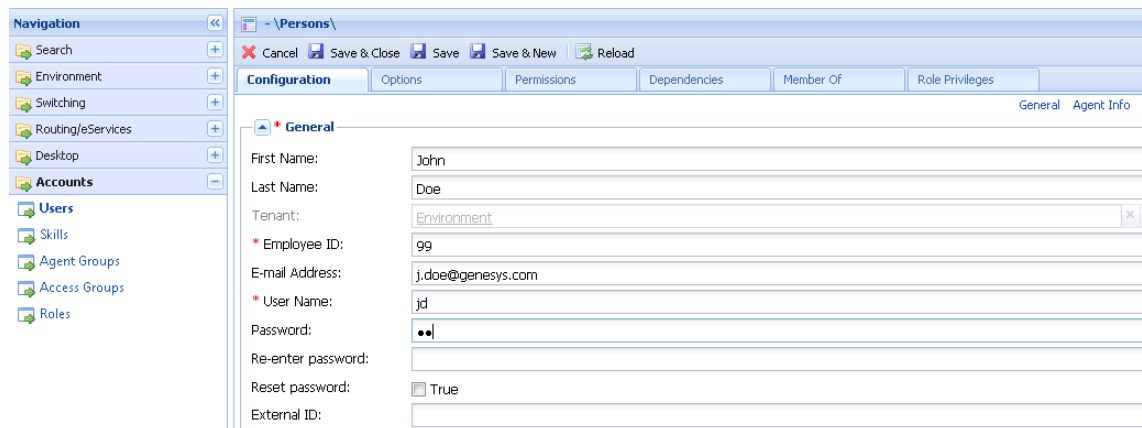
Fig. 447: Genesys Administrator - configure switch instance

3. Enter the same name in the configuration as in the Genesys T-Server.
4. Check whether the T-Server is identical to the T-Server configured in the Genesys T-Server.
5. Click on the button **Save** to save the entries.

7.2.2.4 Create users for the Genesys Configuration Server

To access the Genesys Configuration Server, you have to create a user.

1. Click on the menu item *Account > Users* in the navigation bar.
2. Click on the button **New**.
⇒ The window *Configuration > General* appears.



The screenshot displays the Genesys administrator interface for creating a new user. On the left, a 'Navigation' pane lists various system components. The main workspace is titled '- \Persons\' and contains a 'Configuration' tab. Within this tab, the 'General' sub-tab is active, showing a form for a user named 'John Doe'. The form includes fields for 'First Name', 'Last Name', 'Tenant' (set to 'Environment'), 'Employee ID' (99), 'E-mail Address' (j.doe@genesys.com), 'User Name' (jd), 'Password', 'Re-enter password', 'Reset password' (checkbox), and 'External ID'. The 'Password' field is masked with dots.

Fig. 448: 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 can be recorded, check:

- whether the transport protocol and the port have been configured correctly.
- that the PBX connection and the [SIP](#) authentication have been configured correctly and are active when the recording server has to register on the PBX.

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 the 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 and 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	Selection of the certificate.....	13
Fig. 3	Import certificate.....	13
Fig. 4	Confirm alias.....	14
Fig. 5	Message - Successful import.....	14
Fig. 6	Selection of the certificate.....	14
Fig. 7	Export PBX certificate from recording server.....	15
Fig. 8	System Configuration - web interface.....	17
Fig. 9	System Configuration - main view:.....	18
Fig. 10	Recording architectures - main view.....	19
Fig. 11	Toolbar Recording Architectures module.....	19
Fig. 12	Create recording architecture - All-in-one Basic Recording.....	21
Fig. 13	Recording architecture - tab Details.....	21
Fig. 14	Select integration type.....	22
Fig. 15	Recording architecture - tab Server Assignment.....	22
Fig. 16	Recording architecture - assign server.....	23
Fig. 17	Recording architecture - activate recording variant.....	23
Fig. 18	Recording architecture - activate recording architecture.....	24
Fig. 19	Servers - main view.....	24
Fig. 20	Toolbar Servers module.....	25
Fig. 21	Add server locations.....	26
Fig. 22	Delete server location.....	27
Fig. 23	Servers - tab Details.....	27
Fig. 24	Servers - tab usage.....	28
Fig. 25	Group field API Server.....	28
Fig. 26	Select storage expansion.....	30
Fig. 27	Group field Audio Analysis.....	30
Fig. 28	Select server for emotion detection.....	31
Fig. 29	Group field Recording Control/Key Management.....	31
Fig. 30	Group field Data Processing.....	32
Fig. 31	Select server.....	34
Fig. 32	Group field Replay.....	34
Fig. 33	Select server.....	36
Fig. 34	Group field Virtualization.....	36
Fig. 35	Servers module - tab Media Streamer.....	37
Fig. 36	Servers Module - tab Replay Server Address Mapping.....	39
Fig. 37	Servers module - tab Key Management.....	40
Fig. 38	Servers module - tab Keystore/Virtualization.....	42
Fig. 39	PBX module - main view.....	43
Fig. 40	Toolbar PBX module.....	43
Fig. 41	Create new PBX - tab Details.....	45

