

EVOIPneo active for Noetica Outbound Dialer Integration



Administration manual for system providers

3/31/2021

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	4
2	Introduction	5
3	System requirements.....	6
3.1	Hardware components	6
3.1.1	Recorder	6
3.2	Software components	6
3.3	External components	6
3.3.1	Supported PBXs and end devices	6
4	Installation requirements	8
4.1	Licenses	8
4.2	Information	8
5	Overview of how to install and configure the product	9
6	Installation	10
7	Configuration.....	11
7.1	System Configuration.....	11
7.1.1	Start application	11
7.1.2	Configure recording solution	12
7.1.2.1	Configure recording solution All-in-one Basic	12
7.1.2.2	Configure recording solution All-in-one Parallel Recording.....	52
7.1.2.3	Configure recording solution Multi-Server Recording	91
7.1.2.4	Configure recording solution Multi-Server Parallel Recording	130
7.1.3	Duplicates in parallel recording architectures	170
7.1.3.1	Configure duplicate detection.....	171
7.1.3.2	Additional data	173
7.1.3.3	Criteria to be ignored.....	174
7.1.4	Configure Recording Content Validation	174
7.1.5	Adjust neo configuration file	177
7.1.5.1	Adjust Recording module	177
7.1.5.2	Copy ASC.ScenarioConfig.Noetica.xml	179
8	Troubleshooting.....	180
	List of figures	181
	List of tables	187
	Glossary.....	188

1 General information

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

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

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

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

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

The conversations run via the NVP.

The Noetica Voice platform is connected to the recording server via a nailed-up connection. For every agent logging in to the Noetica Voice platform a nailed-up connection to the recording server is established. Via the API the NVP controls the recording and delivers the metadata.

This recording solution also supports a parallel recording architecture. In an All-in-one Parallel Recording recording architecture, all nailed-up and API connections are established twice.



In this recording solution, the conversations are saved as mixed data stream in mono mode.

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.

Noetica Dialer Integration

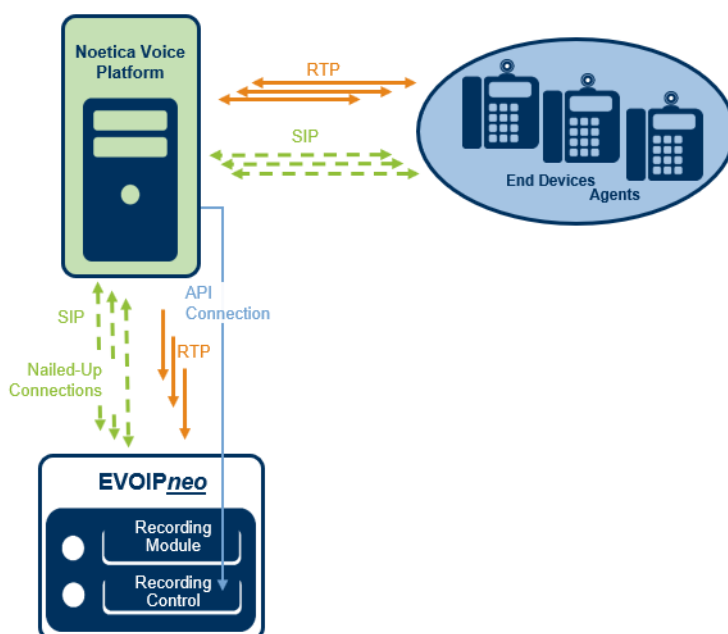


Fig. 1: Overview of the recording solution

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 Noetica Outbound Dialer	1 license per concurrent recording

Tab. 1: Licenses of ASC

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 of how to install and configure the product

The following steps have to be taken:

1. Install neo software
2. Configure Noetica Voice platform
 - As the configuration is manufacturer-specific it cannot be described here. A telecommunication engineer usually takes care of the configuration.
3. Configure System Configuration
 - Create and activate recording architectures
 - The recording servers, recording types, and the integration types are assigned in the Recording Architectures module.
 - Configure servers
 - In the Servers module, the usage of the server is configured.
A server can be used for archiving, import, export, replay, data storage or for audio analysis.
 - Create PBX
 - A PBX configuration can either be created via the PBX module or via the configuration in the Integrations module.
 - Configure additional data
 - In the Additional Data module, you can map the additional data to a customCP field..
 - 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.
 - Adjust neo configuration files
 - Adjust Recording module
 - Copy and rename ASC.ScenarioConfig.Noetica.xml

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*.

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.

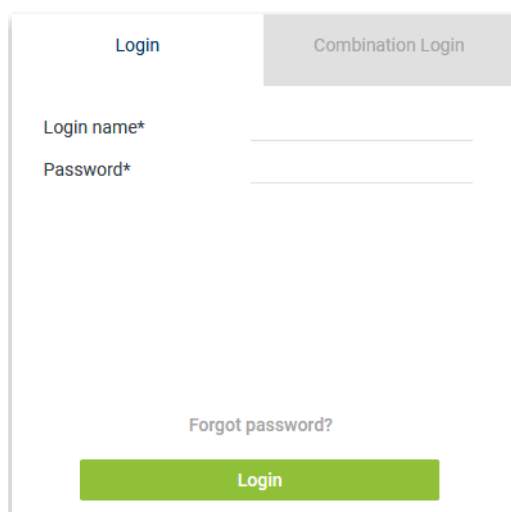


Fig. 2: System Configuration - web interface

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. 2: Login data - system provider

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

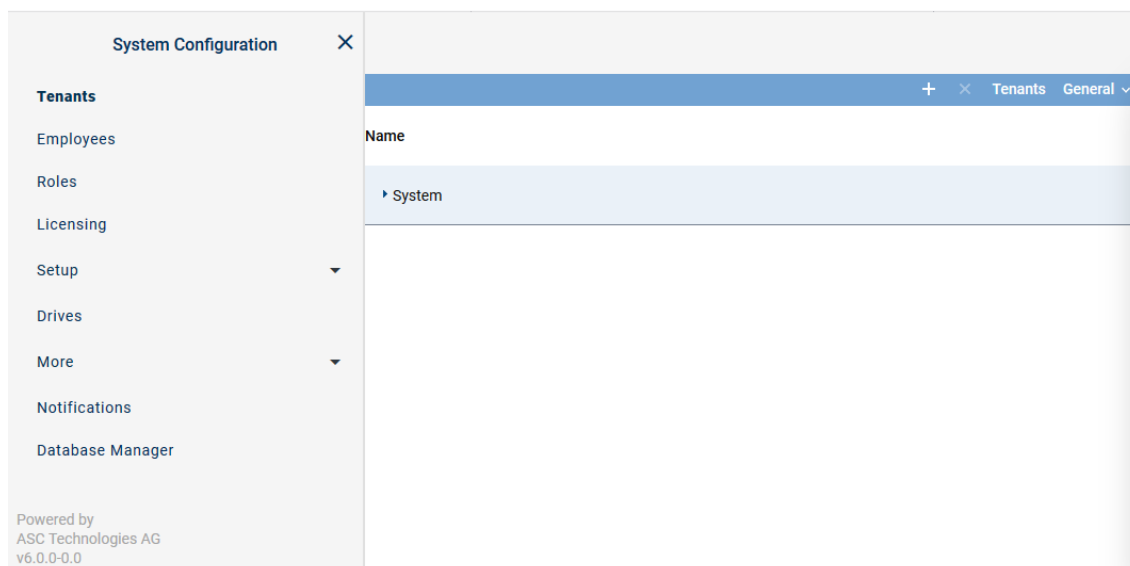


Fig. 3: System Configuration - main view:

7.1.2 Configure recording solution

Supported recording architectures

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

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

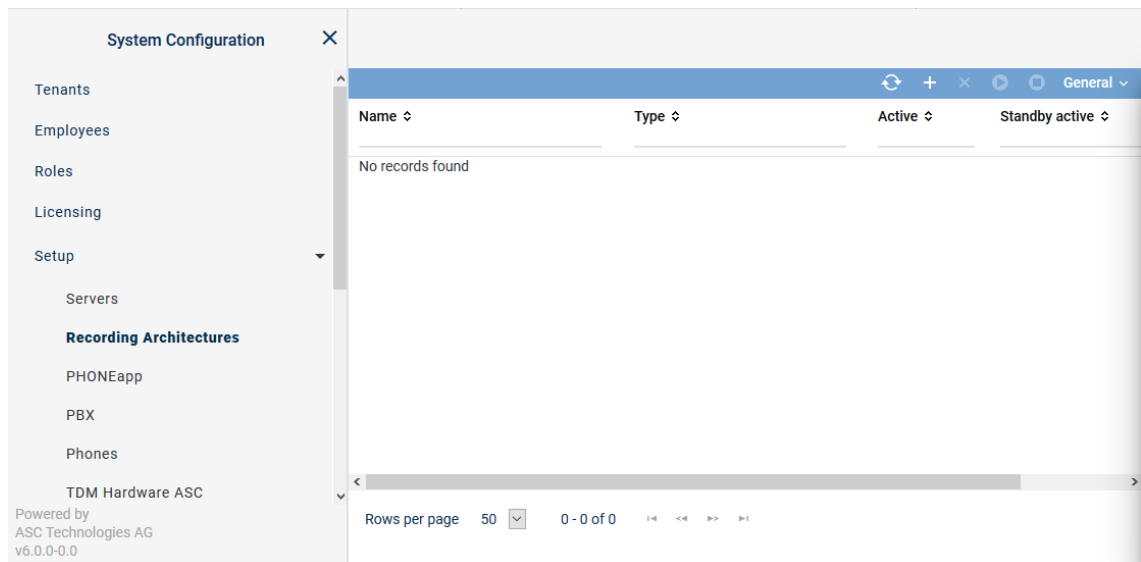




Fig. 4: Recording architectures - main view

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  (Deactivate) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (Activate) 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. 5: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon  is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.

	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

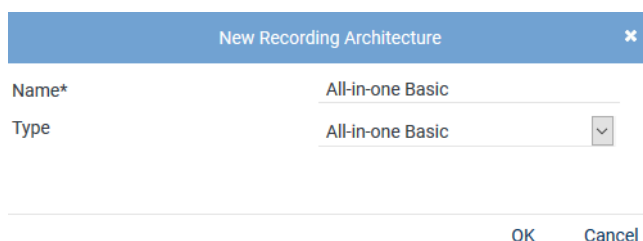
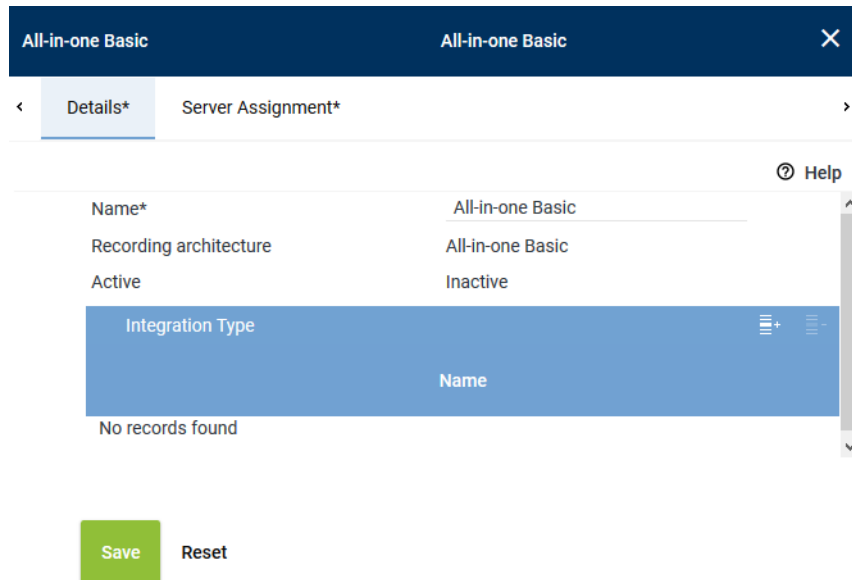


Fig. 6: Create recording architecture - All-in-one Basic Recording


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

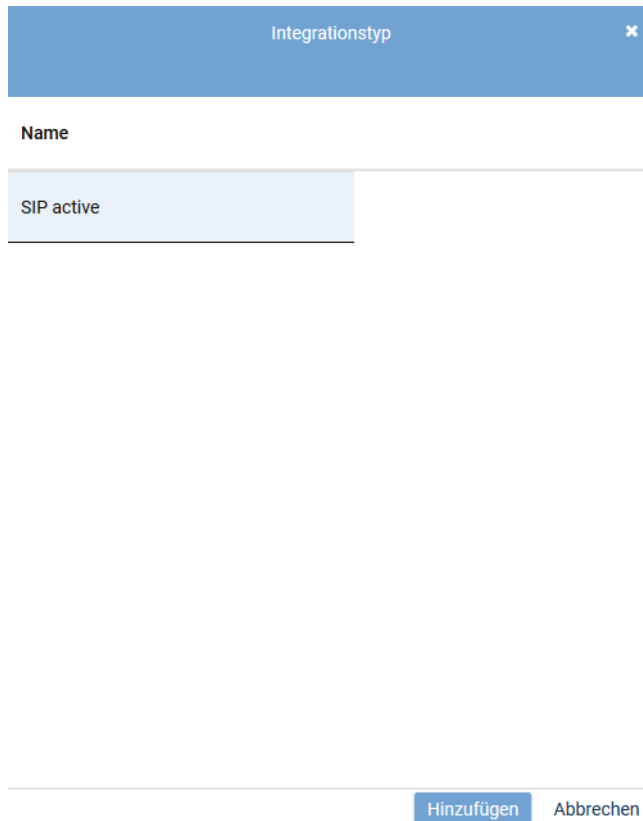


The screenshot shows a configuration window titled 'All-in-one Basic'. It has two tabs: 'Details*' (selected) and 'Server Assignment*'. In the 'Details*' tab, there are three input fields: 'Name*' (containing 'All-in-one Basic'), 'Recording architecture' (containing 'All-in-one Basic'), and 'Active' (containing 'Inactive'). Below these fields is a table titled 'Integration Type'. The table has one column header 'Name' and is currently empty, with a message 'No records found' at the bottom. To the right of the table is a vertical scrollbar. At the bottom of the window are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 7: Recording architecture - tab Details

Add integration type

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



Integrationstyp

Name

SIP active

Hinzufügen Abbrechen

Fig. 8: Select integration type



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

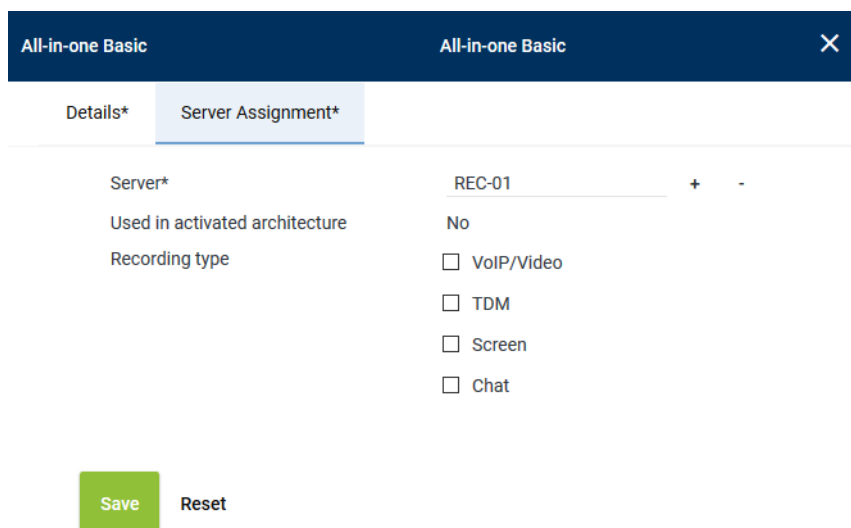


Any number of integration types can be assigned to a recording architecture.

- 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 Basic

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



All-in-one Basic All-in-one Basic

Details* Server Assignment*

Server* REC-01 + -

Used in activated architecture No

Recording type

☐ VoIP/Video

☐ TDM

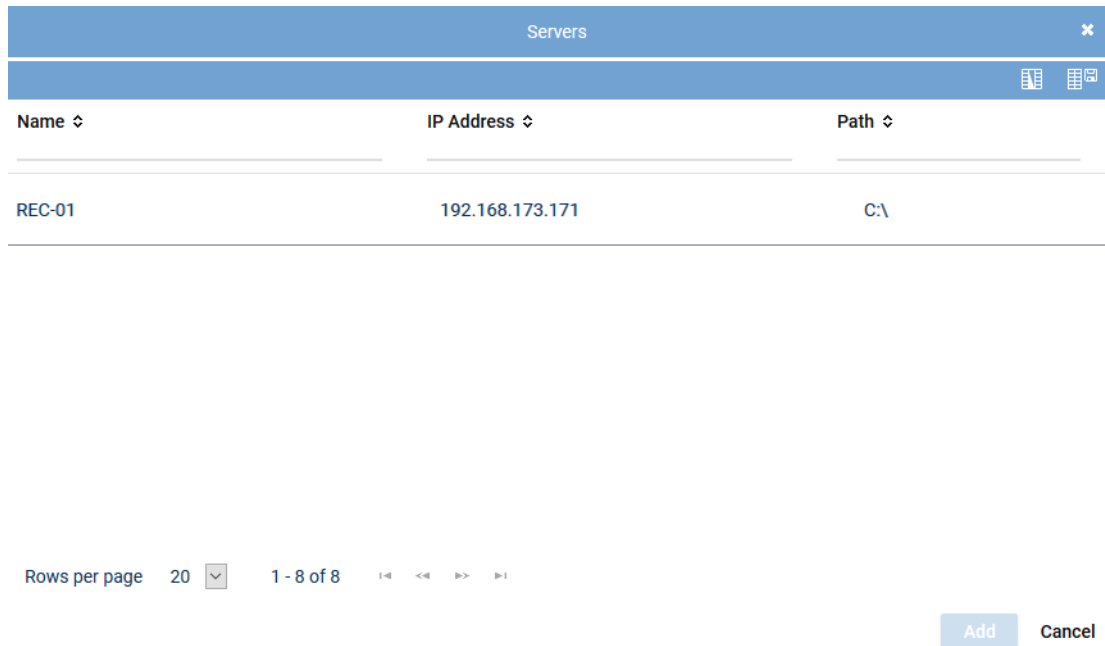
☐ Screen

☐ Chat

Save Reset

Fig. 9: 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. 10: 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. 11: 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.

- 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. 12: 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.



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.

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

System Configuration	
Tenants	
Employees	
Roles	
Licensing	
Setup	
Servers	
Recording Architectures	
PHONEapp	
PBX	
Phones	
TDM Hardware ASC	
Powered by ASC Technologies AG v6.0.0-0.0	

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

Rows per page 50 1 - 8 of 8

Fig. 13: 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.

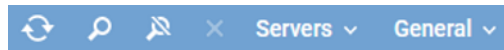







Fig. 14: Toolbar Servers module

	<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. 19 .
	<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.



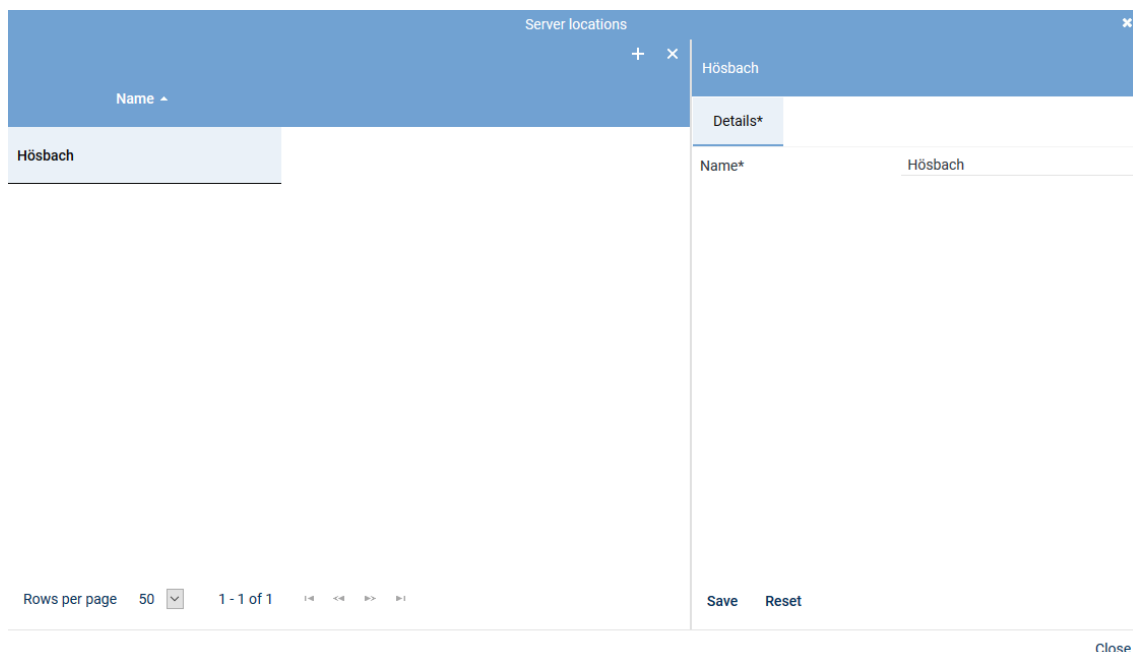
For detailed information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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 with a label "Name*" and a text input field containing "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. 15: Add server locations

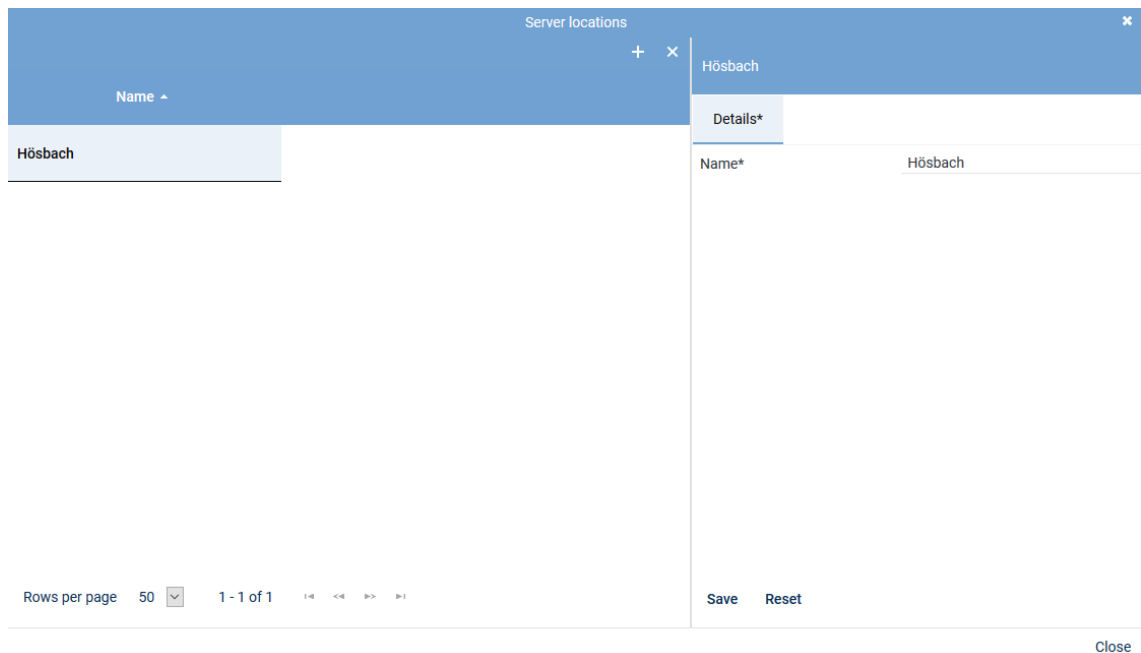
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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



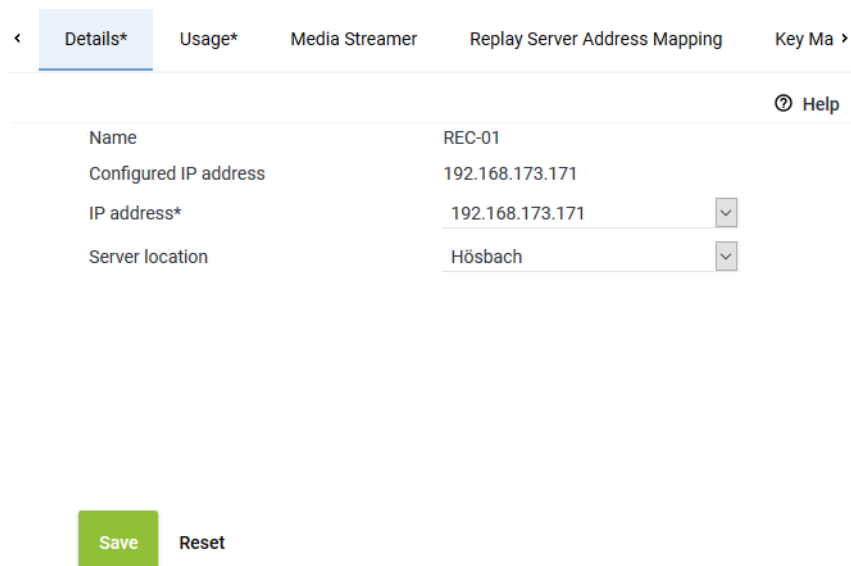
The screenshot shows a window titled "Server locations" with a close button (x) in the top right. Below the title bar is a table with one row containing the text "Hösbach". To the right of the table is a "Details*" tab. Below the tab, there is a form with a label "Name*" and a text input field containing "Hösbach". At the bottom of the window, there is a "Rows per page" dropdown set to "50", a "1 - 1 of 1" indicator, and navigation arrows. On the right side of the bottom bar, there are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the window.