Fig. 42	Tenants - main view - tab Extensions	46
Fig. 43	Assign extensions to tenants	47
Fig. 44	Remove extensions.....	48
Fig. 45	Select extensions	49
Fig. 46	Additional Data module main view	49
Fig. 47	Configure additional data	50
Fig. 48	Additional data - configure availability	50
Fig. 49	Integrations - main view	51
Fig. 50	Toolbar Integrations module	51
Fig. 51	Create integration type	52
Fig. 52	Select PBX	53
Fig. 53	Assign recording architecture - All-in-one Basic	53
Fig. 54	Configuration steps of the integration	54
Fig. 55	Configuration step - Configure Recording Architecture.....	54
Fig. 56	Configuration step - Global Recording Settings	55
Fig. 57	Tab SIP Header Tagging Configure sources	56
Fig. 58	SIP Additional Data	57
Fig. 59	Configuration step - Configure recording servers	57
Fig. 60	Recording server - Configure extension for SIP trunk.....	58
Fig. 61	Tab Extensions	59
Fig. 62	Add extensions.....	59
Fig. 63	Added extensions.....	60
Fig. 64	Overview of Sparkassen FI ISP	61
Fig. 65	Configure add-on for Sparkassen FI ISP	62
Fig. 66	Arbitrary assignment of the additional data	63
Fig. 67	Configure add-on for OSCC	65
Fig. 68	Configure connection data	66
Fig. 69	Arbitrary assignment of the additional data	67
Fig. 70	Overview of the add on of Genesys T-Server	68
Fig. 71	Configure add-on for Genesys T-Server	69
Fig. 72	Configure connection data	70
Fig. 73	Arbitrary assignment of the additional data	72
Fig. 74	Configure miscellaneous settings	72
Fig. 75	Activate integration.....	73
Fig. 76	Activated integration.....	73
Fig. 77	Deactivate integration	74
Fig. 78	Recording architectures - main view	75
Fig. 79	Toolbar Recording Architectures module.....	75
Fig. 80	Create recording architecture - All-in-one Failover	76
Fig. 81	Recording architecture - tab Details - All-in-one Failover.....	77
Fig. 82	Select integration type.....	78
Fig. 83	Recording Architecture - tab Server Assignment	79