Fig. 16: 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. Below the title bar is a tabbed interface with tabs: "Details*", "Usage*", "Media Streamer", "Replay Server Address Mapping", and "Key Ma". The "Details*" tab is active. Below the tabs is a form with the following fields:

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

At the bottom of the window, there is a "Save" button (green) and a "Reset" button (grey).

Fig. 17: 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.

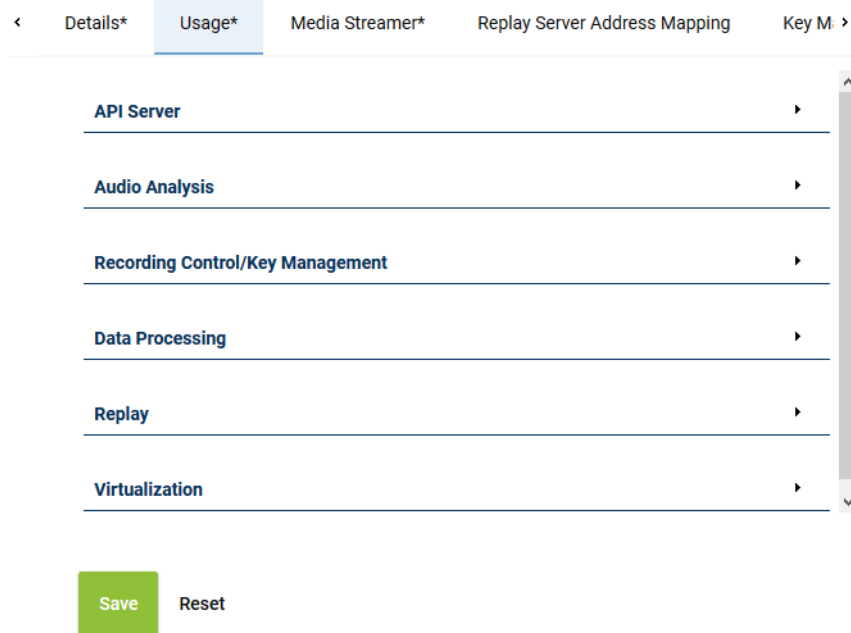
- Click on the button **Save** if the entries are correct.

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.



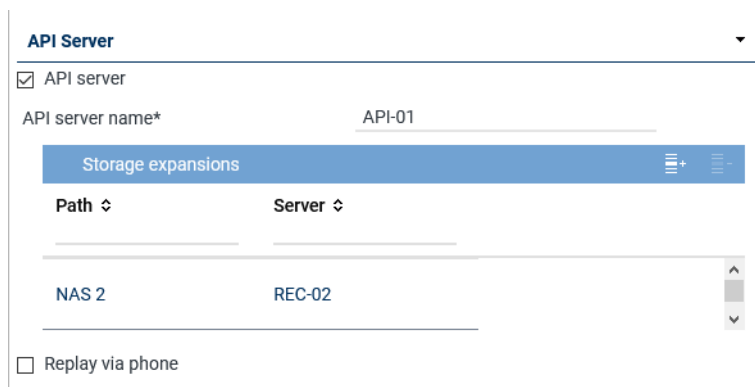
< Details* Usage* Media Streamer* Replay Server Address Mapping Key M. >

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

Save Reset

Fig. 18: Servers - tab usage

Group field API Server



API Server

☒ API server

API server name* API-01

Storage expansions

Path	Server
NAS 2	REC-02

☐ Replay via phone

Fig. 19: Group field API Server



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



The ASC API Server must have been activated on every server where the Recording Control Service runs.


The ASC API Server does not only offer an interface for the internal modules; additionally, the client applications communicate with the neo system by means of this interface, too, using defined commands.

Furthermore, the ASC API Server is responsible for replay by means of the web browser. 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>Tick the check box to start the 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>In order to be able to reach the 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. 32.</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 the storage expansions, see chapter "Add storage expansion for replay", p. 24. By clicking on the icon  (<i>Remove</i>), you can remove the 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 POWER<i>play</i> Pro Application POWER<i>play</i> 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>

Parameter	Value/Description
	<p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 31. 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. 20: 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. 21: 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>	If the function emotion detection has been activated, the parameter to select the respective server becomes active.

Parameter	Value/Description
	<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. 3: Configure audio analysis

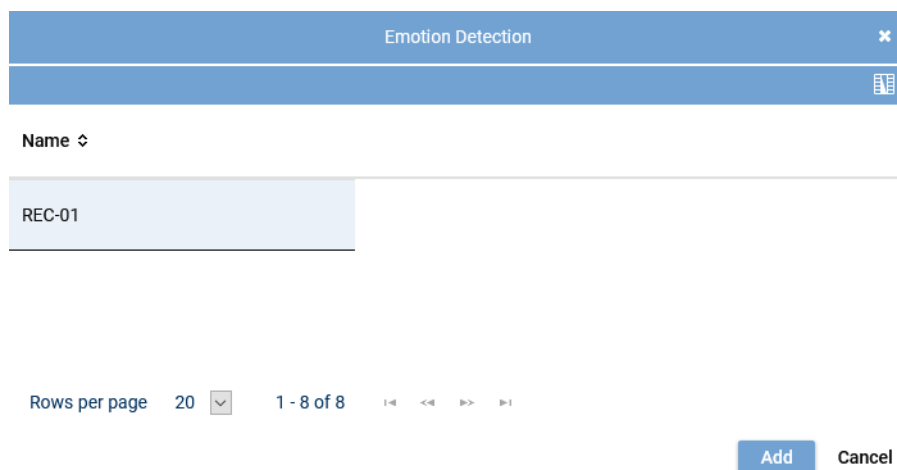


Fig. 22: Select server for emotion detection

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

Group field Recording Control/Key Management

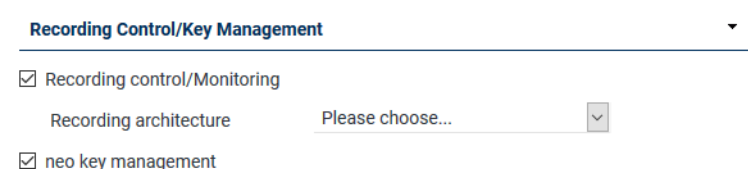


Fig. 23: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/monitoring</i>	<p>Activate the check box, if you would like to use <code>CLIENTcommand</code> or API recording control. 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. 4: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
REC-02	192.168.173.188

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
REC-03	192.168.173.189

Activate period of time ☒

Start 22:00 ▼

End 4:00 ▼

Receives data from

Name	Only Replay
No records found	



☐ Archiving





☒ Export

☒ Import

Recording architecture All-in-one Basic ▼

Fig. 24: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	Activate the check box to allow the modification of the additional functions of data processing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</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. 27. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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 data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be</p>

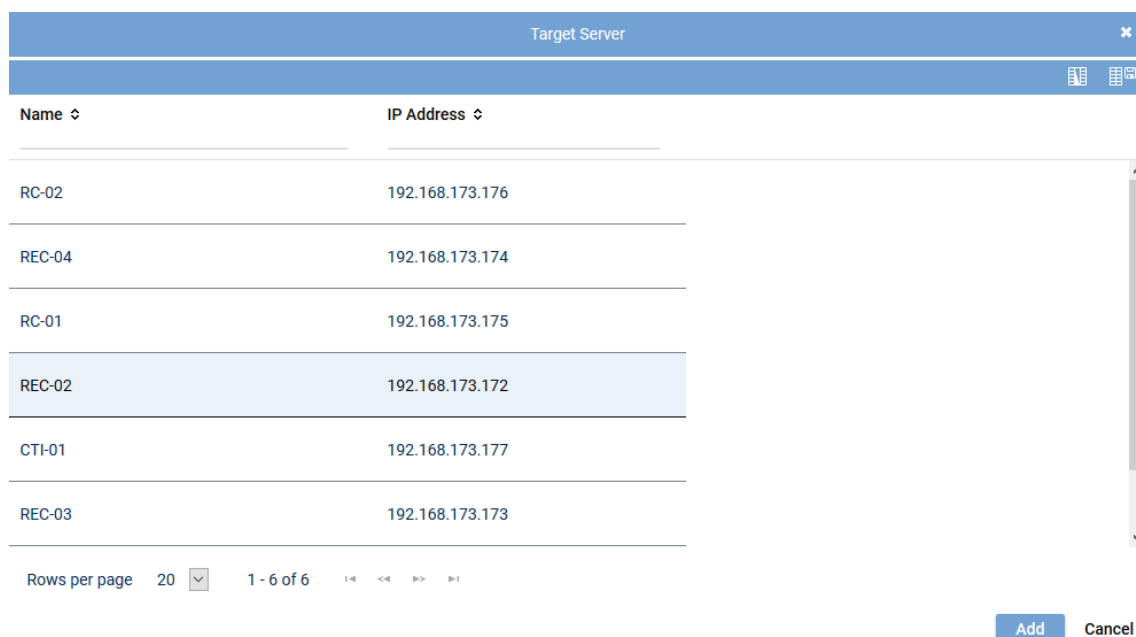
Parameter	Value/Description
	<p>transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 27. By clicking on the icon  (<i>Remove</i>), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</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>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 5: Configure data storage

Add target server to a list

- 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

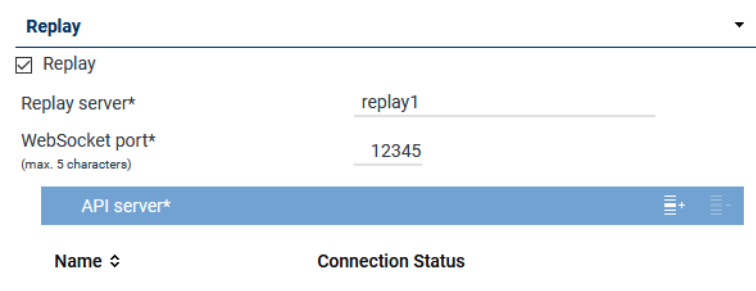
Fig. 25: Select server



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. 26: Group field Replay

Parameter	Value/Description
Replay	<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>

Parameter	Value/Description
<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 (maximum of 5 characters)</i>	Enter the port via which the data to be replayed in <i>POWERplay</i> Web are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 29. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 6: 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.

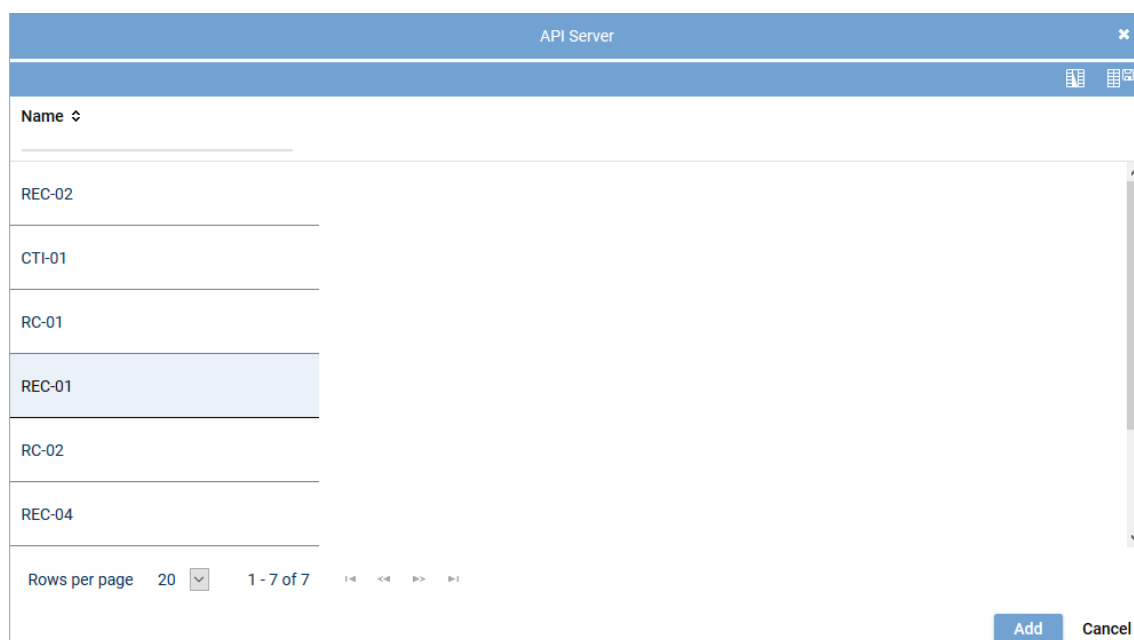


Fig. 27: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 22](#).

- 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. 28: 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. 7: 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*.

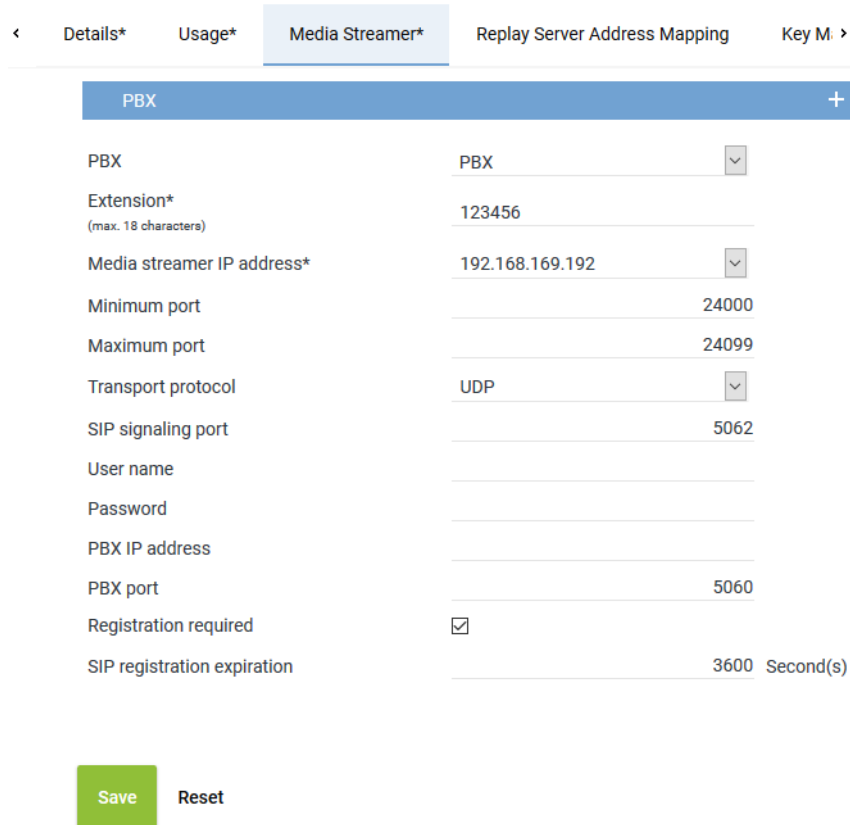


Fig. 29: Servers module - tab Media Streamer

- 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. 36.</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. In the drop-down list, all IP addresses of the server are displayed.</p>

	If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.
<i>Minimum port</i>	Enter the minimum port which is supposed to be used for the audio data exchange.
<i>Maximum port</i>	Enter the maximum port which is supposed to be used for the audio data exchange. 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.
<i>Transport protocol</i>	Select the transport protocol type you would like to use for the SIP communication from the drop-down list. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select UDP in the drop-down list.
<i>SIP signaling port</i>	Enter the port for the SIP communication. Port for data exchange: 5062
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX . If an external analog gateway has been integrated, enter the IP address 169.254.254.101 .
<i>PBX port</i>	Enter the port of the SIP registrar of the PBX . If an external analog gateway has been integrated, enter the value 5060 .
<i>Registration required</i>	Select whether the SIP extension has to be registered with the SIP registrar of the PBX . <input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box Registration required .
<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*.

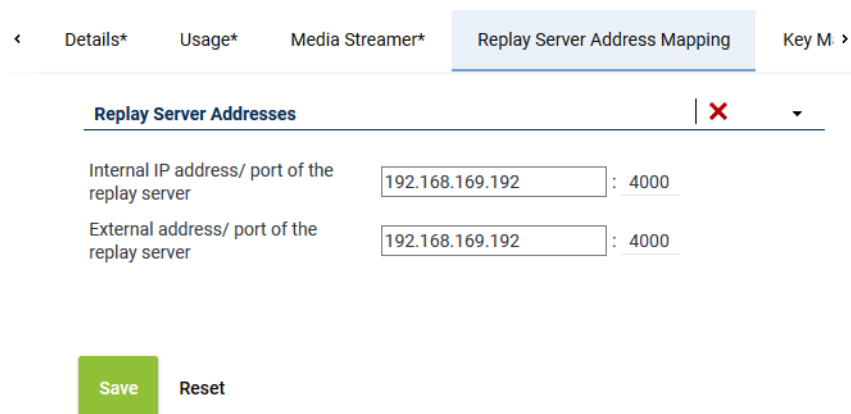


Fig. 30: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

<i>Internal IP address/ port of the replay server</i>	Enter the destination IP address and the port of the replay server at which the Replay module can be reached internally.
<i>External address / Port of the replay server</i>	Enter the URL or the IP address and the port at which the Replay module can be reached via the browser from outside. When entering the external address consider whether the SSL certificate has been created for an IP address or for a DNS address. In the latter case, it is imperative to enter the DNS name! Otherwise the certificate check in the replay applications 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. 31: Servers module - tab Key Management

<i>Key creation interval</i>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> • <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • <i>Create key manually</i> Select that a key is supposed to be generated manually. <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p>

	CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
<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.

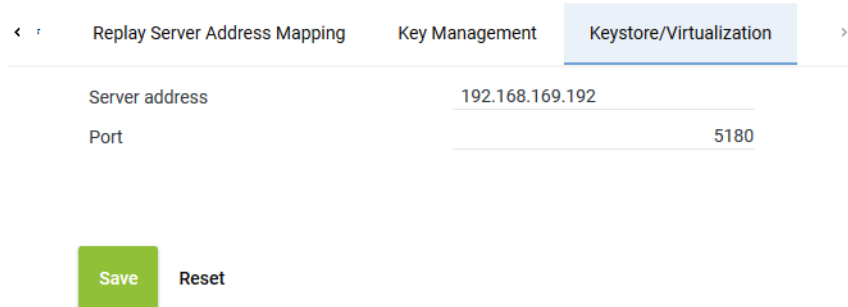


Fig. 32: Servers module - tab Keystore/Virtualization

<i>Server address</i>	<p>Enter the address of the server for this connection.</p> <ul style="list-style-type: none"> • If you use the neo key management as well as the virtualization: IP address of the server that the service <i>DongleMan</i> has been installed on. • If you use only virtualization, you can authenticate the VM via the ASC License Management System, too. In this case, enter the following address: <i>licensing.asc.de</i> • If you use only the ASC key management: IP address of the server with the master password database
<i>Port</i>	<p>Enter the port for the connection.</p> <p>Default value: <i>5180</i></p>



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

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

7.1.2.1.3 Create PBX

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

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

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

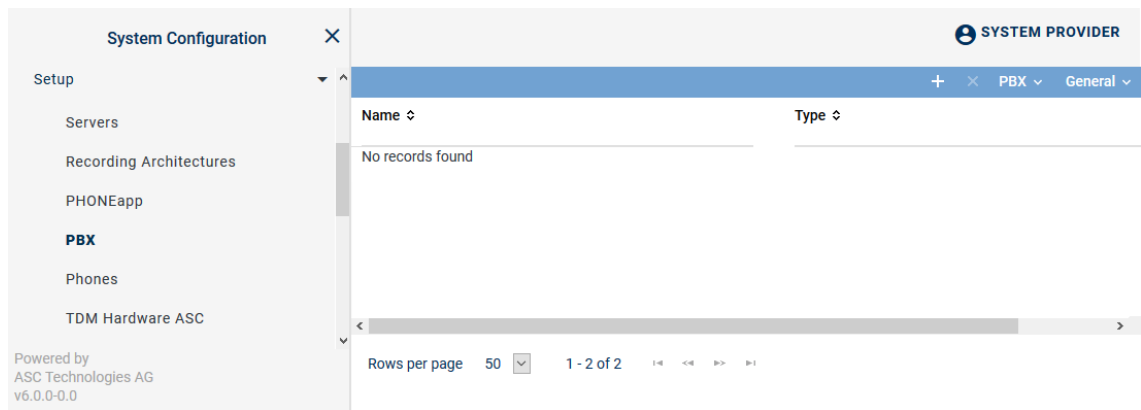




Fig. 33: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 34: 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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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

Country code
☒ Select from list
United States (1)
☐ 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. 35: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka 094.
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 8: 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. 9: 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

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.

Assign extensions to tenants

If you would like to make an assignment based on extensions, you can assign the respective tenant the extension designated for recording in the Tenants module.



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

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



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

The manual assignment of extensions is not possible until a PBX has been created since extensions are assigned in relation to the PBX.