Fig. 84	Recording Architecture - assign server - example	79
Fig. 85	Recording Architecture - activate recording type	80
Fig. 86	Recording architecture - activate recording architecture.....	80
Fig. 87	Servers - main view.....	81
Fig. 88	Toolbar Servers module.....	81
Fig. 89	Add server locations.....	83
Fig. 90	Delete server location	84
Fig. 91	Servers - tab Details.....	84
Fig. 92	Servers - tab usage.....	85
Fig. 93	Group field API Server	85
Fig. 94	Select storage expansion.....	87
Fig. 95	Group field Audio Analysis.....	87
Fig. 96	Select server for emotion detection.....	88
Fig. 97	Group field Recording Control/Key Management	88
Fig. 98	Group field Data Processing	89
Fig. 99	Select server	91
Fig. 100	Group field Replay	91
Fig. 101	Select server	93
Fig. 102	Group field Virtualization.....	93
Fig. 103	Servers module - tab Media Streamer	94
Fig. 104	Servers Module - tab Replay Server Address Mapping.....	96
Fig. 105	Servers module - tab Key Management.....	97
Fig. 106	Servers module - tab Keystore/Virtualization	99
Fig. 107	PBX module - main view.....	100
Fig. 108	Toolbar PBX module	100
Fig. 109	Create new PBX - tab Details	102
Fig. 110	Tenants - main view - tab Extensions	103
Fig. 111	Assign extensions to tenants	104
Fig. 112	Remove extensions.....	105
Fig. 113	Select extensions	106
Fig. 114	Additional Data module main view.....	106
Fig. 115	Configure additional data	107
Fig. 116	Additional data - configure availability.....	107
Fig. 117	Integrations - main view	108
Fig. 118	Toolbar Integrations module	108
Fig. 119	Create integration type.....	109
Fig. 120	Select PBX.....	110
Fig. 121	Assign recording architecture - All-in-one Failover	110
Fig. 122	Configuration steps of the integration	111
Fig. 123	Configuration step - Configure Recording Architecture.....	111
Fig. 124	Configuration step - Global Recording Settings.....	112
Fig. 125	Tab SIP Header Tagging Configure sources	113

Fig. 126	SIP Additional Data	114
Fig. 127	Configuration step - Configure recording servers	115
Fig. 128	Recording server - Configure extension for SIP trunk.....	116
Fig. 129	Tab Extensions	116
Fig. 130	Add extensions.....	117
Fig. 131	Added extensions.....	118
Fig. 132	Overview of Sparkassen FI ISP	119
Fig. 133	Configure add-on for Sparkassen FI ISP	120
Fig. 134	Arbitrary assignment of the additional data.....	121
Fig. 135	Configure add-on for OSCC.....	123
Fig. 136	Configure connection data	124
Fig. 137	Arbitrary assignment of the additional data.....	125
Fig. 138	Overview of the add on of Genesys T-Server	126
Fig. 139	Configure add-on for Genesys T-Server	127
Fig. 140	Configure connection data	128
Fig. 141	Arbitrary assignment of the additional data.....	130
Fig. 142	Configure miscellaneous settings	130
Fig. 143	Activate integration.....	131
Fig. 144	Activated integration.....	131
Fig. 145	Deactivate integration	132
Fig. 146	Recording architectures - main view	133
Fig. 147	Toolbar Recording Architectures module.....	133
Fig. 148	Create recording architecture - All-in-one Parallel Recording	134
Fig. 149	Recording architecture - tab Details - All-in-one Parallel Recording	135
Fig. 150	Select integration type.....	136
Fig. 151	Recording Architecture - tab Server Assignment.....	137
Fig. 152	Recording Architecture - assign server - example	137
Fig. 153	Recording Architecture - activate recording type	138
Fig. 154	Activate recording architecture.....	138
Fig. 155	Servers - main view.....	139
Fig. 156	Toolbar Servers module.....	139
Fig. 157	Add server locations.....	141
Fig. 158	Delete server location	142
Fig. 159	Servers - tab Details.....	142
Fig. 160	Servers - tab usage.....	143
Fig. 161	Group field API Server	143
Fig. 162	Select storage expansion.....	145
Fig. 163	Group field Audio Analysis	145
Fig. 164	Select server for emotion detection.....	146
Fig. 165	Group field Recording Control/Key Management	146
Fig. 166	Group field Data Processing	147
Fig. 167	Select server	149