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

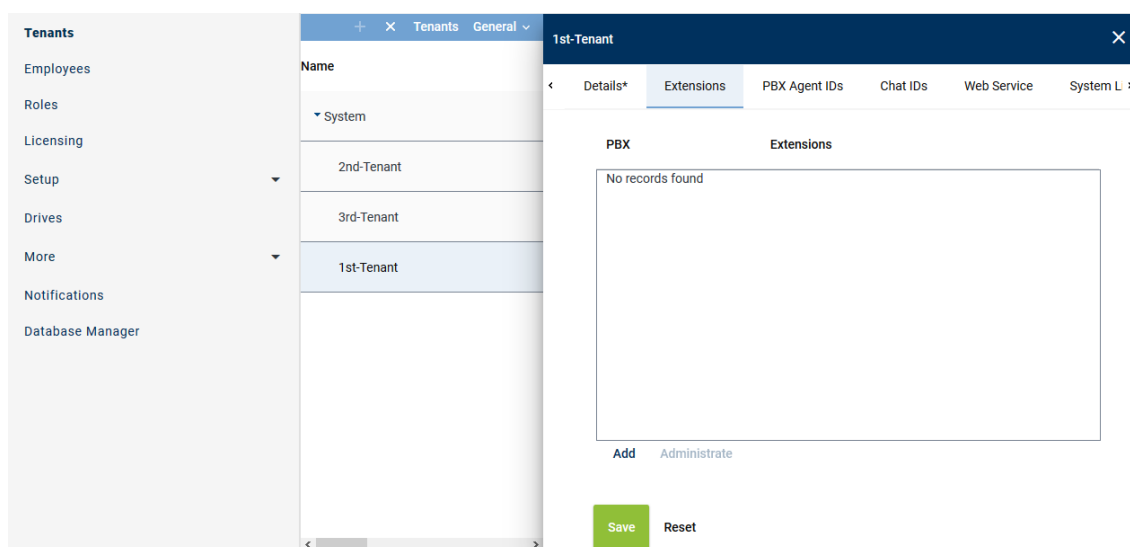


Fig. 36: Tenants - main view - tab Extensions

Add extensions

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

⇒ The following window appears:

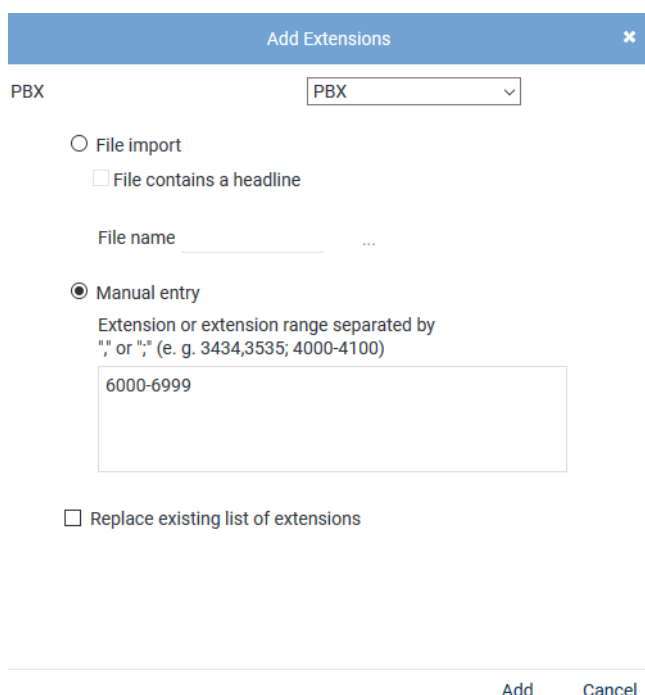


Fig. 37: Assign extensions to tenants

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

- 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.

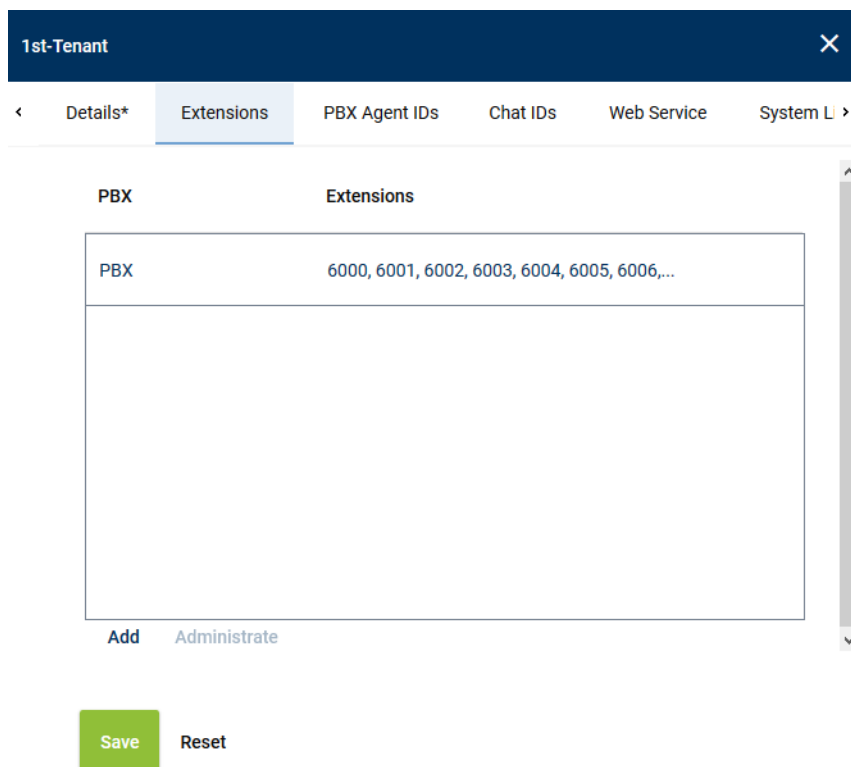
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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. 38: 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. 39: Select extensions

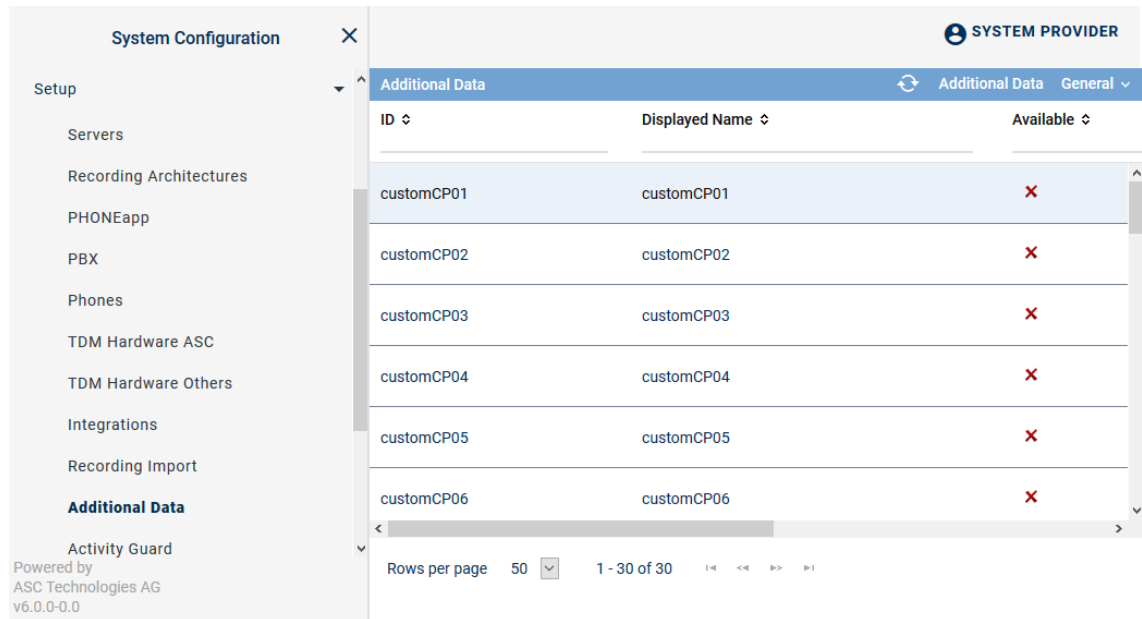
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

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.

In order to have the fields displayed in the drop-down list to be selected, they must 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

Rows per page: 50 | 1 - 30 of 30

Fig. 40: Additional Data module main view

The following additional data is always available:

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

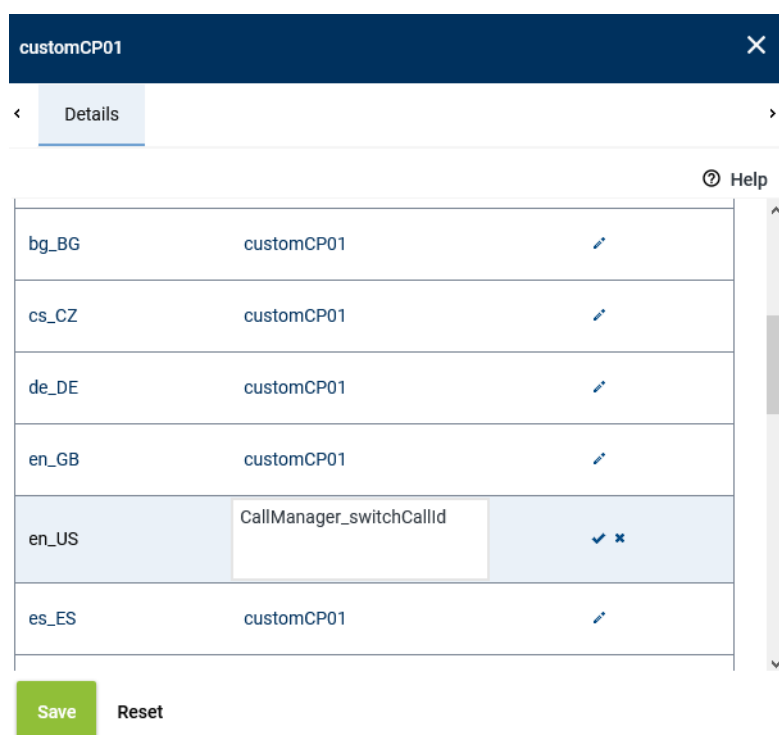
For this recording solution, you can additionally configure the following additional data:

- *CallManager_switchCallId*

2. Select a data set

⇒ In the detail view, the information that can be configured appears.

Change display name



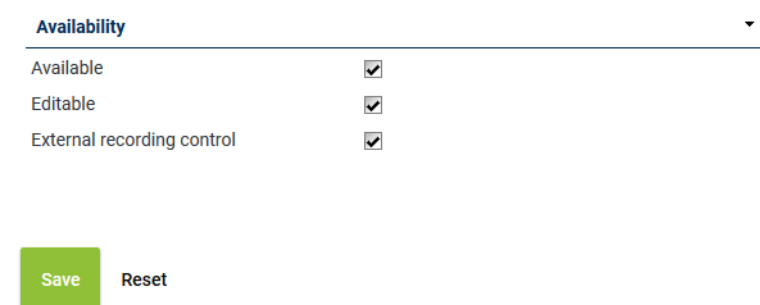
customCP01		
bg_BG	customCP01	
cs_CZ	customCP01	
de_DE	customCP01	
en_GB	customCP01	
en_US	CallManager_switchCallId	
es_ES	customCP01	

Save Reset

Fig. 41: Configure additional data

1. To change the display name, click on the pen icon in the line of the language that 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. 42: Additional data - configure availability

1. To make the data field available for the entire system, activate the check box of the option *Available*.
2. To make the data field editable for the search and replay applications subsequently, tick the check box of the option *Editable*.
3. To use the data field for external recording control, tick 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*.

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:

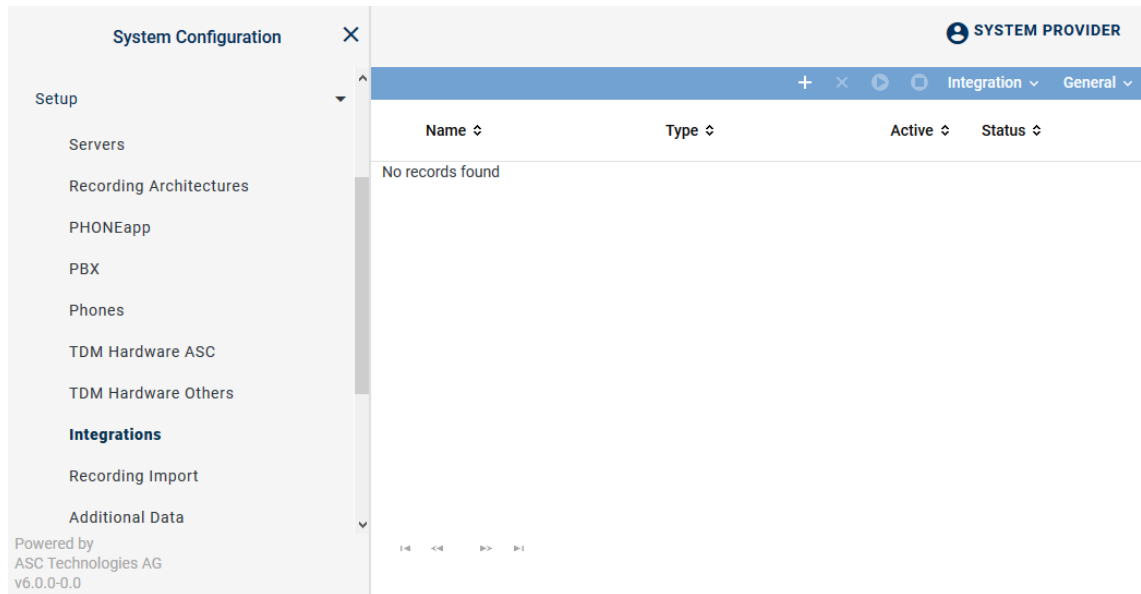




Fig. 43: Integrations - main view

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. 44: 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.

	<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.

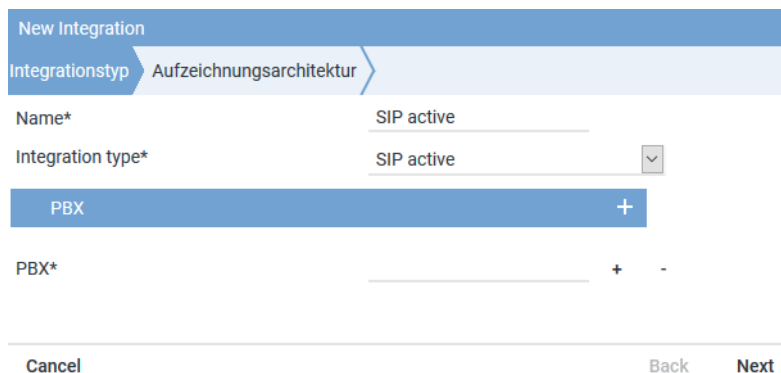



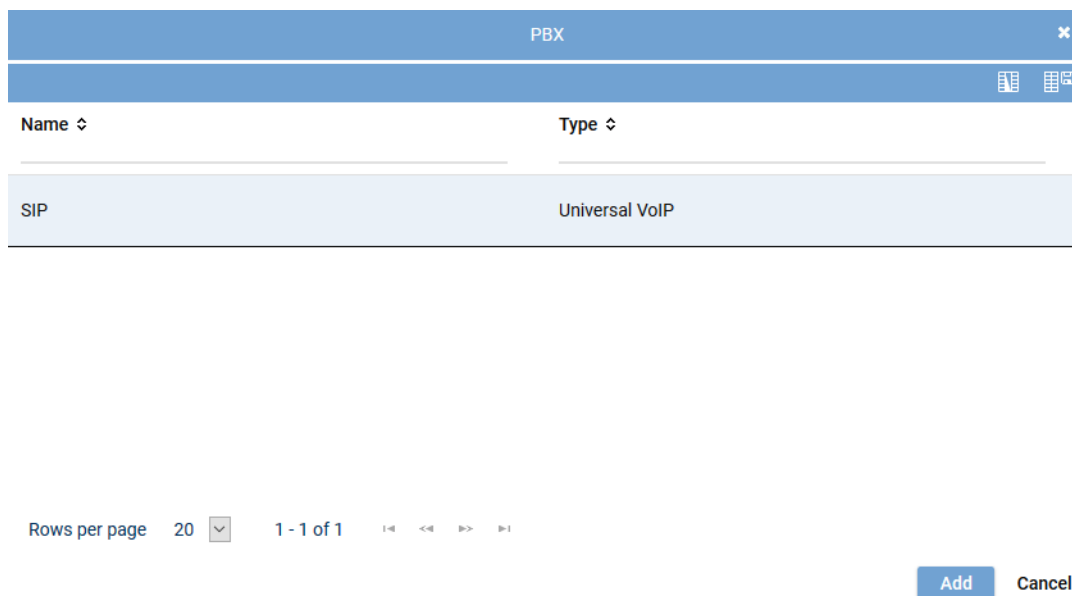
Fig. 45: Create integration type

- 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. 10: 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. 46: 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. 47: 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. 48: 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. 49: 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

- 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. 50: Configuration step - Global recording settings

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


Parameter	Value/Description
<i>Transport protocol</i>	Select the deployed transport protocol for the SIP signaling between recording server and PBX from the drop-down list. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling on which the recording server waits for 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 must configure a separate SIP port for each integration. NOTICE! If you would like to use a media streamer for re-play, configure a separate SIP port for it, too. In case of issues in the communication with the Media Streamer this can otherwise affect recording.
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name for the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password for the SIP registration</i>	Enter the password if an authentication for SIP registration is supposed to be used.
<i>Activate PBX connection</i>	Activate the check box, if the recording server is supposed to register on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration expires, 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 . Default value is 5060.

Parameter	Value/Description
<i>Activate SMS recording</i>	This functionality is not supported in this recording solution.

Tab. 11: Global recording settings

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

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.

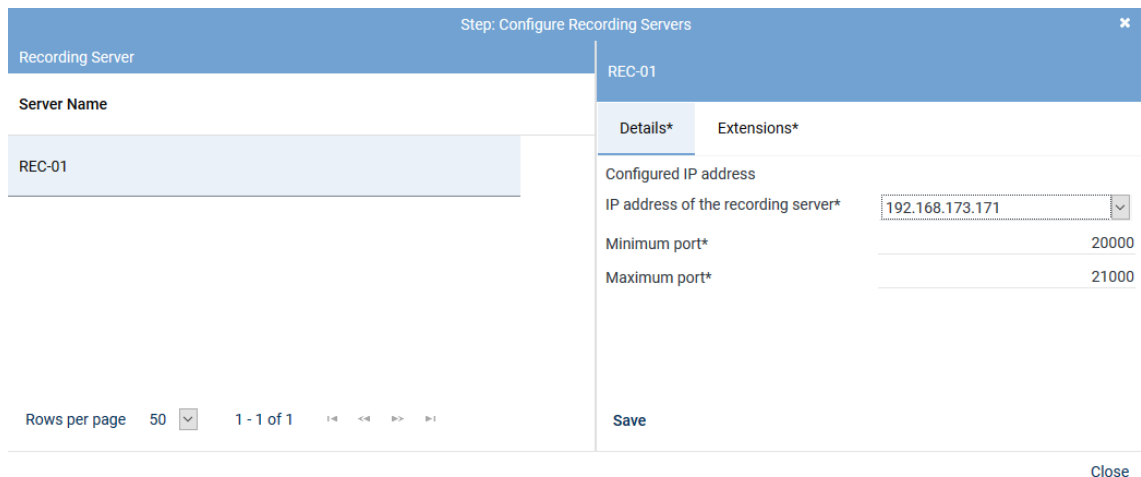


Fig. 51: Configuration step - Configure recording servers

- 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. <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. 12: Configure recording servers



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



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

Configure add-on



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



Add-ons are not supported in this recording solution.


Configure miscellaneous settings





Configuring these settings is not required for this recording solution. Even without this configuration step, the integration has been configured comprehensively and can be activated.

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. 52: 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. 53: 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. 54: 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 Parallel Recording

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:

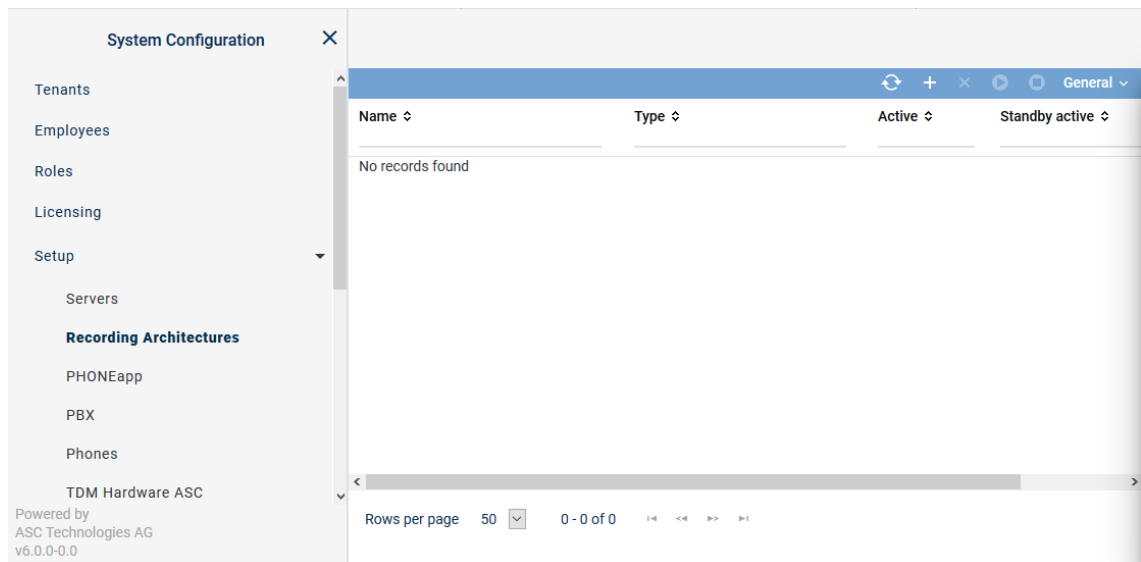




Fig. 55: Recording architectures - main view

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. 56: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon  is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.


	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

Create recording architecture All-in-one Parallel Recording

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

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

⇒ The window *New Recording Architecture* appears.

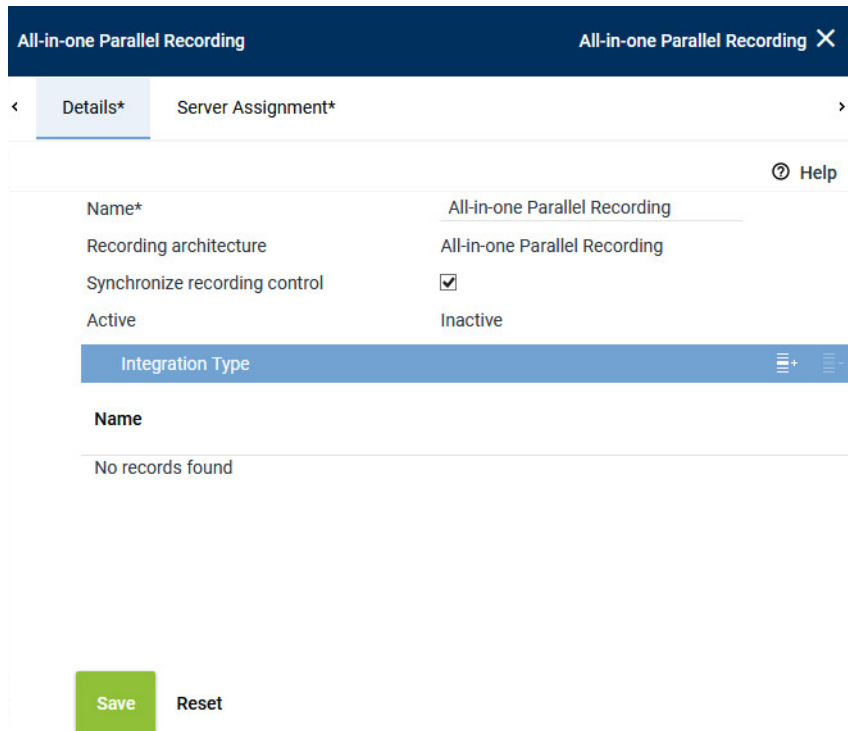


Fig. 57: Create recording architecture - All-in-one Parallel Recording

2. In the entry field *Name*, enter a descriptive name for the recording architecture.
3. From the drop-down list *Type*, select the recording architecture type *All-in-one Parallel Recording*.

NOTICE! The drop-down list only displays the supported recording architecture types.

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



All-in-one Parallel Recording All-in-one Parallel Recording ✕

< **Details*** **Server Assignment*** >

🔗 Help

Name*	All-in-one Parallel Recording
Recording architecture	All-in-one Parallel Recording
Synchronize recording control	<input checked="" type="checkbox"/>
Active	Inactive

Integration Type ⋮ + ⋮ -

Name

No records found

Save Reset


Fig. 58: 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 Synchronization recording control.