Fig. 168	Group field Replay	149
Fig. 169	Select server	151
Fig. 170	Group field Virtualization	151
Fig. 171	Servers module - tab Media Streamer	152
Fig. 172	Servers Module - tab Replay Server Address Mapping	154
Fig. 173	Servers module - tab Key Management.....	155
Fig. 174	Servers module - tab Keystore/Virtualization	157
Fig. 175	PBX module - main view	158
Fig. 176	Toolbar PBX module	158
Fig. 177	Create new PBX - tab Details	160
Fig. 178	Tenants - main view - tab Extensions	161
Fig. 179	Assign extensions to tenants	162
Fig. 180	Remove extensions.....	163
Fig. 181	Select extensions	164
Fig. 182	Additional Data module main view	164
Fig. 183	Configure additional data	165
Fig. 184	Additional data - configure availability	165
Fig. 185	Integrations - main view	166
Fig. 186	Toolbar Integrations module	166
Fig. 187	Create integration type	167
Fig. 188	Select PBX	168
Fig. 189	Assign recording architecture - All-in-one Parallel	168
Fig. 190	Configuration steps of the integration	169
Fig. 191	Configuration step - Configure Recording Architecture.....	169
Fig. 192	Configuration step - Global Recording Settings	170
Fig. 193	Configure device group 1	171
Fig. 194	Configure device group 2	171
Fig. 195	Tab SIP Header Tagging Configure sources	172
Fig. 196	SIP Additional Data	173
Fig. 197	Configuration step - Configure recording servers	174
Fig. 198	Recording server - Configure extension for SIP trunk.....	175
Fig. 199	Tab Extensions	176
Fig. 200	Add extensions.....	176
Fig. 201	Added extensions.....	177
Fig. 202	Overview of Sparkassen FI ISP	178
Fig. 203	Configure add-on for Sparkassen FI ISP	179
Fig. 204	Arbitrary assignment of the additional data.....	180
Fig. 205	Configure add-on for OSCC.....	182
Fig. 206	Configure connection data	183
Fig. 207	Arbitrary assignment of the additional data.....	184
Fig. 208	Overview of the add on of Genesys T-Server	185
Fig. 209	Configure add-on for Genesys T-Server	186

Fig. 210	Configure connection data	187
Fig. 211	Arbitrary assignment of the additional data	189
Fig. 212	Configure miscellaneous settings	189
Fig. 213	Activate integration.....	190
Fig. 214	Activated integration.....	190
Fig. 215	Deactivate integration	191
Fig. 216	Recording architectures - main view	192
Fig. 217	Toolbar Recording Architectures module	192
Fig. 218	Create recording architecture - Multi-Server Recording.....	193
Fig. 219	Recording architecture - tab Details - Multi-Server Recording.....	194
Fig. 220	Select integration type.....	195
Fig. 221	Recording architecture - tab Server Assignment	196
Fig. 222	Recording architecture - assign server - example.....	196
Fig. 223	Add recording server	197
Fig. 224	Recording architecture - activate recording architecture.....	198
Fig. 225	Servers - main view.....	199
Fig. 226	Toolbar Servers module.....	199
Fig. 227	Add server locations.....	200
Fig. 228	Delete server location	201
Fig. 229	Servers - tab Details.....	202
Fig. 230	Servers - tab usage	202
Fig. 231	Group field API Server	203
Fig. 232	Select storage expansion.....	204
Fig. 233	Group field Audio Analysis	205
Fig. 234	Select server for emotion detection.....	205
Fig. 235	Group field Recording Control/Key Management	205
Fig. 236	Group field Data Processing	206
Fig. 237	Select server	208
Fig. 238	Group field Replay	209
Fig. 239	Select server	210
Fig. 240	Group field Virtualization	211
Fig. 241	Servers module - tab Media Streamer	212
Fig. 242	Servers Module - tab Replay Server Address Mapping	214
Fig. 243	Servers module - tab Key Management.....	215
Fig. 244	Servers module - tab Keystore/Virtualization	217
Fig. 245	PBX module - main view	218
Fig. 246	Toolbar PBX module	218
Fig. 247	Create new PBX - tab Details	219
Fig. 248	Tenants - main view - tab Extensions	221
Fig. 249	Assign extensions to tenants	221
Fig. 250	Remove extensions.....	223
Fig. 251	Select extensions	223