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

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

Add integration type

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. 59: Select integration type



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

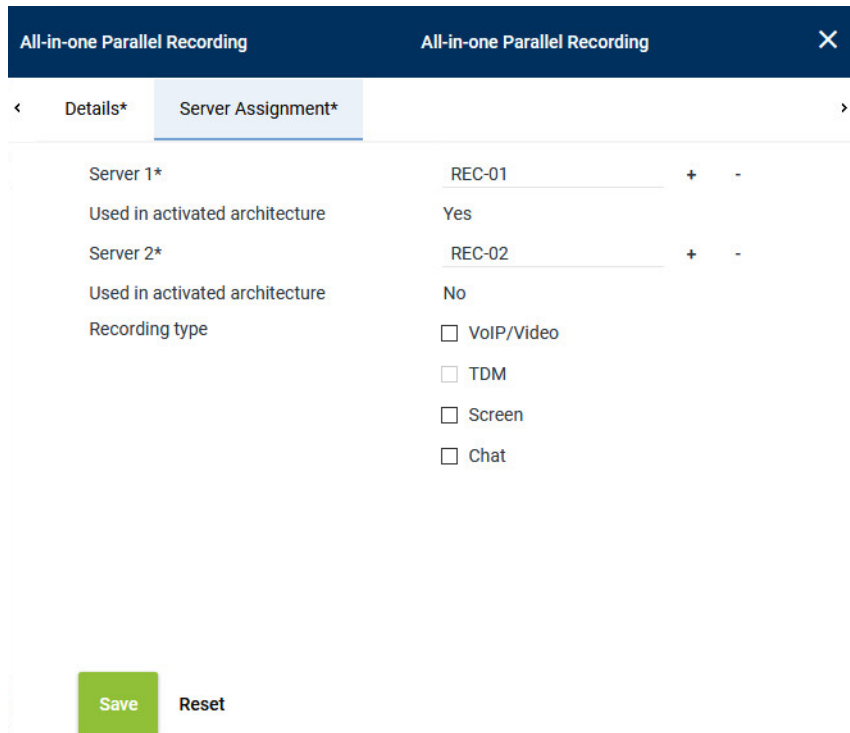


Any number of integration types can be assigned to a recording architecture.

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 X

< **Details*** **Server Assignment*** >

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		

Save **Reset**

Fig. 60: Recording Architecture - tab Server Assignment

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



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. 61: 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. 62: 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. 63: Activate recording architecture

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



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



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



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

7.1.2.2.2 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:

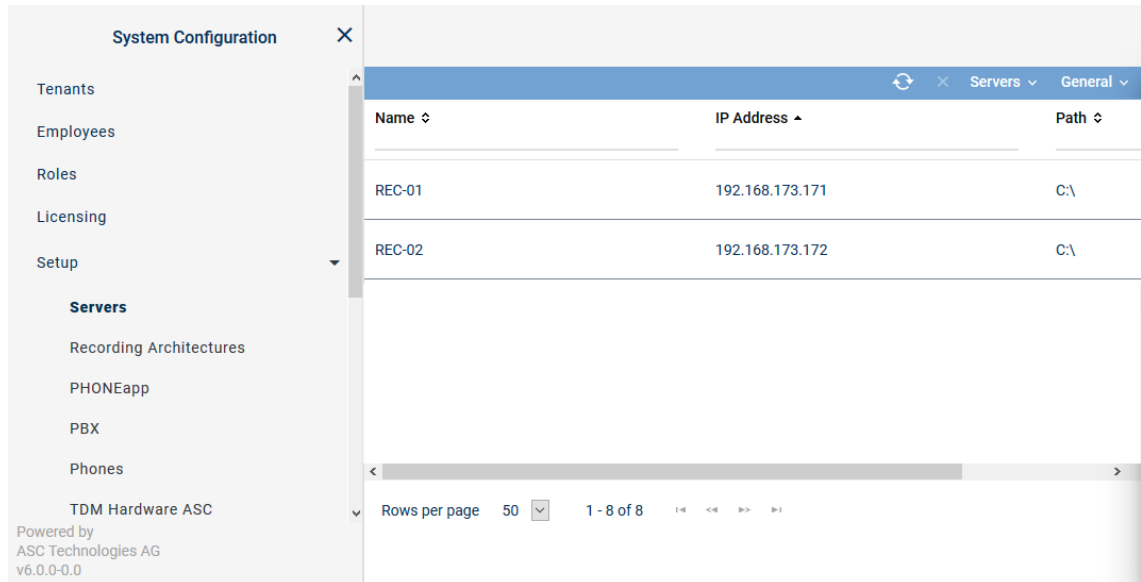


Fig. 64: Servers - main view

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. 65: 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. 60.
	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

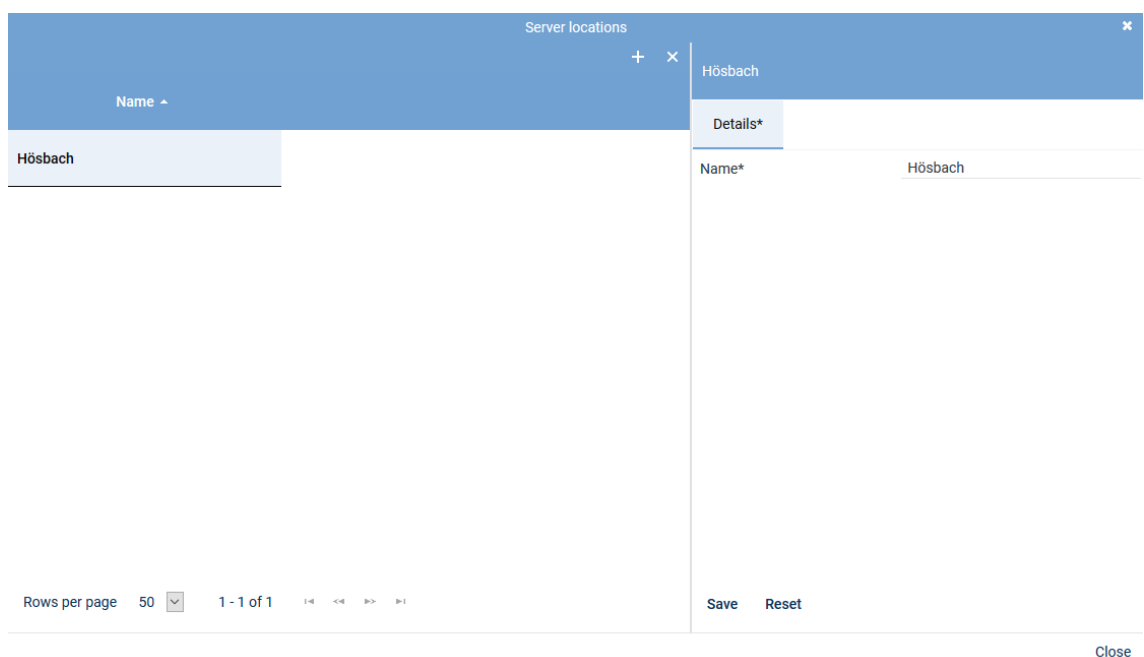



Fig. 66: Add server locations

- 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.

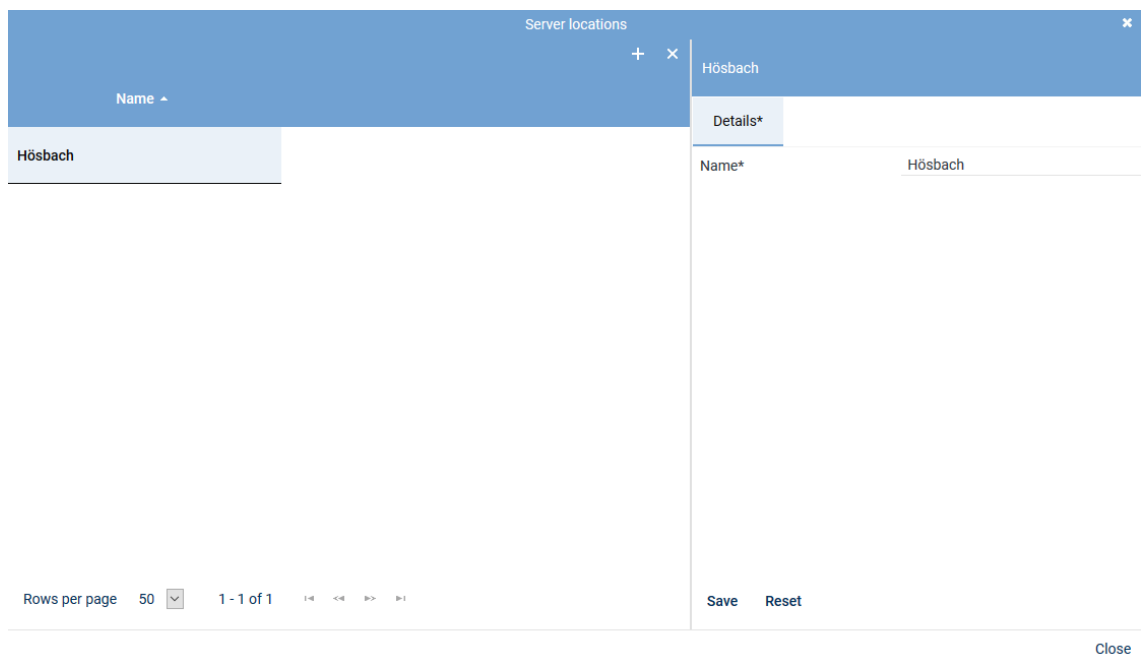



Fig. 67: Delete server location

- 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 <input type="button" value="v"/>
Server location	Hörsbach <input type="button" value="v"/>

Fig. 68: 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.



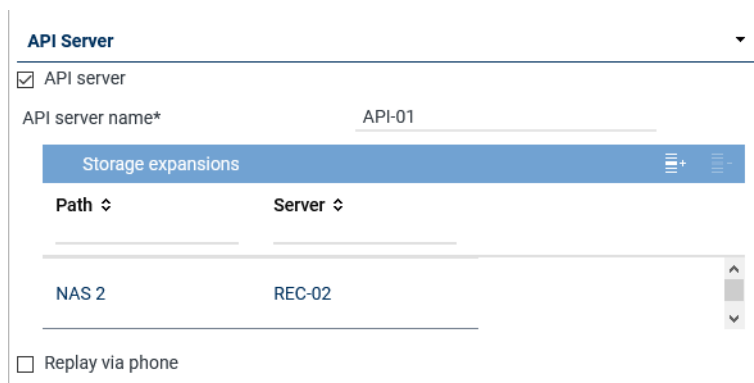
As a server may be used for several recording solutions, all intended purposes are displayed. Note that some intended purposes do not apply for certain recording solutions. In chat recording, for instance, audio analysis or replay via phone cannot be used.

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

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

Fig. 69: Servers - tab usage



Group field API Server



API Server ▼

☒ API server

API server name*

Storage expansions  

Path ↕	Server ↕
NAS 2	REC-02

☐ Replay via phone

Fig. 70: Group field API Server


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




The ASC API Server must have been activated on every server where the Recording Control Service runs.


The ASC API Server does not only offer an interface for the internal modules; additionally, the client applications communicate with the neo system by means of this interface, too, using defined commands.

Furthermore, the ASC API Server is responsible for replay by means of the web browser. 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>Tick the check box to start the 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>In order to be able to reach the 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. 73.</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 the storage expansions, see chapter "Add storage expansion for replay", p. 64.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (<i>Remove</i>), you can remove the 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. <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. 71. To be able to do so, at least 1 PBX must have been configured in the system.</p>

Add storage expansion for replay

- Click on the icon  (*Add*) in the toolbar of the list.
- 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. 71: 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. 72: 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. 13: Configure audio analysis

Emotion Detection

Name

REC-01

Rows per page 20

1 - 8 of 8

1-8

<<

>>

8-1

Add

Cancel

Fig. 73: 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. 74: 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. 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. 14: Configure recording control/key management

Group field Data Processing

Data Processing

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
REC-02	192.168.173.188

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
REC-03	192.168.173.189

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	







☐ Archiving

☒ Export

☒ Import

Recording architecture

Fig. 75: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to allow the modification of the additional functions of data processing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</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. 68. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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 data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</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. 68. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</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>

Group field Replay

Replay

☒ Replay

Replay server*

replay1

WebSocket port*

12345


(max. 5 characters)


API server*

Name

Connection Status

Fig. 77: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 70.

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

Tab. 16: 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.

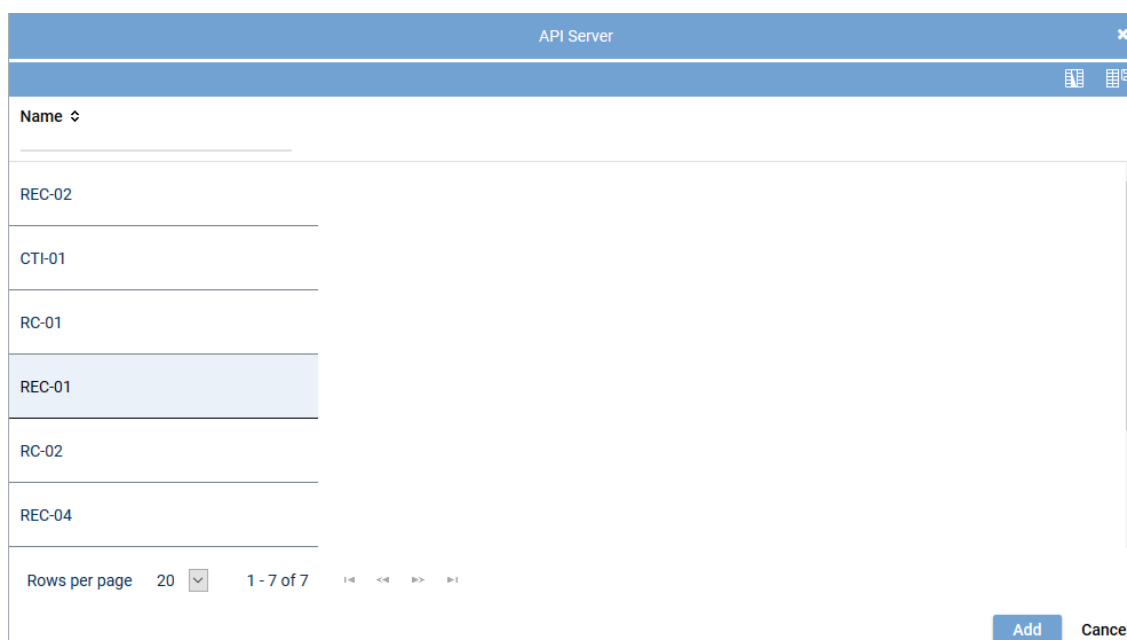


Fig. 78: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 63](#).

- 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. 79: 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. 17: 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. 80: 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. 36.</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. In the drop-down list, all IP addresses of the server are displayed.</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>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</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>
Transport protocol	<p>Select the transport protocol type you would like to use for the SIP communication from the drop-down list.</p>

	<p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>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 <i>SIP</i> communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the <i>SIP</i> server.
<i>Password</i>	Enter the password for the authentication on the <i>SIP</i> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <i>SIP</i> registrar of the <i>PBX</i>.</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 <i>SIP</i> registrar of the <i>PBX</i>.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the <i>SIP</i> extension has to be registered with the <i>SIP</i> registrar of the <i>PBX</i>.</p> <p><input checked="" type="checkbox"/> = <i>SIP</i> extension has to be registered.</p> <p><input type="checkbox"/> = <i>SIP</i> 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*.

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

Replay Server Addresses
|
✖
▼

Internal IP address/ port of the replay server : 4000

External address/ port of the replay server : 4000

Save
Reset

Fig. 81: 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 destination IP address and the port of the replay server at which the Replay module can be reached internally.
<i>External address / Port of the replay server</i>	Enter the URL or the IP address and the port at which the Replay module can be reached via the browser from outside. When entering the external address consider whether the SSL certificate has been created for an IP address or for a DNS address. In the latter case, it is imperative to enter the DNS name! Otherwise the certificate check in the replay applications 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 Day(s) Hour(s)

☐ Key expiration date

after Day(s)

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

Save
Reset

Fig. 82: Servers module - tab Key Management

<i>Key creation interval</i>	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: <ul style="list-style-type: none"> • All
------------------------------	--

	<p>Select the intervals in which a new key is supposed to be generated automatically.</p> <p>Possible time interval: 1 to 365 days</p> <p>Default value: 365 days</p> <ul style="list-style-type: none"> • <i>Create key manually</i> <p>Select that a key is supposed to be generated manually.</p> <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</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.

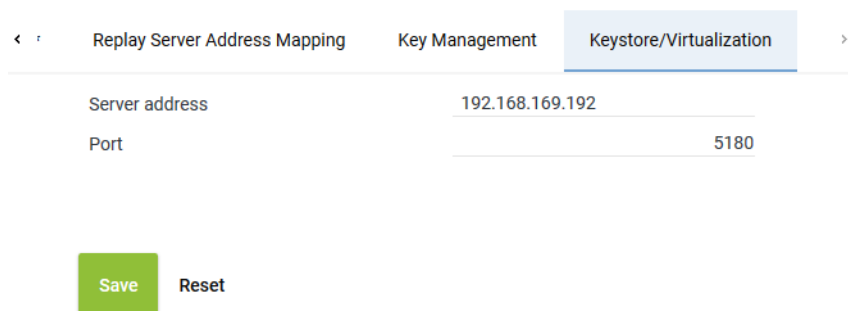
For licensing, there are the following options:

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 configuration window with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is selected. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom, there are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 83: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for this connection.</p> <ul style="list-style-type: none"> • If you use the neo key management as well as the virtualization: IP address of the server that the service <i>DongleMan</i> has been installed on. • If you use only virtualization, you can authenticate the VM via the ASC License Management System, too. In this case, enter the following address:
-----------------------	---

	<i>licensing.asc.de</i> <ul style="list-style-type: none"> If you use only the ASC key management: IP address of the server with the master password database
Port	Enter the port for the connection. Default value: 5180



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 Assign recording resources

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.

Assign extensions to tenants

If you would like to make an assignment based on extensions, you can assign the respective tenant the extension designated for recording in the Tenants module.



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

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



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

The manual assignment of extensions is not possible until a PBX has been created since extensions are assigned in relation to the PBX.

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

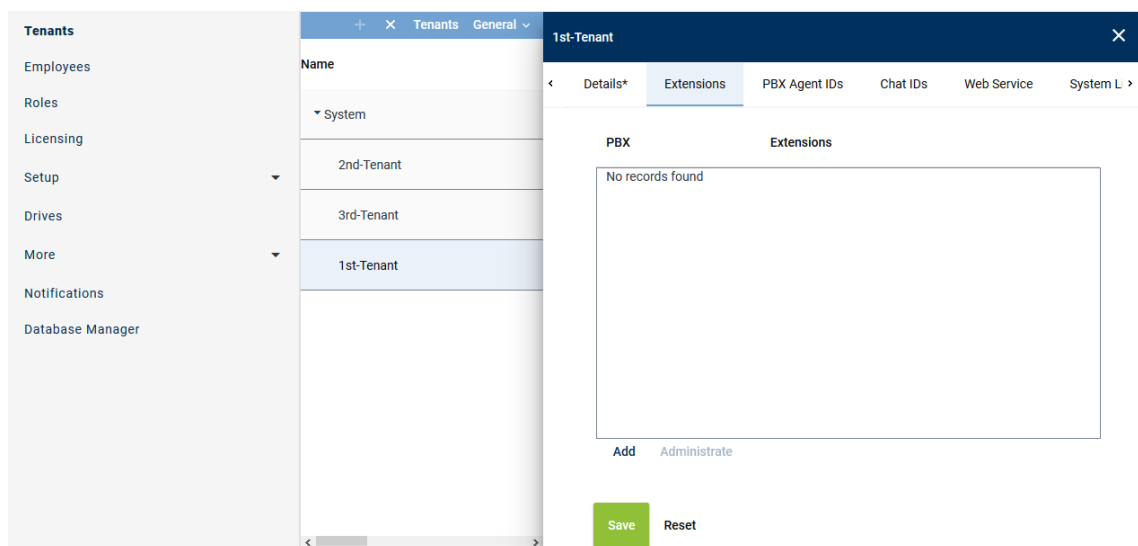


Fig. 84: Tenants - main view - tab Extensions

Add extensions

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

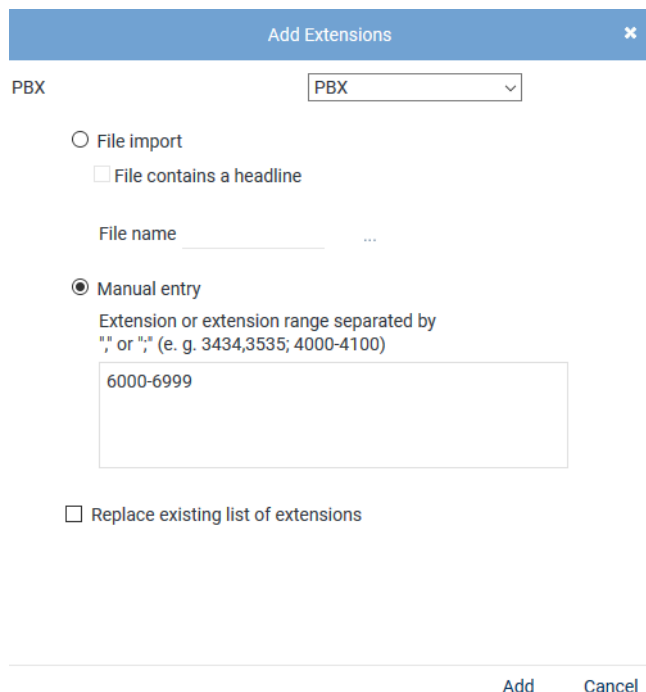




Fig. 85: Assign extensions to tenants

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

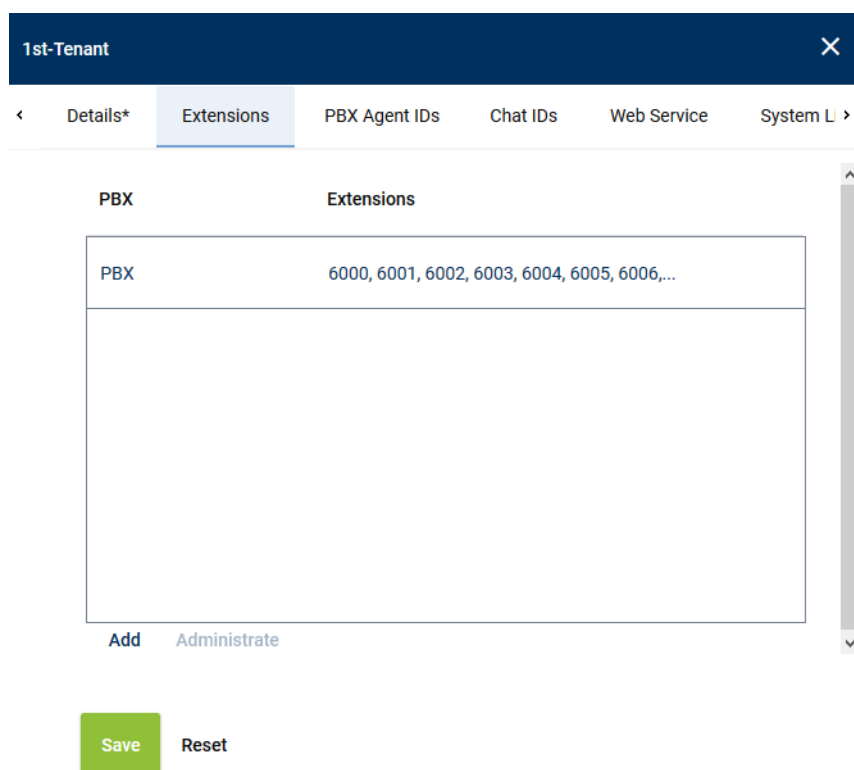
File import	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
File contains a headline	<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>
File name	<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>.

	<ul style="list-style-type: none"> • 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> <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.</p> <p>Enter country codes as number ranges as follows: +4984496800-+4984496810</p> <p>NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.</p>

- 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. 86: 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. 87: Select extensions

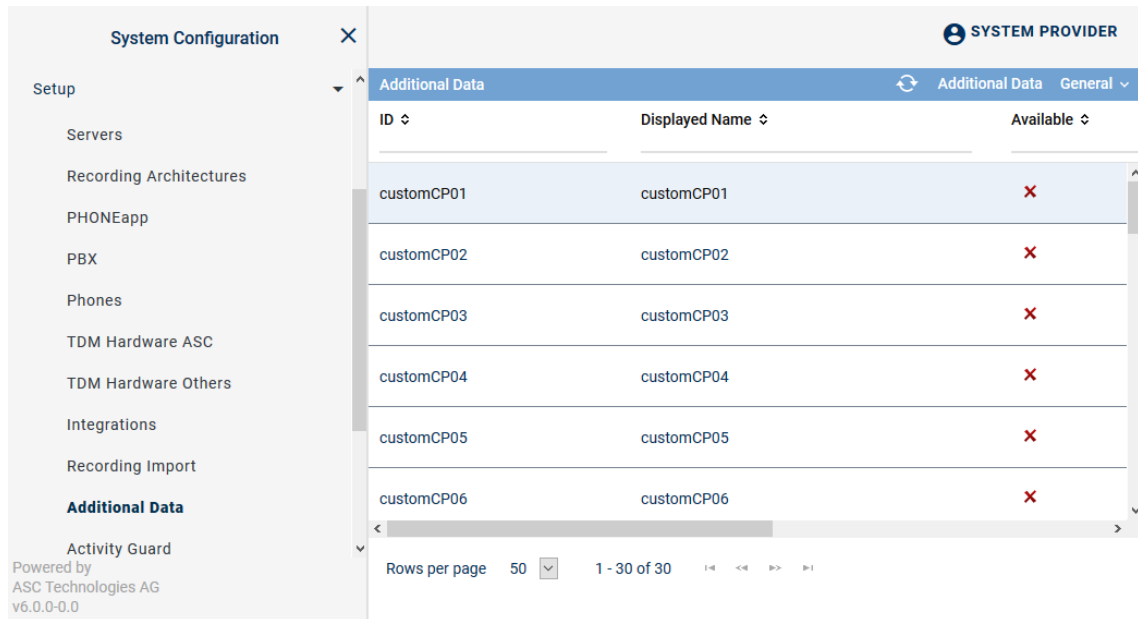
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

7.1.2.2.4 Configure additional data

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

In order to have the fields displayed in the drop-down list to be selected, they must 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

Fig. 88: Additional Data module main view

The following additional data is always available:

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

For this recording solution, you can additionally configure the following additional data:

- *CallManager_switchCallId*

2. Select a data set

⇒ In the detail view, the information that can be configured appears.

Change display name

customCP01

×

<

Details

>

ⓘ Help

bg_BG	customCP01	
cs_CZ	customCP01	
de_DE	customCP01	
en_GB	customCP01	
en_US	<input type="text" value="CallManager_switchCallId"/>	
es_ES	customCP01	

Save

Reset

Fig. 89: Configure additional data

1. To change the display name, click on the pen icon in the line of the language that 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. 90: Additional data - configure availability

1. To make the data field available for the entire system, activate the check box of the option *Available*.
2. To make the data field editable for the search and replay applications subsequently, tick the check box of the option *Editable*.
3. To use the data field for external recording control, tick 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*.

7.1.2.2.5 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:

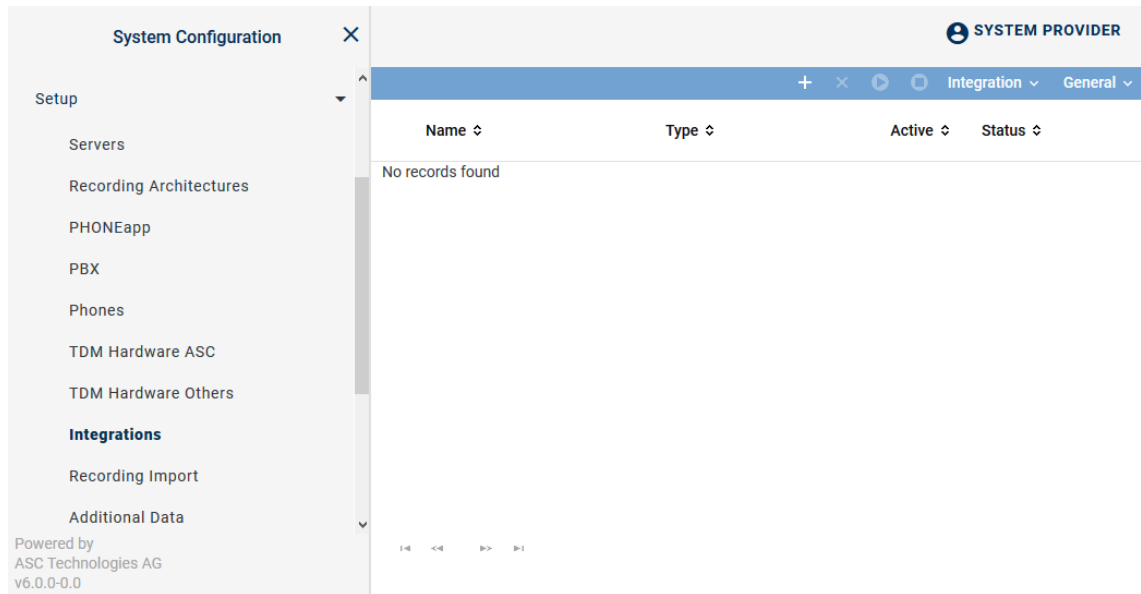




Fig. 91: Integrations - main view

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. 92: 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.

	<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.

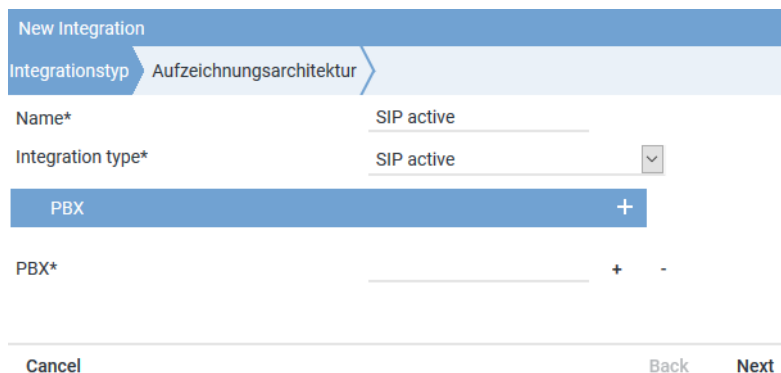



Fig. 93: Create integration type

- 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. 18: Create integration type

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

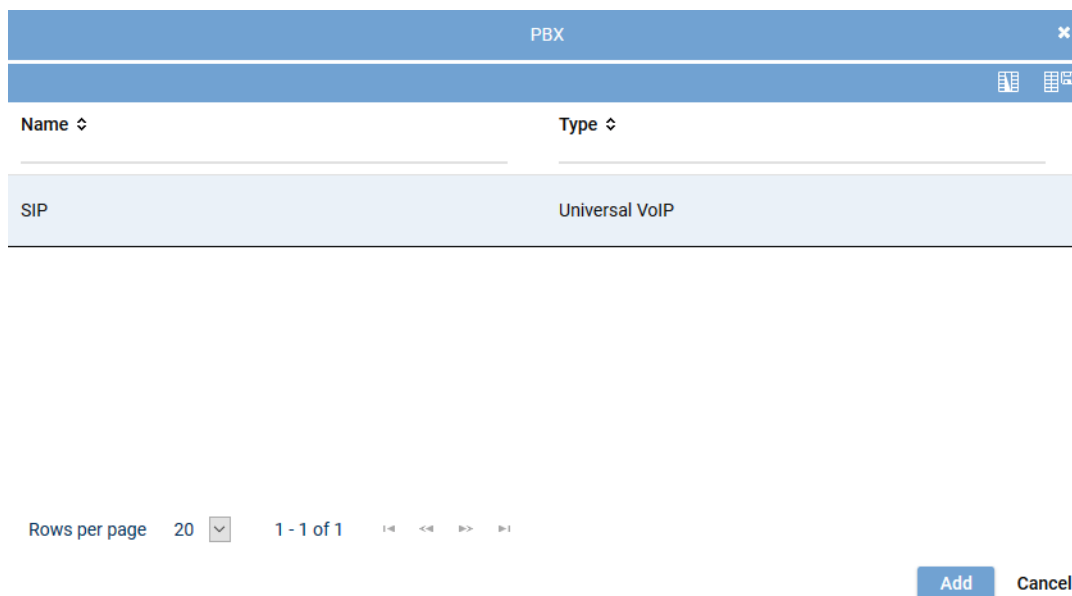


Fig. 94: Select PBX

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

Assign recording architecture for All-in-one Parallel Recording

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

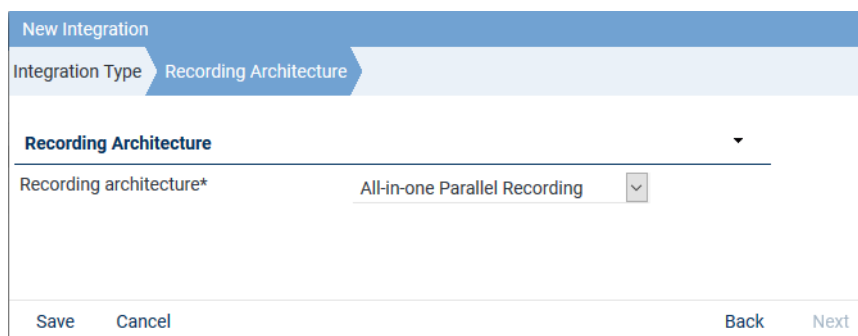


Fig. 95: Assign recording architecture - All-in-one Parallel

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




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

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



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see Duplicates in parallel recording architectures.

Configuration steps

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







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

Fig. 96: 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. 97: 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

- 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*
Transport protocol	UDP		
Port SIP signaling*	5060		
Activate SIP authentication	<input checked="" type="checkbox"/>		
User name for the SIP registration	123456		
Password for the SIP registration		
Activate SMS recording	<input type="checkbox"/>		

Save
Cancel

Fig. 98: Configuration step - Global recording settings

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

Parameter	Value/Description
<i>Transport protocol</i>	Select the deployed transport protocol for the SIP signaling between recording server and PBX from the drop-down list. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling on which the recording server waits for the signaling. Default value is 5060.
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication.
<i>User name for the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password for the SIP registration</i>	Enter the password if an authentication for SIP registration is supposed to be used.
<i>Activate SMS recording</i>	This functionality is not supported in this recording solution.

Tab. 19: Global recording settings



To make the registration on the SIP registrar or on the PBX work, SIP authentication as well as the PBX connection have to be activated.

The corresponding parameters have to be assigned to the correct values. In addition, the extensions of the recording server which are supposed to be registered must be configured.

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

Tab Device Groups

In parallel recording, you can configure connections to different PBXs.

- Select the tab Device Group 1 to configure the connection to PBX 1.

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. 99: 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. 100: 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.

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*.

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

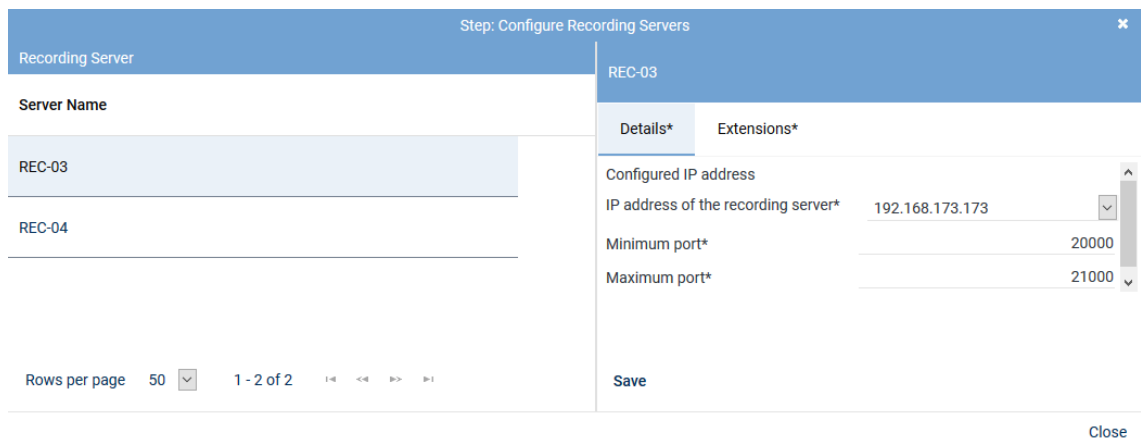


Fig. 101: Configuration step - Configure recording servers

- 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. 20: Configure recording servers



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



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

Configure add-on



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



Add-ons are not supported in this recording solution.


Configure miscellaneous settings





Configuring these settings is not required for this recording solution. Even without this configuration step, the integration has been configured comprehensively and can be activated.

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. 102: 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. 103: 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. 104: Deactivate integration

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

7.1.2.3 Configure recording solution Multi-Server 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:

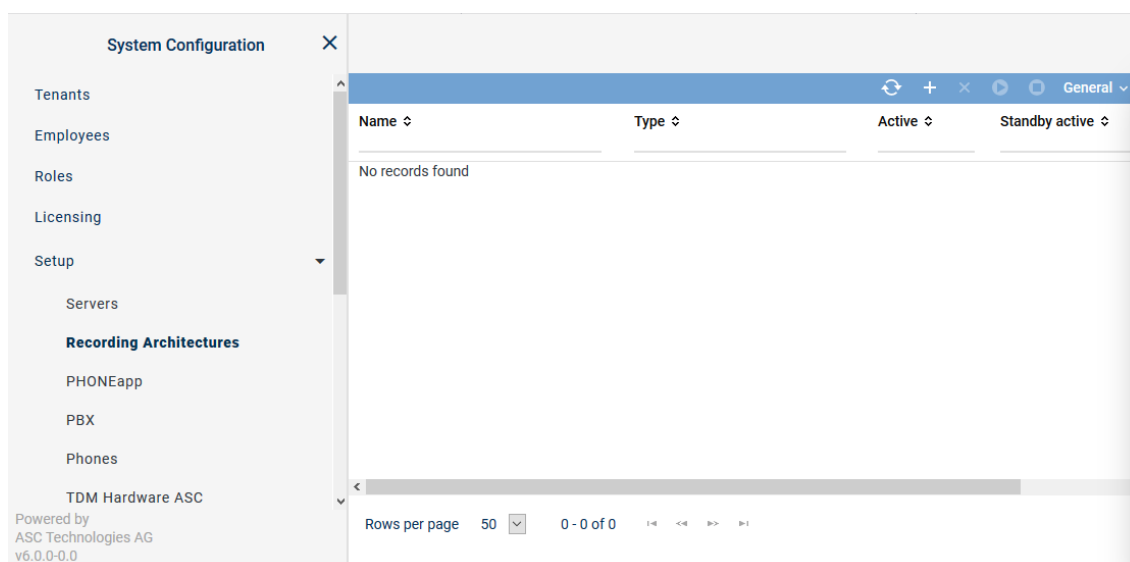




Fig. 105: Recording architectures - main view

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. 106: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon  is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.


	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

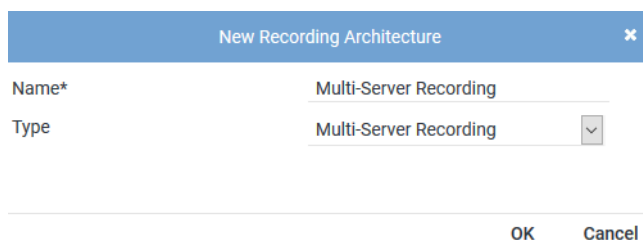
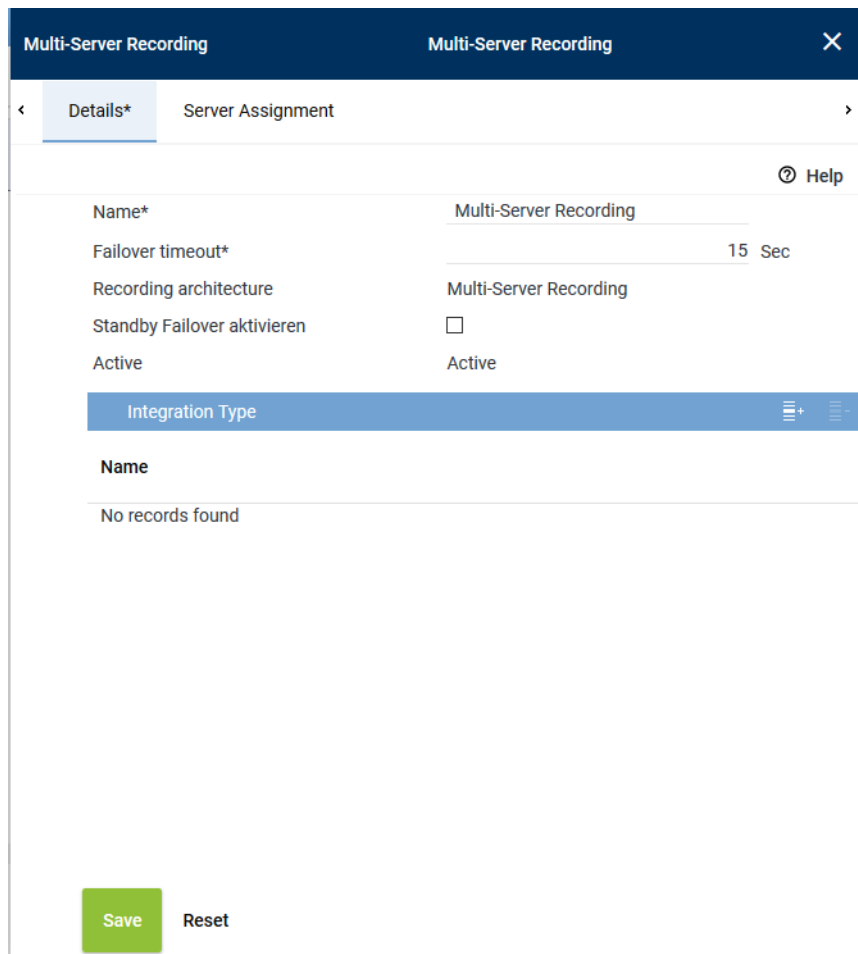


Fig. 107: Create recording architecture - Multi-Server Recording

- In the entry field *Name*, enter a descriptive name for the recording architecture.
- From the drop-down list *Type*, select the recording architecture type *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 the 'Multi-Server Recording' configuration window with the 'Details*' tab selected. The window has a dark blue header with the title 'Multi-Server Recording' and a close button. Below the header, there are two tabs: 'Details*' and 'Server Assignment'. The 'Details*' tab is active, showing a form with the following fields:

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

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


Fig. 108: 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. 109: 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*	CTI-01	+	-
Used in activated architecture	No		

Recording Server

Recording Server

Server
Standby

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

Save
Reset

Fig. 110: 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. 111: 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:

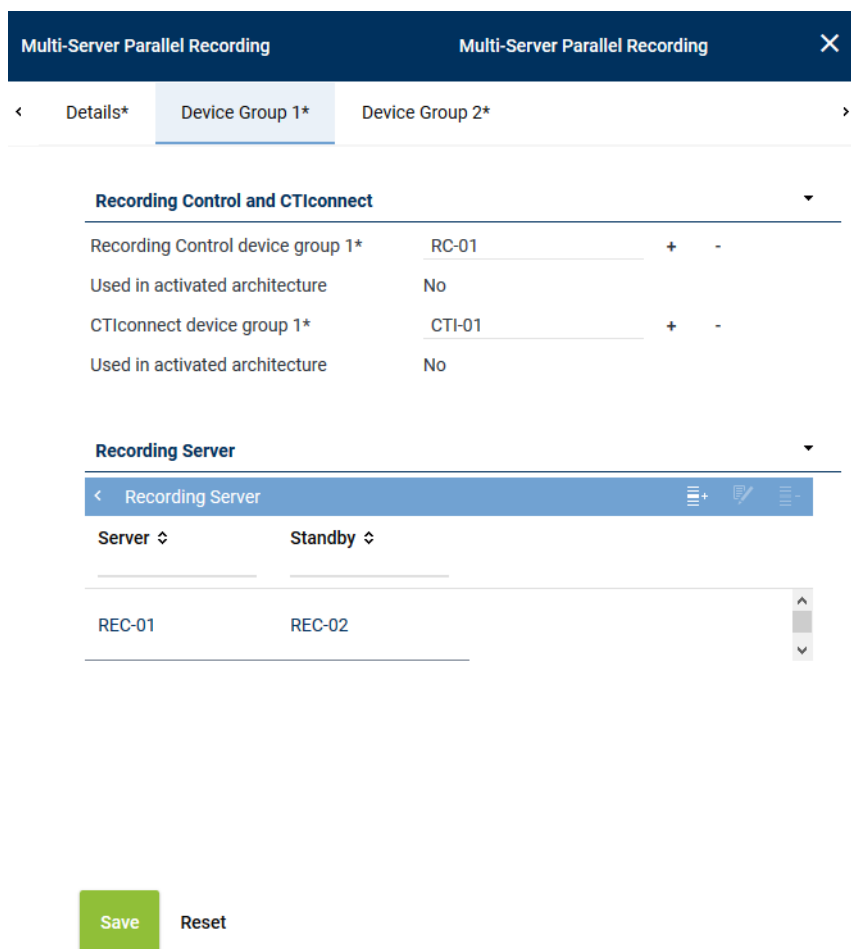









Fig. 112: Add recording server

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. 113: 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.

7.1.2.3.2 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:

System Configuration		Servers		General
Tenants		Name	IP Address	Path
Employees				
Roles		REC-01	192.168.173.171	C:\
Licensing		REC-02	192.168.173.172	C:\
Setup		REC-03	192.168.173.173	C:\
Servers		REC-04	192.168.173.174	C:\
Recording Architectures		RC-01	192.168.173.175	C:\
PHONEapp				
PBX				
Phones				
TDM Hardware ASC				
Powered by ASC Technologies AG v6.0.0-0.0		Rows per page 50 1 - 8 of 8		

Fig. 114: 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.

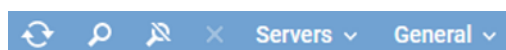







Fig. 115: Toolbar Servers module

	<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. 100.

	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

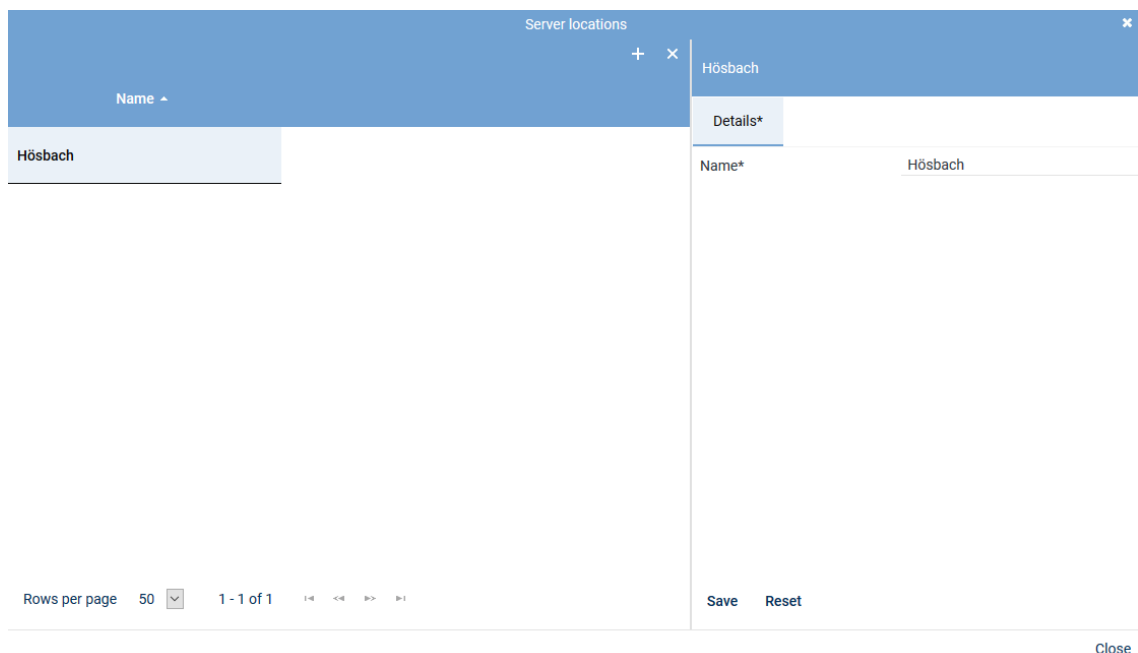



Fig. 116: Add server locations

- 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.