Fig. 252	Additional Data module main view	224
Fig. 253	Configure additional data	224
Fig. 254	Additional data - configure availability	225
Fig. 255	Integrations - main view	226
Fig. 256	Toolbar Integrations module	226
Fig. 257	Create integration type	227
Fig. 258	Select PBX	227
Fig. 259	Assign recording architecture - Multi-Server Recording	228
Fig. 260	Configuration steps of the integration	228
Fig. 261	Configuration step - Configure Recording Architecture	229
Fig. 262	Configuration step - Global Recording Settings	229
Fig. 263	Tab SIP Header Tagging Configure sources	230
Fig. 264	SIP Additional Data	231
Fig. 265	Configuration step - Configure recording servers	232
Fig. 266	Recording server - Configure extension for SIP trunk	233
Fig. 267	Tab Extensions	234
Fig. 268	Add extensions	234
Fig. 269	Added extensions	235
Fig. 270	Overview of Sparkassen FI ISP	236
Fig. 271	Configure add-on for Sparkassen FI ISP	237
Fig. 272	Arbitrary assignment of the additional data	238
Fig. 273	Configure add-on for OSCC	240
Fig. 274	Configure connection data	241
Fig. 275	Arbitrary assignment of the additional data	242
Fig. 276	Overview of the add on of Genesys T-Server	243
Fig. 277	Configure add-on for Genesys T-Server	244
Fig. 278	Configure connection data	245
Fig. 279	Arbitrary assignment of the additional data	247
Fig. 280	Configure miscellaneous settings	247
Fig. 281	Activate integration	248
Fig. 282	Activated integration	248
Fig. 283	Deactivate integration	249
Fig. 284	Recording architectures - main view	250
Fig. 285	Toolbar Recording Architectures module	250
Fig. 286	Create recording architecture - Multi-Server Failover	251
Fig. 287	Recording architecture - tab Details - Multi-Server Failover	252
Fig. 288	Select integration type	253
Fig. 289	Recording Architecture - tab Server Assignment	254
Fig. 290	Recording Architecture - assign server - example	255
Fig. 291	Add Recording Server	256
Fig. 292	Recording architecture - activate recording architecture	257
Fig. 293	Servers - main view	257

Fig. 294	Toolbar Servers module	258
Fig. 295	Add server locations.....	259
Fig. 296	Delete server location	260
Fig. 297	Servers - tab Details.....	260
Fig. 298	Servers - tab usage	261
Fig. 299	Group field API Server	261
Fig. 300	Select storage expansion.....	263
Fig. 301	Group field Audio Analysis	263
Fig. 302	Select server for emotion detection.....	264
Fig. 303	Group field Recording Control/Key Management	264
Fig. 304	Group field Data Processing	265
Fig. 305	Select server	267
Fig. 306	Group field Replay	267
Fig. 307	Select server	269
Fig. 308	Group field Virtualization	269
Fig. 309	Servers module - tab Media Streamer	270
Fig. 310	Servers Module - tab Replay Server Address Mapping	272
Fig. 311	Servers module - tab Key Management.....	273
Fig. 312	Servers module - tab Keystore/Virtualization	275
Fig. 313	PBX module - main view	276
Fig. 314	Toolbar PBX module	276
Fig. 315	Create new PBX - tab Details	278
Fig. 316	Tenants - main view - tab Extensions	279
Fig. 317	Assign extensions to tenants	280
Fig. 318	Remove extensions.....	281
Fig. 319	Select extensions	282
Fig. 320	Additional Data module main view	282
Fig. 321	Configure additional data	283
Fig. 322	Additional data - configure availability	283
Fig. 323	Integrations - main view	284
Fig. 324	Toolbar Integrations module	284
Fig. 325	Choose file	285
Fig. 326	Upload grammar	285
Fig. 327	Create integration type.....	286
Fig. 328	Select PBX.....	286
Fig. 329	Assign recording architecture - Multi-Server Failover	287
Fig. 330	Configuration steps of the integration	287
Fig. 331	Configuration step - Configure Recording Architecture.....	288
Fig. 332	Configuration step - Global Recording Settings	288
Fig. 333	Tab SIP Header Tagging Configure sources	289
Fig. 334	SIP Additional Data	290
Fig. 335	Configuration step - Configure recording servers	291