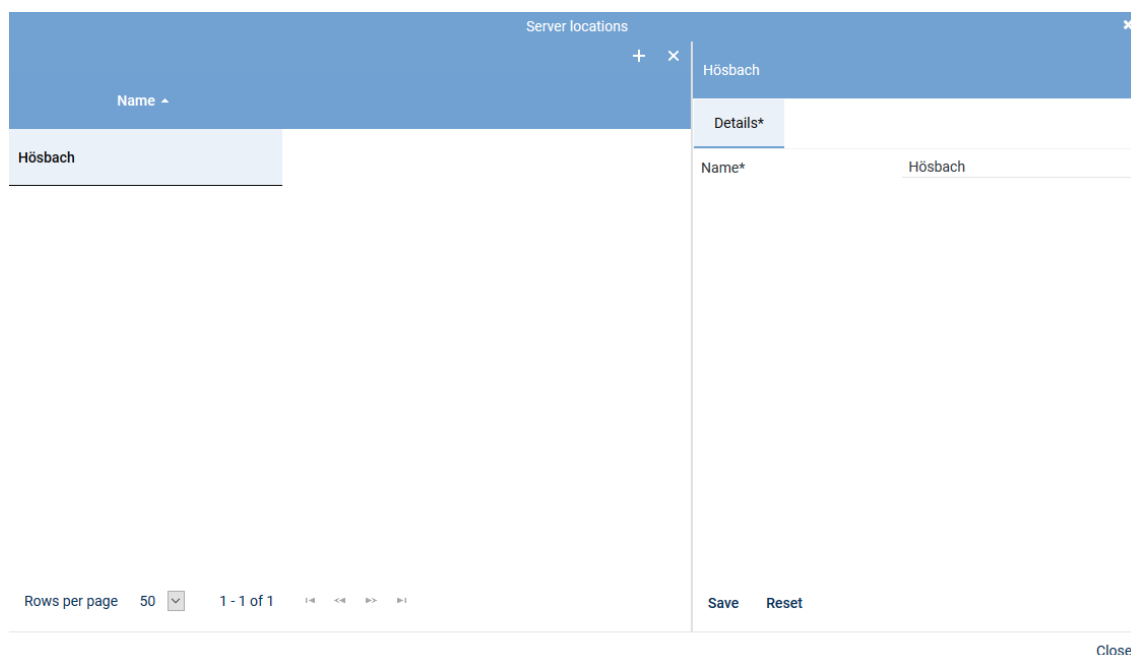
6. To close the window, click on the button *Close*.

Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a toolbar with a "+" icon and a "x" icon. The main area contains a table with one row: "Hösbach". To the right of the table is a "Details*" panel. The "Details*" panel has a "Name*" field with the value "Hösbach". At the bottom of the window, there is a "Rows per page" dropdown set to "50", a "1 - 1 of 1" indicator, and navigation icons. On the right side of the bottom bar, there are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the window.

Fig. 117: 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. 118: 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. 119: Servers - tab usage

Group field API Server

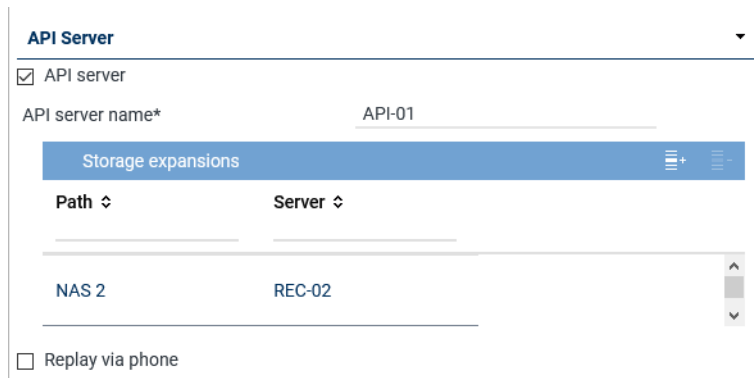


Fig. 120: Group field API Server


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




The ASC API Server must have been activated on every server where the Recording Control Service runs.


The ASC API Server does not only offer an interface for the internal modules; additionally, the client applications communicate with the neo system by means of this interface, too, using defined commands.

Furthermore, the ASC API Server is responsible for replay by means of the web browser. 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>Tick the check box to start the 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>In order to be able to reach the 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. 113.</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 the storage expansions, see chapter "Add storage expansion for replay", p. 104.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (<i>Remove</i>), you can remove the 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. <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. 111. To be able to do so, at least 1 PBX must have been configured in the system.</p>

Add storage expansion for replay

- Click on the icon  (*Add*) in the toolbar of the list.
- 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. 121: 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. 122: 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. 21: Configure audio analysis

Emotion Detection ✕

📄

Name ↕

REC-01

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

Add Cancel

Fig. 123: 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. 124: 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<code>command</code> or API recording control. 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 ASC_KEY_MANAGEMENT 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. 22: Configure recording control/key management

Group field Data Processing

Data Processing

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
REC-02	192.168.173.188

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
REC-03	192.168.173.189

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	







☐ Archiving

☒ Export

☒ Import

Recording architecture


Fig. 125: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to allow the modification of the additional functions of data processing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</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. 108. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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 data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</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. 108. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</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>

Parameter	Value/Description
<i>Export</i>	Activate the check box <i>Export</i> to allow the export from this server.
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 23: Configure data storage

Add target server to a list

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

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

Fig. 126: Select server



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

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

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*

(max. 5 characters)

API server*


+


-

Name ↕

Connection Status

Fig. 127: 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)	<p>Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.</p>
<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. 110.

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

Tab. 24: Configure replay


Search and replay functions



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

Add API server to a list

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

- If the replay server runs on a server with a local [API](#) server, it must not necessarily be assigned as the replay server always addresses the local [API](#) server first.
 - If the replay server runs on a separate server, you must assign at least one [API](#) server that the replay server can address.
 - If several [API](#) servers are available in the network, you can assign further [API](#) servers in addition to the local [API](#) server. The assigned [API](#) servers are addressed in order. For this reason, the local [API](#) server should always be first in the list.
- 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. 128: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 103](#).

- 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. 129: 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. 25: 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. 130: 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. 36.</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. In the drop-down list, all IP addresses of the server are displayed.</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>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</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>
Transport protocol	<p>Select the transport protocol type you would like to use for the SIP communication from the drop-down list.</p>

	<p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>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 <i>SIP</i> communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the <i>SIP</i> server.
<i>Password</i>	Enter the password for the authentication on the <i>SIP</i> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <i>SIP</i> registrar of the <i>PBX</i>.</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 <i>SIP</i> registrar of the <i>PBX</i>.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the <i>SIP</i> extension has to be registered with the <i>SIP</i> registrar of the <i>PBX</i>.</p> <p><input checked="" type="checkbox"/> = <i>SIP</i> extension has to be registered.</p> <p><input type="checkbox"/> = <i>SIP</i> 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*.

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

Replay Server Addresses
|
✖
▼

Internal IP address/ port of the replay server : 4000

External address/ port of the replay server : 4000

Save
Reset

Fig. 131: 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 destination IP address and the port of the replay server at which the Replay module can be reached internally.
<i>External address / Port of the replay server</i>	Enter the URL or the IP address and the port at which the Replay module can be reached via the browser from outside. When entering the external address consider whether the SSL certificate has been created for an IP address or for a DNS address. In the latter case, it is imperative to enter the DNS name! Otherwise the certificate check in the replay applications 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. 132: Servers module - tab Key Management

<i>Key creation interval</i>	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: <ul style="list-style-type: none"> • All
------------------------------	--

	<p>Select the intervals in which a new key is supposed to be generated automatically.</p> <p>Possible time interval: 1 to 365 days</p> <p>Default value: 365 days</p> <ul style="list-style-type: none"> • <i>Create key manually</i> <p>Select that a key is supposed to be generated manually.</p> <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</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.

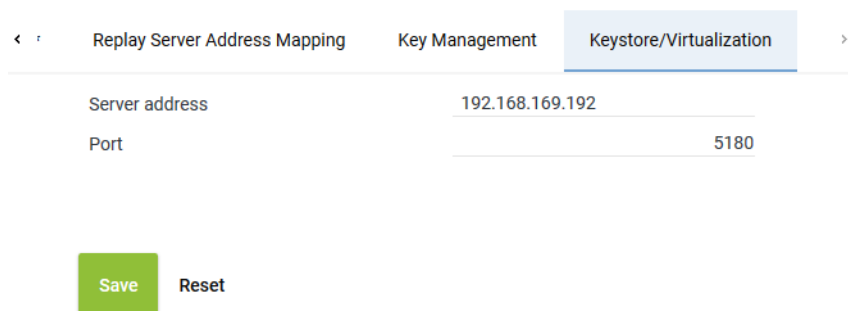
For licensing, there are the following options:

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 configuration window with three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is selected. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom left, there are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 133: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for this connection.</p> <ul style="list-style-type: none"> • If you use the neo key management as well as the virtualization: IP address of the server that the service <i>DongleMan</i> has been installed on. • If you use only virtualization, you can authenticate the VM via the ASC License Management System, too. In this case, enter the following address:
-----------------------	---

	<i>licensing.asc.de</i> <ul style="list-style-type: none"> If you use only the ASC key management: IP address of the server with the master password database
Port	Enter the port for the connection. Default value: 5180



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 Assign recording resources

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.

Assign extensions to tenants

If you would like to make an assignment based on extensions, you can assign the respective tenant the extension designated for recording in the Tenants module.



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

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



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

The manual assignment of extensions is not possible until a PBX has been created since extensions are assigned in relation to the PBX.

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

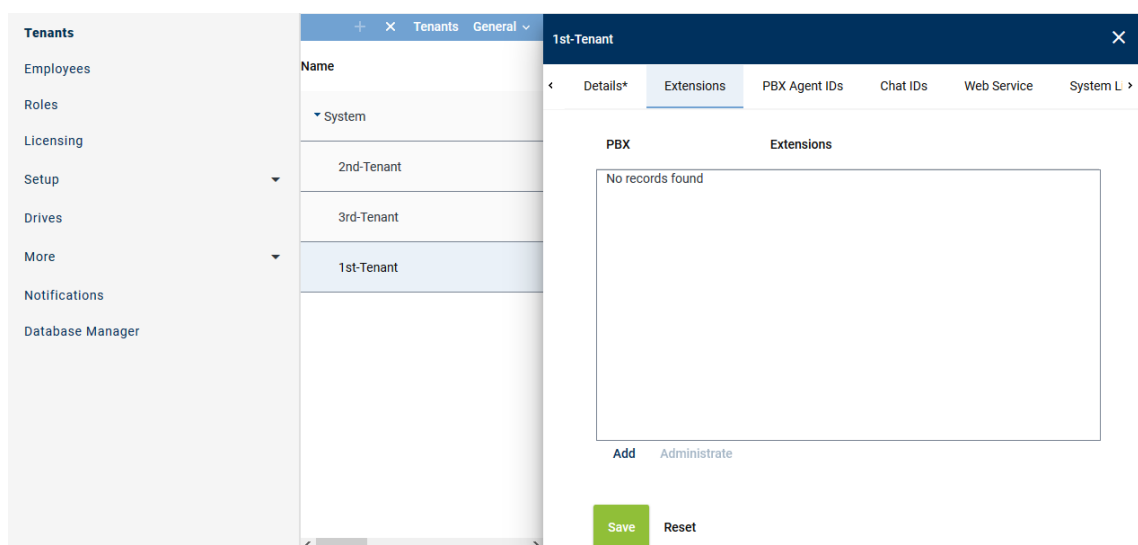


Fig. 134: Tenants - main view - tab Extensions

Add extensions

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

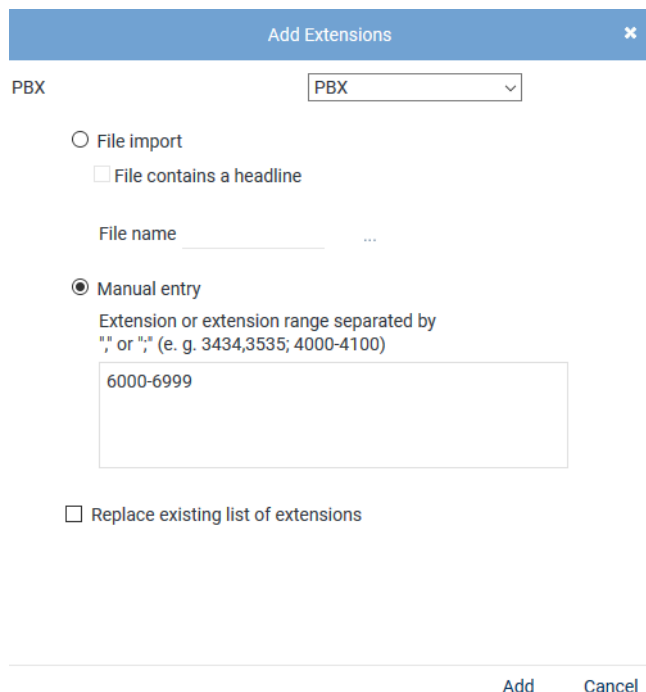




Fig. 135: Assign extensions to tenants

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

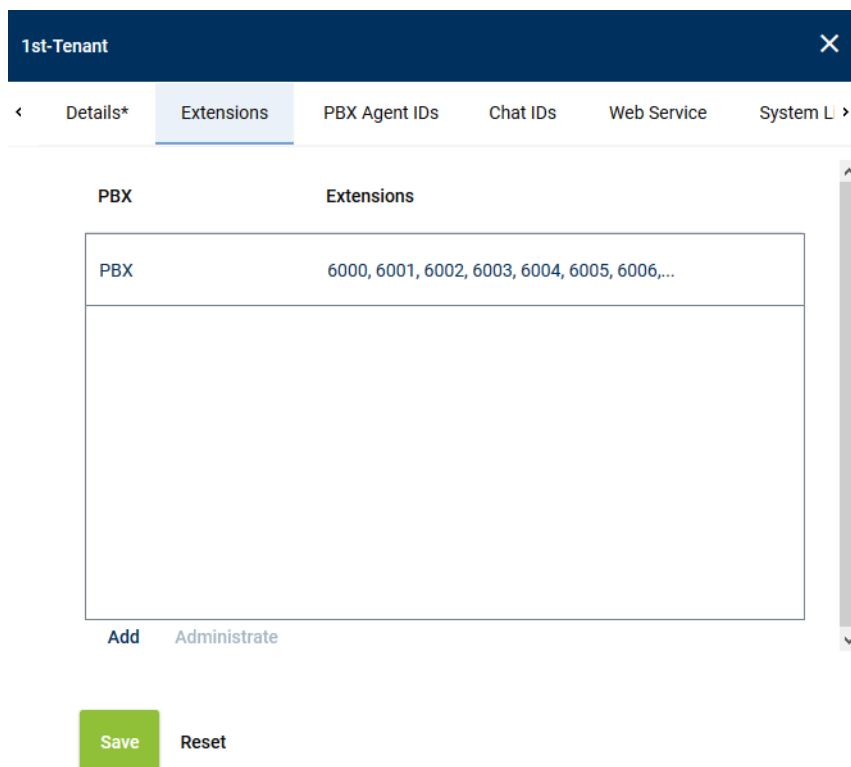
File import	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
File contains a headline	<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>
File name	<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>.

	<ul style="list-style-type: none"> • 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> <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.</p> <p>Enter country codes as number ranges as follows: +4984496800-+4984496810</p> <p>NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.</p>

- 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. 136: 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. 137: Select extensions

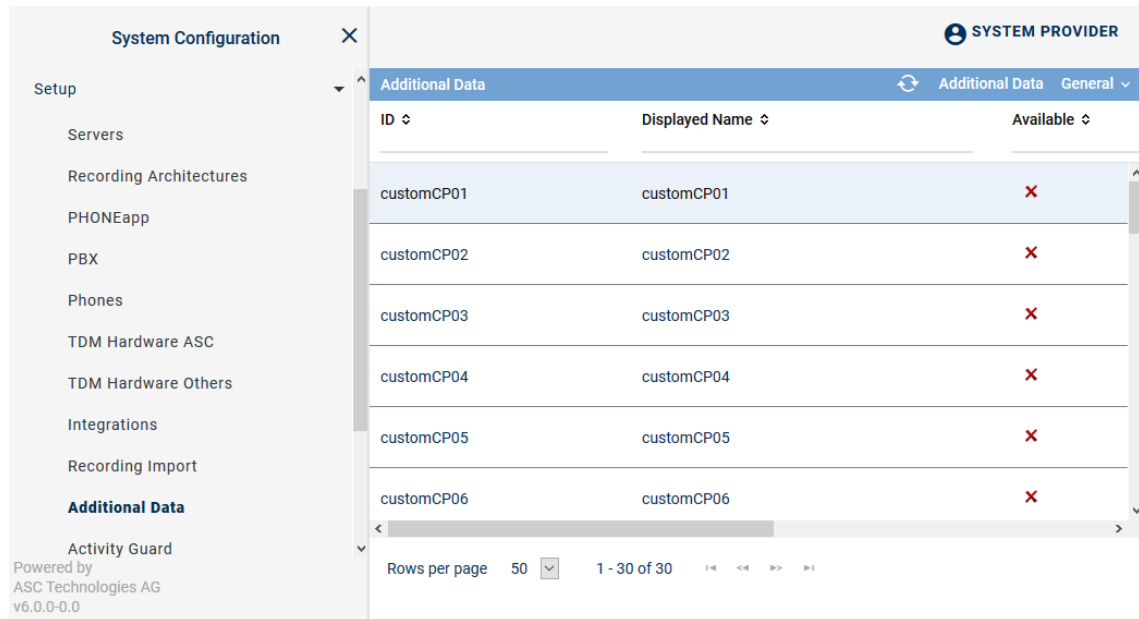
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

7.1.2.3.4 Configure additional data

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

In order to have the fields displayed in the drop-down list to be selected, they must 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

Fig. 138: Additional Data module main view

The following additional data is always available:

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

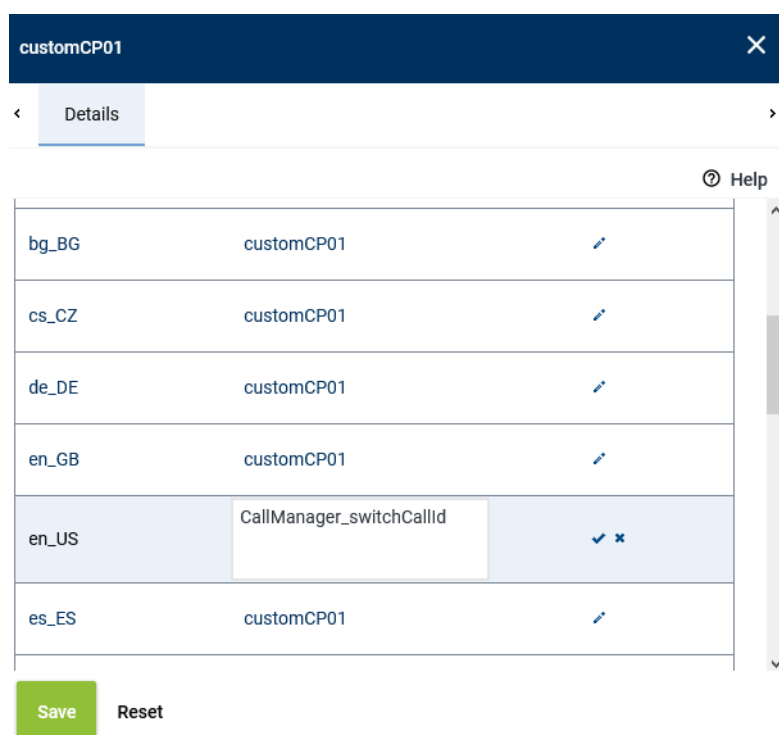
For this recording solution, you can additionally configure the following additional data:

- *CallManager_switchCallId*

2. Select a data set

⇒ In the detail view, the information that can be configured appears.

Change display name



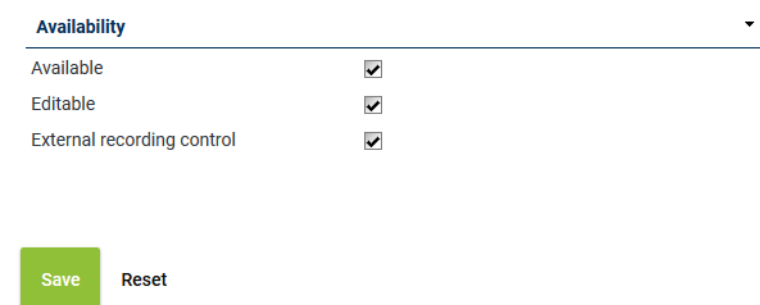
customCP01		
bg_BG	customCP01	
cs_CZ	customCP01	
de_DE	customCP01	
en_GB	customCP01	
en_US	CallManager_switchCallId	
es_ES	customCP01	

Save Reset

Fig. 139: Configure additional data

1. To change the display name, click on the pen icon in the line of the language that 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. 140: Additional data - configure availability

1. To make the data field available for the entire system, activate the check box of the option *Available*.
2. To make the data field editable for the search and replay applications subsequently, tick the check box of the option *Editable*.
3. To use the data field for external recording control, tick 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*.

7.1.2.3.5 Create integration for Multi-Server Recording

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

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

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

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

⇒ The following window appears:

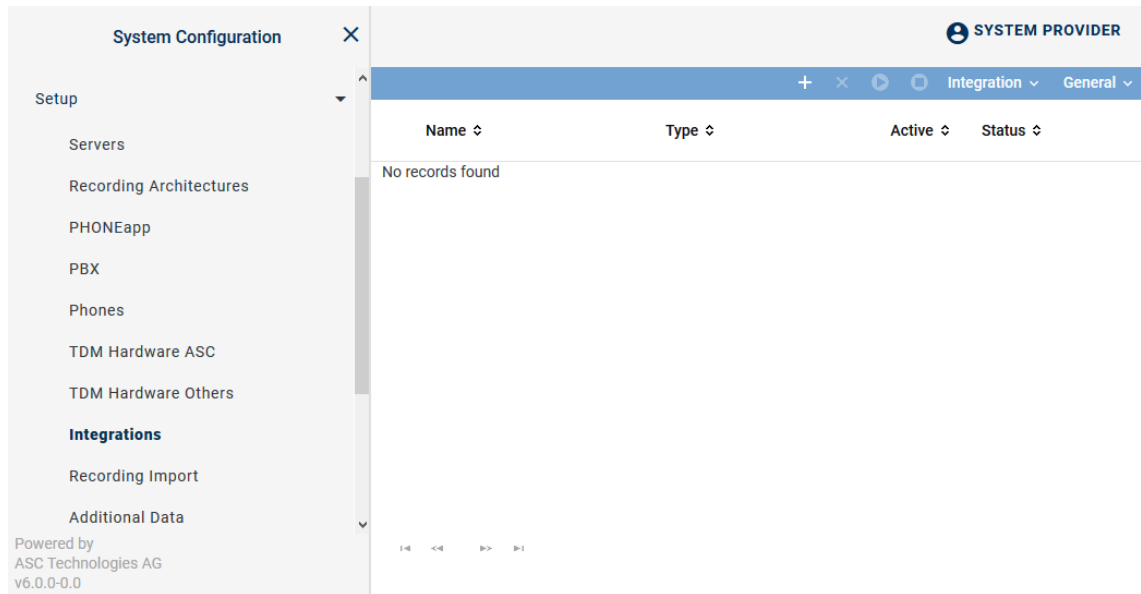




Fig. 141: Integrations - main view

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. 142: 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.

	<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.