Fig. 336	Recording server - Configure extension for SIP trunk.....	292
Fig. 337	Tab Extensions	292
Fig. 338	Add extensions.....	293
Fig. 339	Added extensions.....	294
Fig. 340	Overview of Sparkassen FI ISP	295
Fig. 341	Configure add-on for Sparkassen FI ISP	296
Fig. 342	Arbitrary assignment of the additional data	297
Fig. 343	Configure add-on for OSCC.....	299
Fig. 344	Configure connection data	300
Fig. 345	Arbitrary assignment of the additional data.....	301
Fig. 346	Overview of the add on of Genesys T-Server	302
Fig. 347	Configure add-on for Genesys T-Server	303
Fig. 348	Configure connection data	304
Fig. 349	Arbitrary assignment of the additional data.....	306
Fig. 350	Configure miscellaneous settings	306
Fig. 351	Activate integration.....	307
Fig. 352	Activated integration.....	307
Fig. 353	Deactivate integration	308
Fig. 354	Recording architectures - main view	309
Fig. 355	Toolbar Recording Architectures module.....	309
Fig. 356	Create recording architecture - Multi-Server Parallel Recording.....	310
Fig. 357	Recording architecture - tab Details - Multi-Server Parallel Recording.....	311
Fig. 358	Select integration type.....	312
Fig. 359	Recording architecture - server assignment device group 1	313
Fig. 360	Recording architecture - assign server - example.....	313
Fig. 361	Add recording server	314
Fig. 362	Recording architecture - activate recording architecture - example.....	315
Fig. 363	Servers - main view.....	316
Fig. 364	Toolbar Servers module.....	316
Fig. 365	Add server locations.....	317
Fig. 366	Delete server location	318
Fig. 367	Servers - tab Details.....	319
Fig. 368	Servers - tab usage.....	319
Fig. 369	Group field API Server	320
Fig. 370	Select storage expansion.....	321
Fig. 371	Group field Audio Analysis	322
Fig. 372	Select server for emotion detection.....	322
Fig. 373	Group field Recording Control/Key Management	322
Fig. 374	Group field Data Processing	323
Fig. 375	Select server	325
Fig. 376	Group field Replay	326
Fig. 377	Select server	327

Fig. 378	Group field Virtualization	328
Fig. 379	Servers module - tab Media Streamer	329
Fig. 380	Servers Module - tab Replay Server Address Mapping	331
Fig. 381	Servers module - tab Key Management.....	332
Fig. 382	Servers module - tab Keystore/Virtualization	334
Fig. 383	PBX module - main view	335
Fig. 384	Toolbar PBX module	335
Fig. 385	Create new PBX - tab Details	336
Fig. 386	Tenants - main view - tab Extensions	338
Fig. 387	Assign extensions to tenants	338
Fig. 388	Remove extensions.....	340
Fig. 389	Select extensions	340
Fig. 390	Additional Data module main view	341
Fig. 391	Configure additional data	341
Fig. 392	Additional data - configure availability	342
Fig. 393	Integrations - main view	343
Fig. 394	Toolbar Integrations module	343
Fig. 395	Create integration type	344
Fig. 396	Select PBX	344
Fig. 397	Assign recording architecture - Multi-Server Parallel	345
Fig. 398	Configuration steps of the integration	345
Fig. 399	Configuration step - Configure Recording Architecture.....	346
Fig. 400	Configuration step - Global Recording Settings - Multi-Server Parallel Recording .	346
Fig. 401	Tab SIP Header Tagging Configure sources	347
Fig. 402	SIP Additional Data	348
Fig. 403	Configuration step - Configure recording servers	349
Fig. 404	Recording server - Configure extension for SIP trunk.....	350
Fig. 405	Tab Extensions	351
Fig. 406	Add extensions.....	351
Fig. 407	Added extensions.....	352
Fig. 408	Overview of Sparkassen FI ISP	353
Fig. 409	Configure add-on for Sparkassen FI ISP	354
Fig. 410	Arbitrary assignment of the additional data	355
Fig. 411	Configure add-on for OSCC	357
Fig. 412	Configure connection data	358
Fig. 413	Arbitrary assignment of the additional data	359
Fig. 414	Overview of the add on of Genesys T-Server	360
Fig. 415	Configure add-on for Genesys T-Server	361
Fig. 416	Configure connection data	362
Fig. 417	Arbitrary assignment of the additional data	364
Fig. 418	Configure miscellaneous settings	364
Fig. 419	Activate integration.....	365

Fig. 420	Activated integration.....	365
Fig. 421	Deactivate integration	366
Fig. 422	Synchronize recording control.....	367
Fig. 423	Menu item Manage Synchronization Configurations.....	368
Fig. 424	Configure synchronization configurations	368
Fig. 425	Create synchronization configuration.....	369
Fig. 426	Tab Parallel Recording (integration)	371
Fig. 427	Map additional data	372
Fig. 428	Select additional data.....	373
Fig. 429	Delete additional data assignment.....	373
Fig. 430	Configure standby management.....	374
Fig. 431	Switch server.....	375
Fig. 432	Menu of the standby management.....	376
Fig. 433	Switch server.....	376
Fig. 434	Servers module - Activate emotion detection.....	378
Fig. 435	Create integration - tab Recording Content Validation.....	378
Fig. 436	Select server for emotion detection.....	379
Fig. 437	Path to the configuration file.....	381
Fig. 438	Path to the configuration file.....	382
Fig. 439	Configure recording announcements	382
Fig. 440	Path of the default files.....	383
Fig. 441	Create a user for CTIconnect service	384
Fig. 442	Genesys Administrator - select T-Server	385
Fig. 443	Genesys Administrator - configure T-Server.....	385
Fig. 444	Genesys Administrator - select configuration server.....	386
Fig. 445	Genesys Administrator - configure configuration server	386
Fig. 446	Genesys Administrator - switch instances	387
Fig. 447	Genesys Administrator - configure switch instance	387
Fig. 448	Genesys administrator - create user	388

List of tables

Tab. 1	Licenses of ASC.....	9
Tab. 2	Licenses for OpenScape Contact Center optional	9
Tab. 3	Licenses for Sparkassen FI ISP optional	9
Tab. 4	Licenses for Genesys.....	9
Tab. 5	Login data - system provider.....	17
Tab. 6	Configure audio analysis.....	30
Tab. 7	Configure recording control/key management	31
Tab. 8	Data storage.....	32
Tab. 9	Configure replay.....	34
Tab. 10	Configure virtualization.....	36
Tab. 11	Create PBX	45
Tab. 12	PBX parameters with complete phone number.....	46
Tab. 13	Create integration type.....	52
Tab. 14	Global recording settings	55
Tab. 15	Configure SIP header tagging.....	56
Tab. 16	Configure SIP conversation parameters	57
Tab. 17	Configure recording servers.....	58
Tab. 18	Configure CTIconnect module	62
Tab. 19	Configure connection data	63
Tab. 20	Configure CTIconnect module	65
Tab. 21	Configure connection data	66
Tab. 22	Configure add-on for Genesys T-Server	69
Tab. 23	Configure connection data	70
Tab. 24	Configure audio analysis.....	87
Tab. 25	Configure recording control/key management	88
Tab. 26	Data storage.....	89
Tab. 27	Configure replay.....	91
Tab. 28	Configure virtualization.....	93
Tab. 29	Create PBX	102
Tab. 30	PBX parameters with complete phone number.....	103
Tab. 31	Create integration type.....	109
Tab. 32	Global recording settings	112
Tab. 33	Configure SIP header tagging.....	113
Tab. 34	Configure SIP conversation parameters	114
Tab. 35	Configure recording servers.....	115
Tab. 36	Configure CTIconnect module	120
Tab. 37	Configure connection data	121
Tab. 38	Configure CTIconnect module	123
Tab. 39	Configure connection data	124
Tab. 40	Configure add-on for Genesys T-Server	127
Tab. 41	Configure connection data	128

Tab. 42	Configure audio analysis.....	145
Tab. 43	Configure recording control/key management	146
Tab. 44	Data storage.....	147
Tab. 45	Configure replay.....	149
Tab. 46	Configure virtualization.....	151
Tab. 47	Create PBX	160
Tab. 48	PBX parameters with complete phone number.....	161
Tab. 49	Create integration type	167
Tab. 50	Global recording settings	170
Tab. 51	Configure SIP header tagging.....	172
Tab. 52	Configure SIP conversation parameters	173
Tab. 53	Configure recording servers.....	174
Tab. 54	Configure CTIconnect module	179
Tab. 55	Configure connection data	180
Tab. 56	Configure CTIconnect module	182
Tab. 57	Configure connection data	183
Tab. 58	Configure add-on for Genesys T-Server	186
Tab. 59	Configure connection data	187
Tab. 60	Configure audio analysis.....	205
Tab. 61	Configure recording control/key management	206
Tab. 62	Data storage.....	207
Tab. 63	Configure replay.....	209
Tab. 64	Configure virtualization.....	211
Tab. 65	Create PBX	219
Tab. 66	PBX parameters with complete phone number.....	220
Tab. 67	Create integration type	227
Tab. 68	Global recording settings	229
Tab. 69	Configure SIP header tagging.....	230
Tab. 70	Configure SIP conversation parameters	231
Tab. 71	Configure recording servers.....	232
Tab. 72	Configure CTIconnect module	237
Tab. 73	Configure connection data	238
Tab. 74	Configure CTIconnect module	240
Tab. 75	Configure connection data	241
Tab. 76	Configure add-on for Genesys T-Server	244
Tab. 77	Configure connection data	245
Tab. 78	Configure audio analysis.....	263
Tab. 79	Configure recording control/key management	264
Tab. 80	Data storage.....	265
Tab. 81	Configure replay.....	267
Tab. 82	Configure virtualization.....	269
Tab. 83	Create PBX	278

Tab. 84	PBX parameters with complete phone number.....	279
Tab. 85	Create integration type.....	286
Tab. 86	Global recording settings	288
Tab. 87	Configure SIP header tagging.....	289
Tab. 88	Configure SIP conversation parameters	290
Tab. 89	Configure recording servers.....	291
Tab. 90	Configure CTIconnect module	296
Tab. 91	Configure connection data	297
Tab. 92	Configure CTIconnect module	299
Tab. 93	Configure connection data	300
Tab. 94	Configure add-on for Genesys T-Server	303
Tab. 95	Configure connection data	304
Tab. 96	Configure audio analysis.....	322
Tab. 97	Configure recording control/key management	323
Tab. 98	Data storage.....	324
Tab. 99	Configure replay.....	326
Tab. 100	Configure virtualization.....	328
Tab. 101	Create PBX	336
Tab. 102	PBX parameters with complete phone number.....	337
Tab. 103	Create integration type.....	344
Tab. 104	Global recording settings	347
Tab. 105	Configure SIP header tagging.....	347
Tab. 106	Configure SIP conversation parameters	348
Tab. 107	Configure recording servers.....	349
Tab. 108	Configure CTIconnect module	354
Tab. 109	Configure connection data	355
Tab. 110	Configure CTIconnect module	357
Tab. 111	Configure connection data	358
Tab. 112	Configure add-on for Genesys T-Server	361
Tab. 113	Configure connection data	362

Glossary

API

Application Programming Interface

API server

Server on which the API service runs. (API=Application Programming Interface)

Digest Authentication

In Digest Access Authentication (also RFC 2617) the server sends a random string of characters (nonce) created specifically for this purpose along with the WWW-Authenticate-Header. The browser calculates the hashcode (usually MD5) of a combination of user name, password, contained string of characters, HTTP method, and requested URI. It sends it back to the server in the authentication header along with the user name and the random string of characters. The server then calculates the hash total for comparison purposes. This method resembles Message Authentication Code. Provided that the used hash function is safe in terms of the cryptographic construction, attackers do not profit from sniffing the communication since the hash function prevents a reconstruction of the access data and because the access data are different for the next request due to using a nonce. (Especially the widespread hash function MD5 is not considered safe anymore.) The remaining data transmission is not protected, though. To achieve this Hypertext Transfer Protocol Secure (HTTPS) can be used. Translation of the German-language source: Wikipedia (20/02/2017)

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

OSCC

OpenScape Contact Center

PBX

Private Branch Exchange

RTCP

The Real Time Control Protocol provides feedback on the quality of service (QoS) in media distribution by periodically exchanging control messages between sender and recipient. The Real Time Control Protocol is used together with the Real Time Streaming Protocol (RTSP) which is responsible for controlling the transfer and with the Real Time Transport Protocol (RTP) which is responsible for the transfer itself.

RTP

Real-time Transport Protocol is a protocol to continuously transmit audio and video files via the IP protocol within the network.

SDES

Session Description Protocol Security Descriptions

SDK

Software Development Kit

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

SMS

Short Message Service, text message (GSM, landline)

SRTP

Secure real-time 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