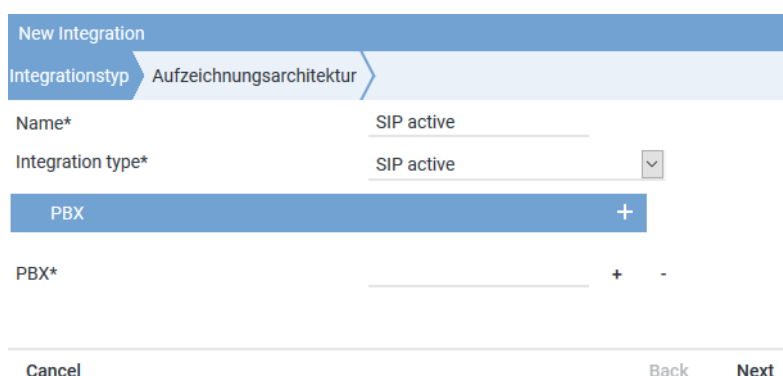



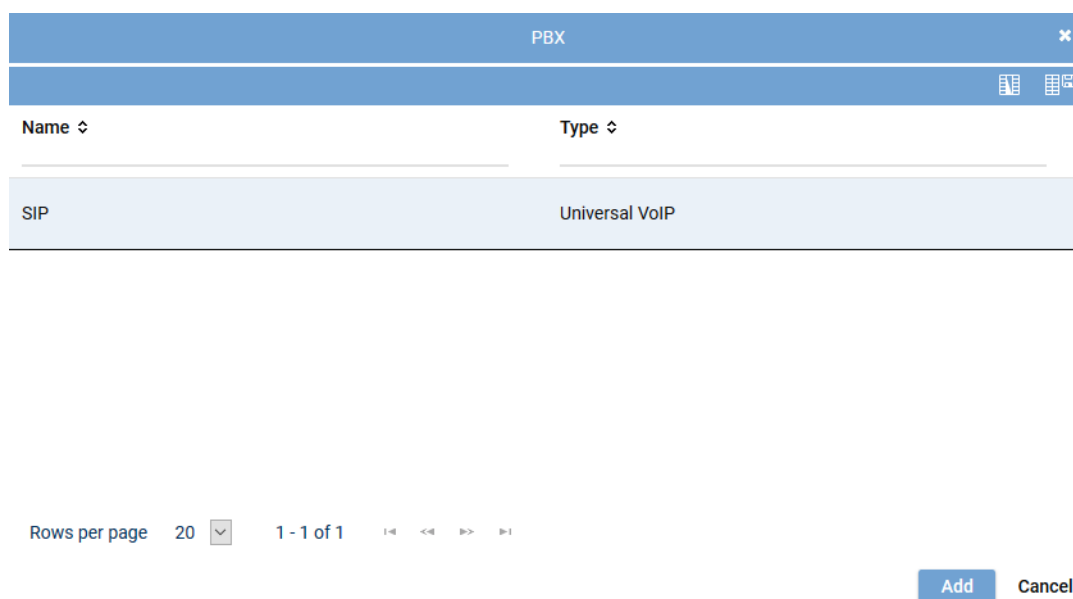
Fig. 143: Create integration type

- 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. 26: Create integration type

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



Name	Type
SIP	Universal VoIP

Rows per page 20 1 - 1 of 1

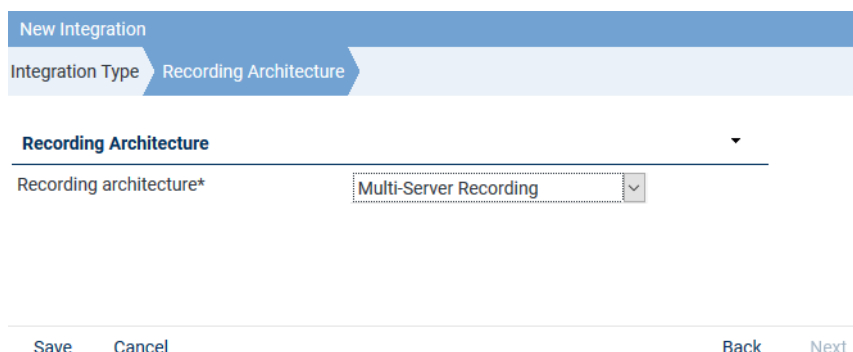
Add Cancel

Fig. 144: Select PBX

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

Assign recording architecture for Multi-Server Recording

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Recording

Save Cancel Back Next

Fig. 145: Assign recording architecture - Multi-Server Recording


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



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

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

Configuration steps

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







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

Fig. 146: Configuration steps of the integration

Configure recording architecture

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

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

Step: Configure Recording Architecture ✕

Details *


Recording architecture*

Save Cancel

Fig. 147: 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

- 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. 148: Configuration step - Global recording settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the deployed transport protocol for the SIP signaling between recording server and PBX from the drop-down list. 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 on which the recording server waits for 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 must configure a separate SIP port for each integration.</p> <p>NOTICE! If you would like to use a media streamer for replay, configure a separate SIP port for it, too. In case of issues in the communication with the Media Streamer this can otherwise affect recording.</p>
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication .
<i>User name for the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password for the SIP registration</i>	Enter the password if an authentication for SIP registration is supposed to be used.
<i>Activate PBX connection</i>	Activate the check box, if the recording server is supposed to register on the PBX.
<i>SIP registration expiration</i>	Enter the time in seconds after which the SIP registration expires, 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 . Default value is 5060.

Parameter	Value/Description
<i>Activate SMS recording</i>	This functionality is not supported in this recording solution.


Tab. 27: Global recording settings

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

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*.

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

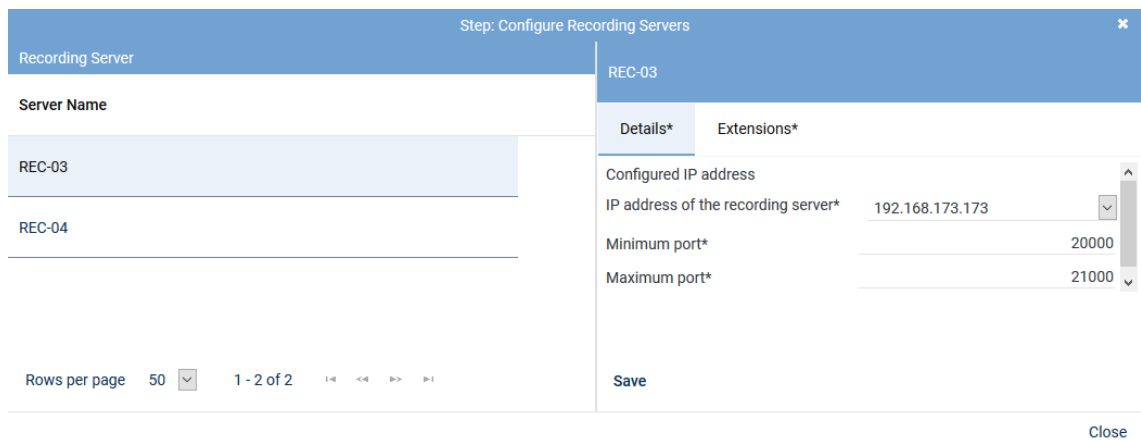


Fig. 149: Configuration step - Configure recording servers

- 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. 28: Configure recording servers



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



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

Configure add-on



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



Add-ons are not supported in this recording solution.


Configure miscellaneous settings





Configuring these settings is not required for this recording solution. Even without this configuration step, the integration has been configured comprehensively and can be activated.

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. 150: 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. 151: 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. 152: 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 Parallel 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:

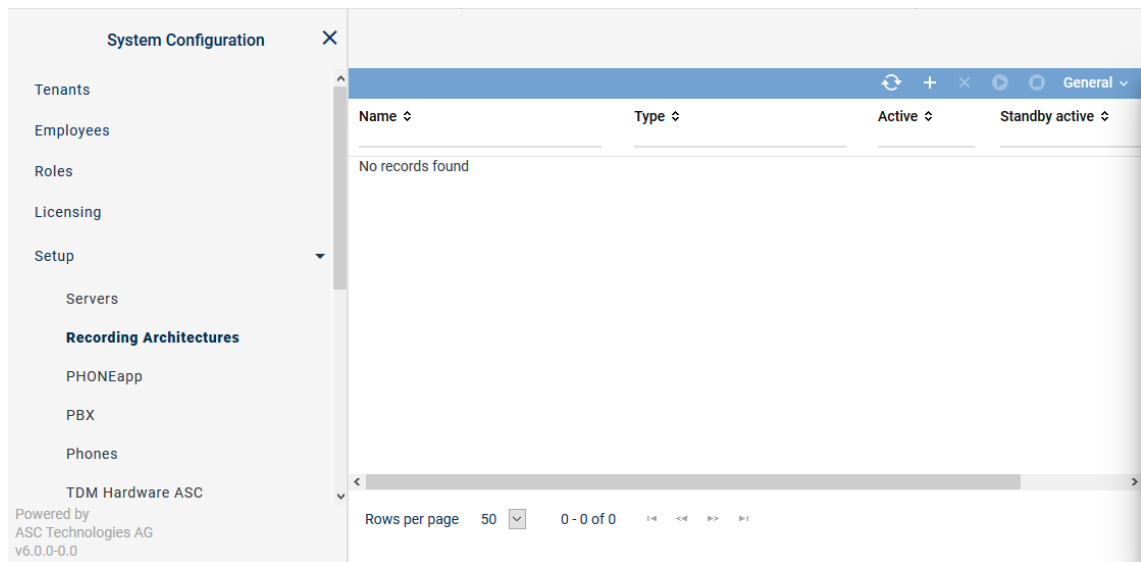




Fig. 153: Recording architectures - main view

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. 154: Toolbar Recording Architectures module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon  is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.


	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

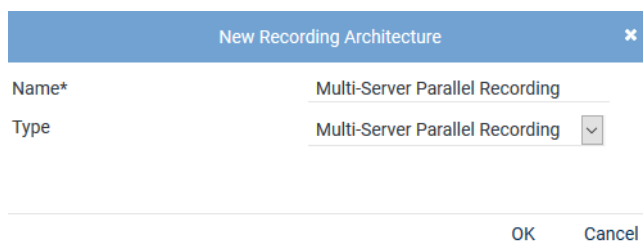
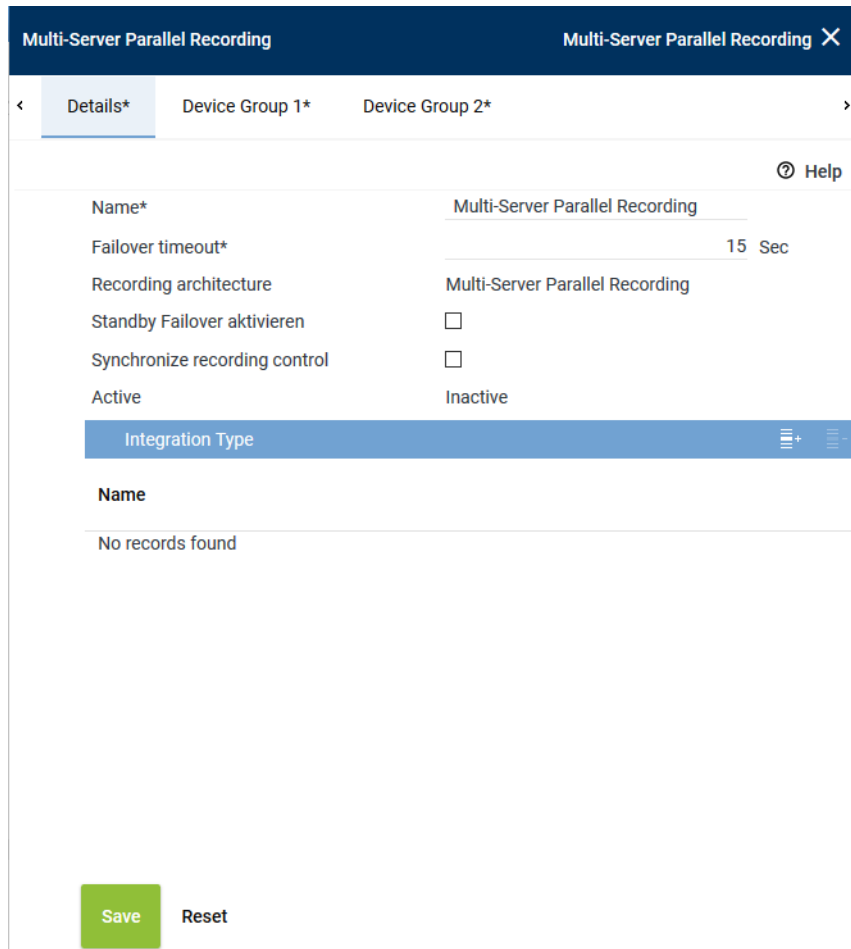


Fig. 155: Create recording architecture - Multi-Server Parallel Recording

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.



The screenshot shows the 'Multi-Server Parallel Recording' configuration window. The 'Details*' tab is selected. The configuration includes the following fields:

- Name***: Multi-Server Parallel Recording
- Failover timeout***: 15 Sec
- Recording architecture**: Multi-Server Parallel Recording
- Standby Failover aktivieren**: ☐
- Synchronize recording control**: ☐
- Active**: Inactive

Below these fields is a section titled 'Integration Type' with a table that currently shows 'No records found'. At the bottom of the window are 'Save' and 'Reset' buttons.

Fig. 156: Recording architecture - tab Details - Multi-Server Parallel Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For more information about the configuration of failover architectures, see Standby management for failover architectures.




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

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

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

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

Add integration type

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

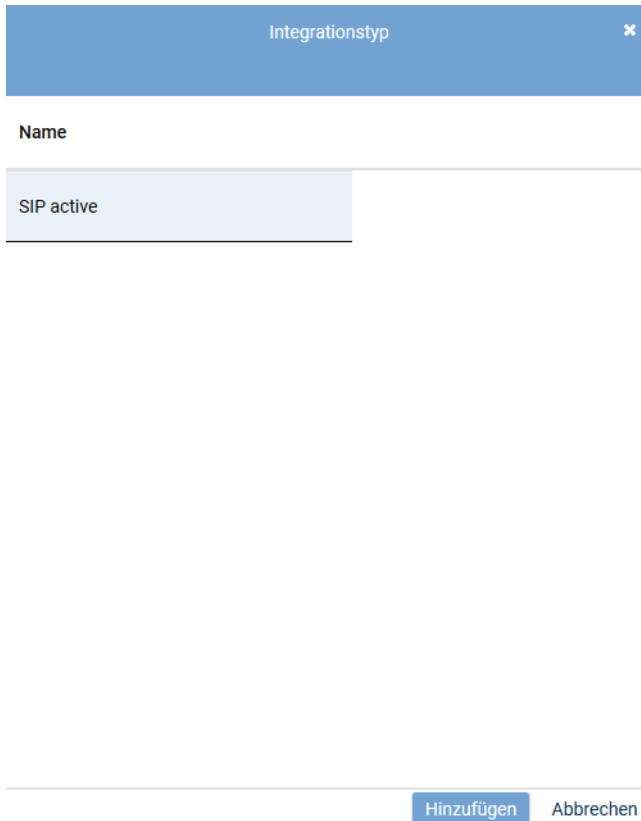


Fig. 157: Select integration type



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 Multi-Server Parallel Recording

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

Tab Device Group 1

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

Group field Recording Control and CTIconnect

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

Multi-Server Parallel Recording

Multi-Server Parallel Recording

×

<

Details*

Device Group 1*

Device Group 2*

>

Recording Control and CTIconnect

▼

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

Recording Server

▼

<

Recording Server

+

✎

⋮

Server ↕	Standby ↕
REC-01	REC-02

Save

Reset

Fig. 158: 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. 159: Recording architecture - assign server - example


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

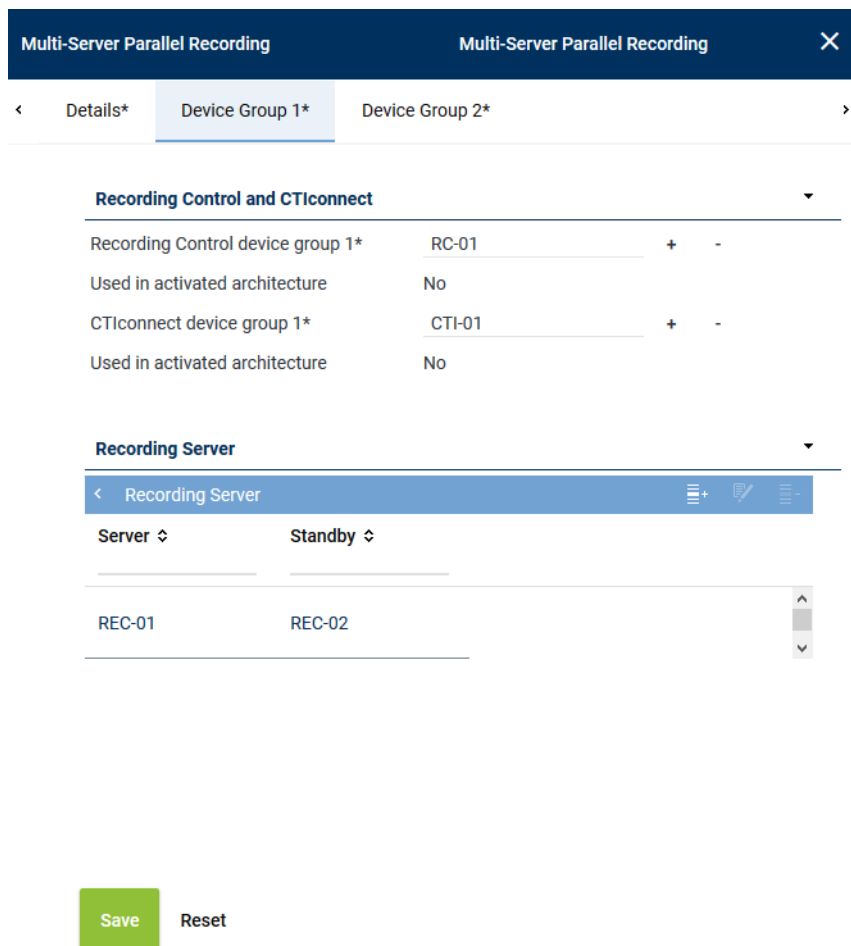


A server can be configured in several recording architectures, but you cannot activate several recording architectures with the same server at the same time.
If you would like to activate several recording architectures at the same time, you have to use different servers to do so.

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

Group field Recording Server

1. Click on the icon  in the table headline Recording Server to add a recording server and the standby server.
⇒ The following window appears:



Multi-Server Parallel Recording Multi-Server Parallel Recording X

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

Recording Control and CTIconnect

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



Recording Server



< Recording Server + -

Server ↕	Standby ↕
REC-01	REC-02

Save Reset

Fig. 160: 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. 161: Recording architecture - activate recording architecture - example

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



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



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



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

7.1.2.4.2 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:

System Configuration			
Tenants			
Employees			
Roles			
Licensing			
Setup			
Servers			
Recording Architectures			
PHONEapp			
PBX			
Phones			
TDM Hardware ASC			
Powered by ASC Technologies AG v6.0.0-0.0			

Name ↕	IP Address ↕	Path ↕
REC-01	192.168.173.171	C:\
REC-02	192.168.173.172	C:\
REC-03	192.168.173.173	C:\
REC-04	192.168.173.174	C:\
RC-01	192.168.173.175	C:\

Rows per page 50 1 - 8 of 8

Fig. 162: 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.

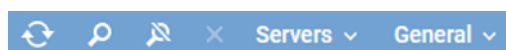







Fig. 163: Toolbar Servers module

	<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. 139.

	<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 information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

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.

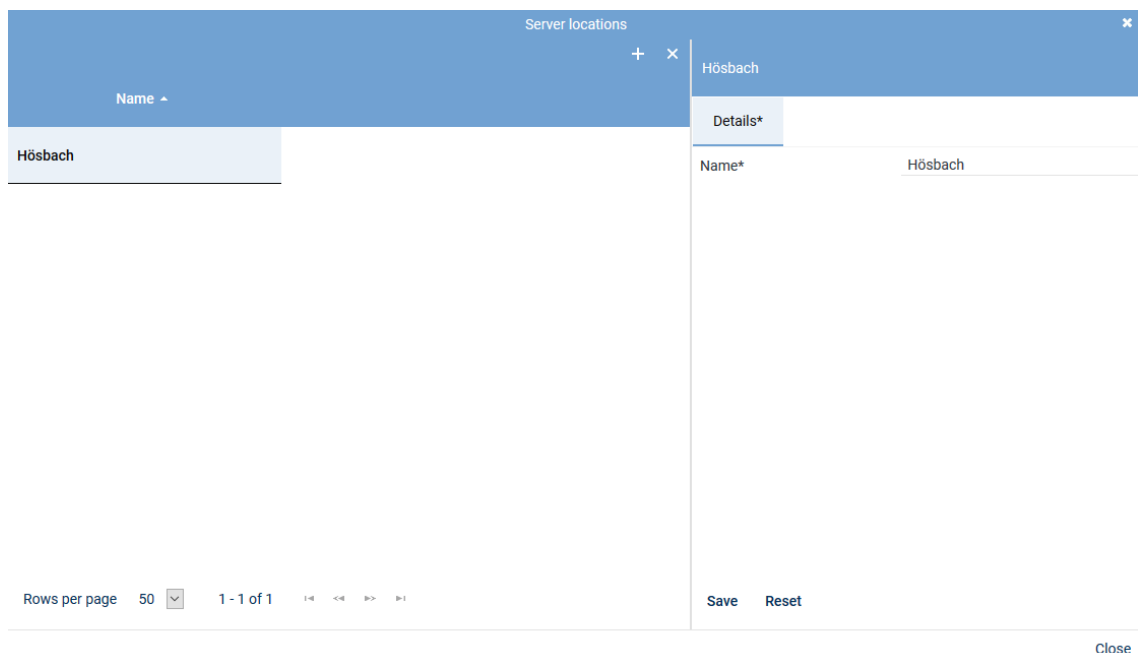



Fig. 164: Add server locations

- 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.

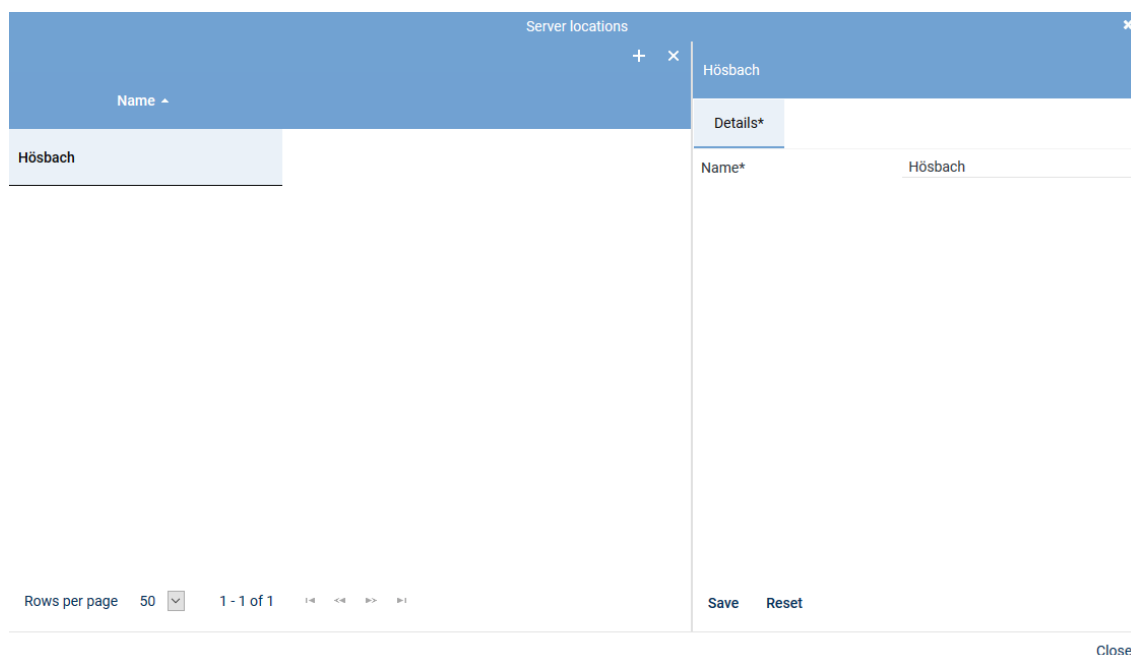
6. To close the window, click on the button *Close*.

Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (X) in the top right corner. Below the title bar is a toolbar with a "+" icon and a "Name" dropdown menu. The main area contains a table with one row: "Hösbach". To the right of the table is a "Details*" panel. The "Details*" panel has a "Name*" field with the value "Hösbach". At the bottom of the window, there is a "Rows per page" dropdown set to "50", a "1 - 1 of 1" indicator, and navigation icons. On the right side of the bottom bar, there are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the window.

Fig. 165: 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. 166: 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. 167: Servers - tab usage

Group field API Server

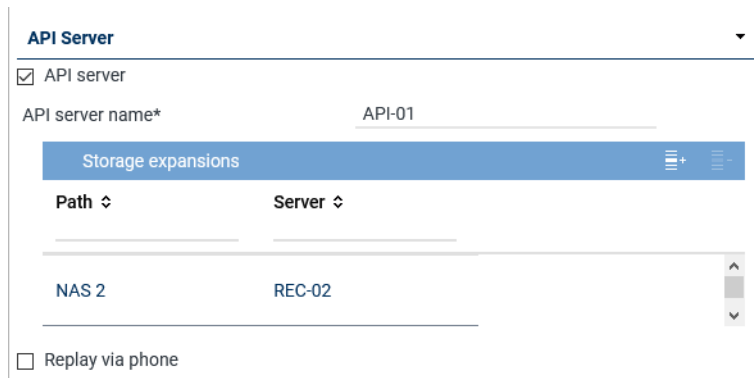


Fig. 168: Group field API Server


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




The ASC API Server must have been activated on every server where the Recording Control Service runs.


The ASC API Server does not only offer an interface for the internal modules; additionally, the client applications communicate with the neo system by means of this interface, too, using defined commands.

Furthermore, the ASC API Server is responsible for replay by means of the web browser. 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>Tick the check box to start the 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>In order to be able to reach the 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. 152.</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 the storage expansions, see chapter "Add storage expansion for replay", p. 143.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (<i>Remove</i>), you can remove the 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. <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. 150. To be able to do so, at least 1 PBX must have been configured in the system.</p>

Add storage expansion for replay

- Click on the icon  (*Add*) in the toolbar of the list.
- 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. 169: 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. 170: 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. 29: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

Rows per page 20 ▼ 1 - 8 of 8 ⏪ ⏩ ⏴ ⏵

Add Cancel

Fig. 171: 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. 172: 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. 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. 30: Configure recording control/key management

Group field Data Processing

Data Processing

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
REC-02	192.168.173.188

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
REC-03	192.168.173.189

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	







☐ Archiving

☒ Export

☒ Import

Recording architecture

Fig. 173: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to allow the modification of the additional functions of data processing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</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. 147. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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 data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</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. 147. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on 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"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</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>

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*

(max. 5 characters)


API server*


+

-

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

Fig. 175: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 149.

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

Tab. 32: 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.

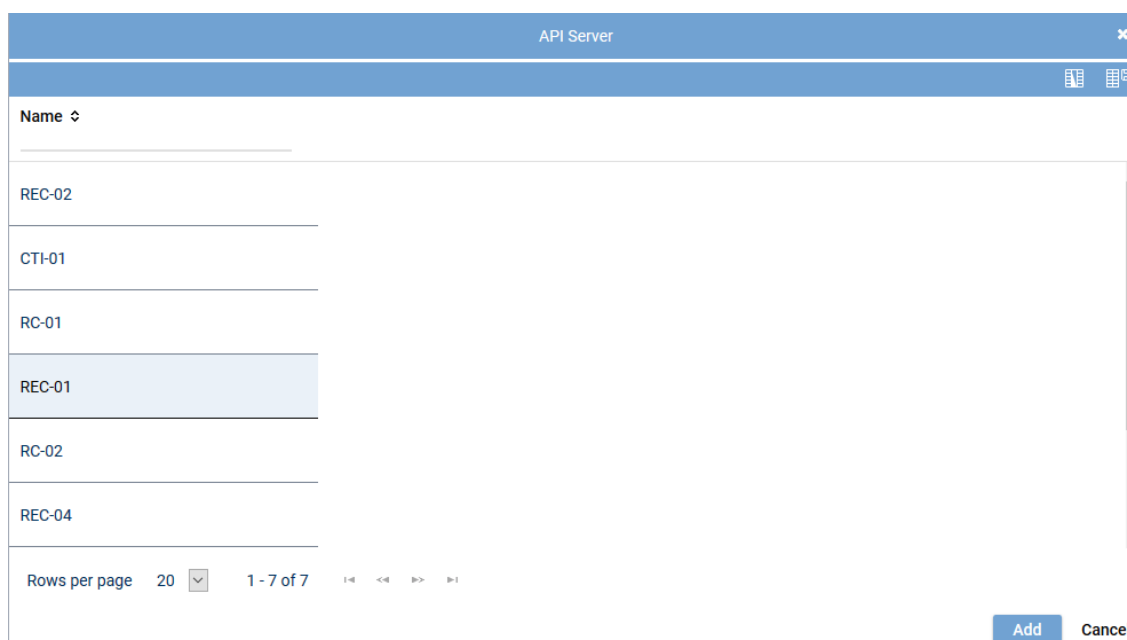


Fig. 176: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 142](#).

- 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. 177: 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. 33: 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. 178: 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. 36.</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. In the drop-down list, all IP addresses of the server are displayed.</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>
Maximum port	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</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>
Transport protocol	<p>Select the transport protocol type you would like to use for the SIP communication from the drop-down list.</p>

	<p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>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 <i>SIP</i> communication.</p> <p>Port for data exchange: <i>5062</i></p>
<i>User name</i>	Enter the user name for the authentication on the <i>SIP</i> server.
<i>Password</i>	Enter the password for the authentication on the <i>SIP</i> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <i>SIP</i> registrar of the <i>PBX</i>.</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 <i>SIP</i> registrar of the <i>PBX</i>.</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 <i>SIP</i> extension has to be registered with the <i>SIP</i> registrar of the <i>PBX</i>.</p> <p><input checked="" type="checkbox"/> = <i>SIP</i> extension has to be registered.</p> <p><input type="checkbox"/> = <i>SIP</i> 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*.

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

Replay Server Addresses
|
✖
▼

Internal IP address/ port of the replay server : 4000

External address/ port of the replay server : 4000


Save
Reset

Fig. 179: 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 destination IP address and the port of the replay server at which the Replay module can be reached internally.
<i>External address / Port of the replay server</i>	Enter the URL or the IP address and the port at which the Replay module can be reached via the browser from outside. When entering the external address consider whether the SSL certificate has been created for an IP address or for a DNS address. In the latter case, it is imperative to enter the DNS name! Otherwise the certificate check in the replay applications 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. 180: Servers module - tab Key Management

<i>Key creation interval</i>	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: <ul style="list-style-type: none"> • All
------------------------------	--

	<p>Select the intervals in which a new key is supposed to be generated automatically.</p> <p>Possible time interval: 1 to 365 days</p> <p>Default value: 365 days</p> <ul style="list-style-type: none"> • <i>Create key manually</i> <p>Select that a key is supposed to be generated manually.</p> <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</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.

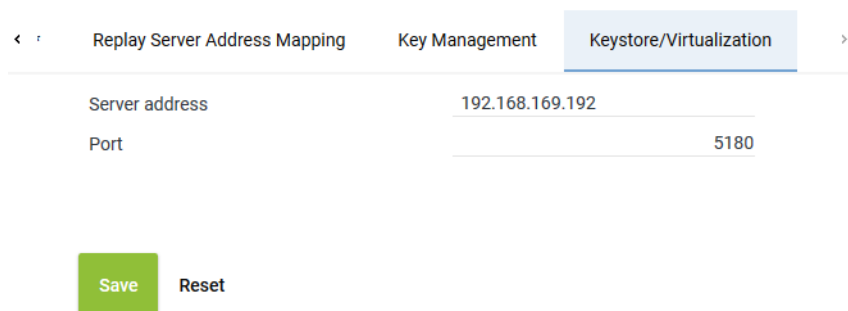
For licensing, there are the following options:

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 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 these fields are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 181: Servers module - tab Keystore/Virtualization

Server address	<p>Enter the address of the server for this connection.</p> <ul style="list-style-type: none"> • If you use the neo key management as well as the virtualization: IP address of the server that the service <i>DongleMan</i> has been installed on. • If you use only virtualization, you can authenticate the VM via the ASC License Management System, too. In this case, enter the following address:
-----------------------	---

	<i>licensing.asc.de</i> <ul style="list-style-type: none"> If you use only the ASC key management: IP address of the server with the master password database
Port	Enter the port for the connection. Default value: 5180



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*.

7.1.2.4.3 Assign recording resources

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.

Assign extensions to tenants

If you would like to make an assignment based on extensions, you can assign the respective tenant the extension designated for recording in the Tenants module.



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

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



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

The manual assignment of extensions is not possible until a PBX has been created since extensions are assigned in relation to the PBX.

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

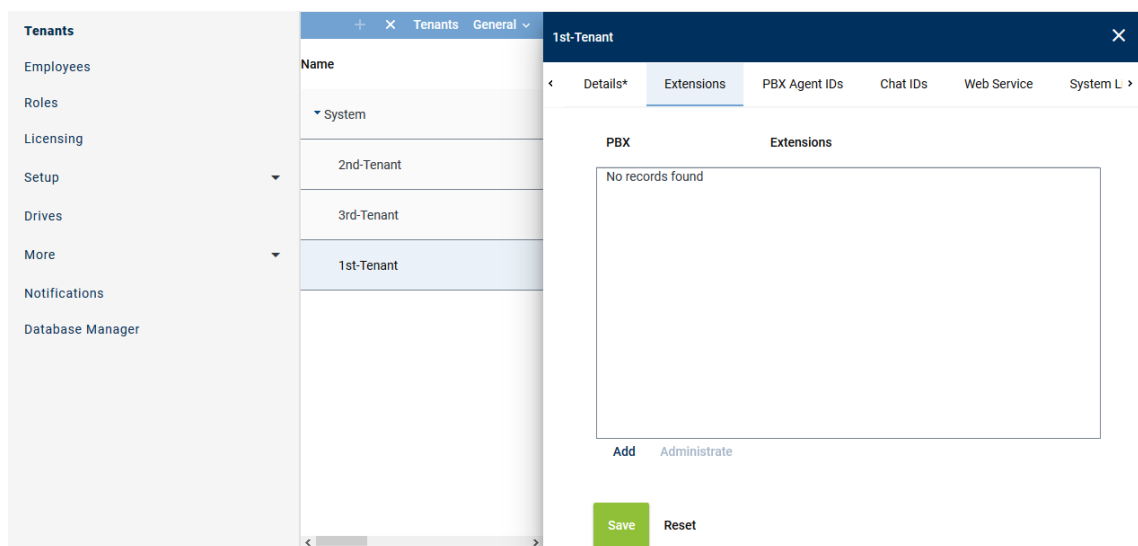


Fig. 182: Tenants - main view - tab Extensions

Add extensions

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

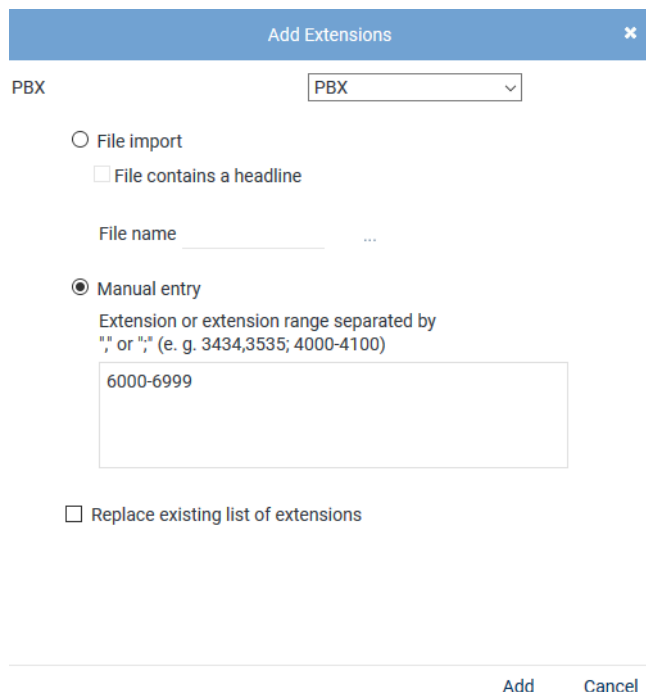




Fig. 183: Assign extensions to tenants

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

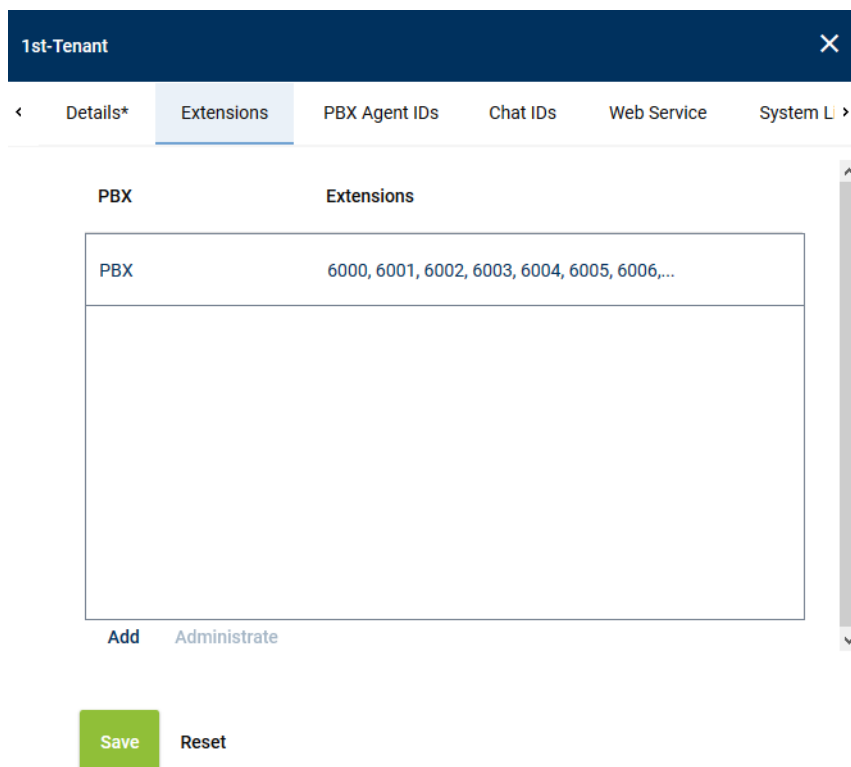
File import	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
File contains a headline	<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>
File name	<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>.

	<ul style="list-style-type: none"> • 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> <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.</p> <p>Enter country codes as number ranges as follows: +4984496800-+4984496810</p> <p>NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.</p>

- 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. 184: 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. 185: Select extensions

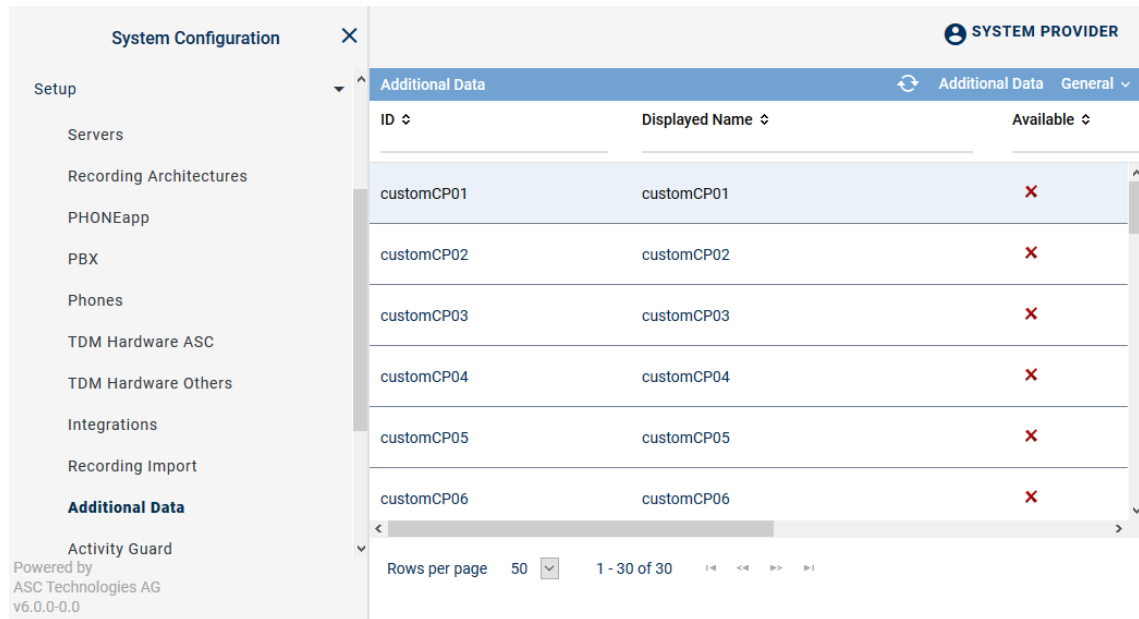
- To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

7.1.2.4.4 Configure additional data

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

In order to have the fields displayed in the drop-down list to be selected, they must 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

Fig. 186: Additional Data module main view

The following additional data is always available:

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

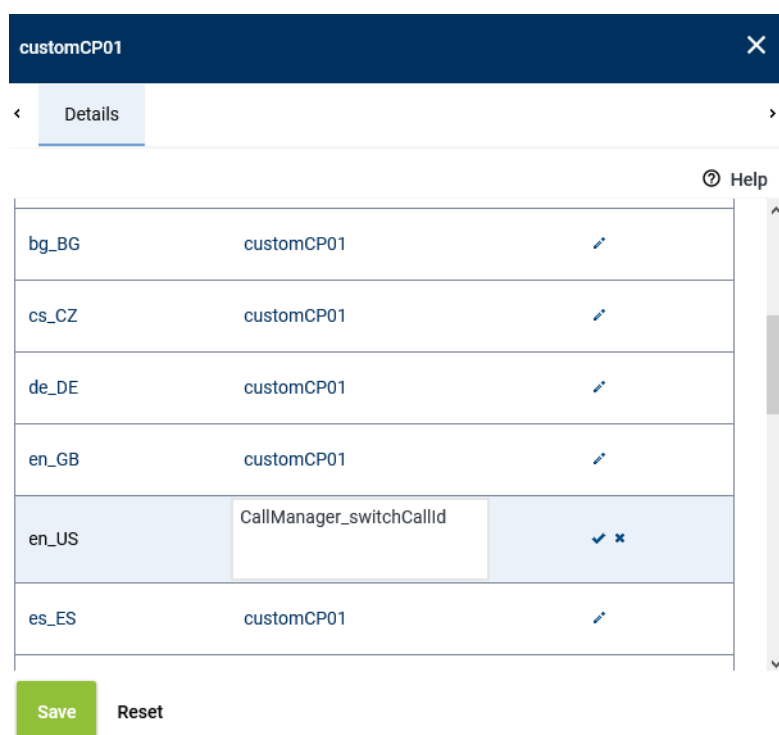
For this recording solution, you can additionally configure the following additional data:

- *CallManager_switchCallId*

2. Select a data set

⇒ In the detail view, the information that can be configured appears.

Change display name



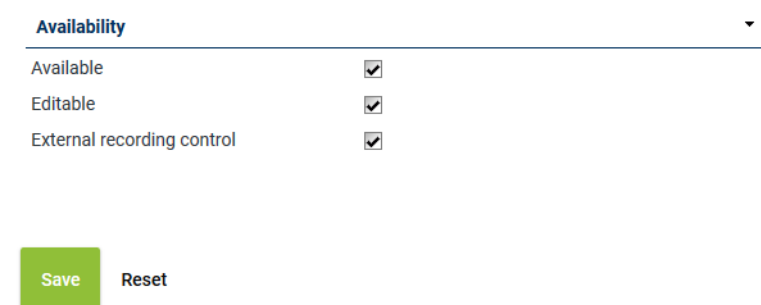
customCP01		
bg_BG	customCP01	
cs_CZ	customCP01	
de_DE	customCP01	
en_GB	customCP01	
en_US	CallManager_switchCallId	
es_ES	customCP01	

Save Reset

Fig. 187: Configure additional data

1. To change the display name, click on the pen icon in the line of the language that 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. 188: Additional data - configure availability

1. To make the data field available for the entire system, activate the check box of the option *Available*.
2. To make the data field editable for the search and replay applications subsequently, tick the check box of the option *Editable*.
3. To use the data field for external recording control, tick 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*.

7.1.2.4.5 Create integration for Multi-Server Parallel Recording

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

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

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

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

⇒ The following window appears:

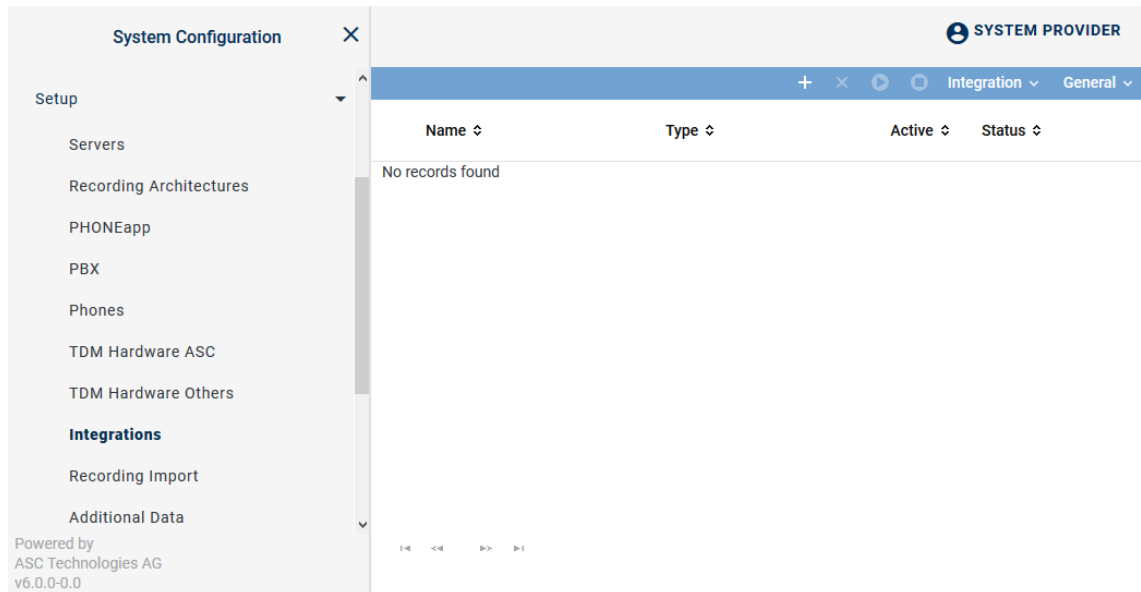




Fig. 189: Integrations - main view

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. 190: 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.

	<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.

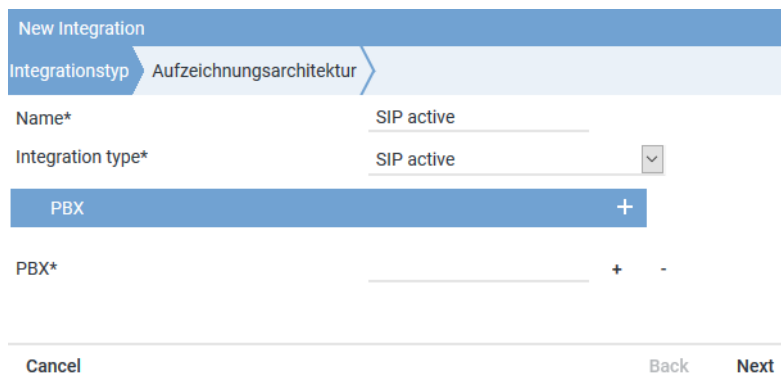



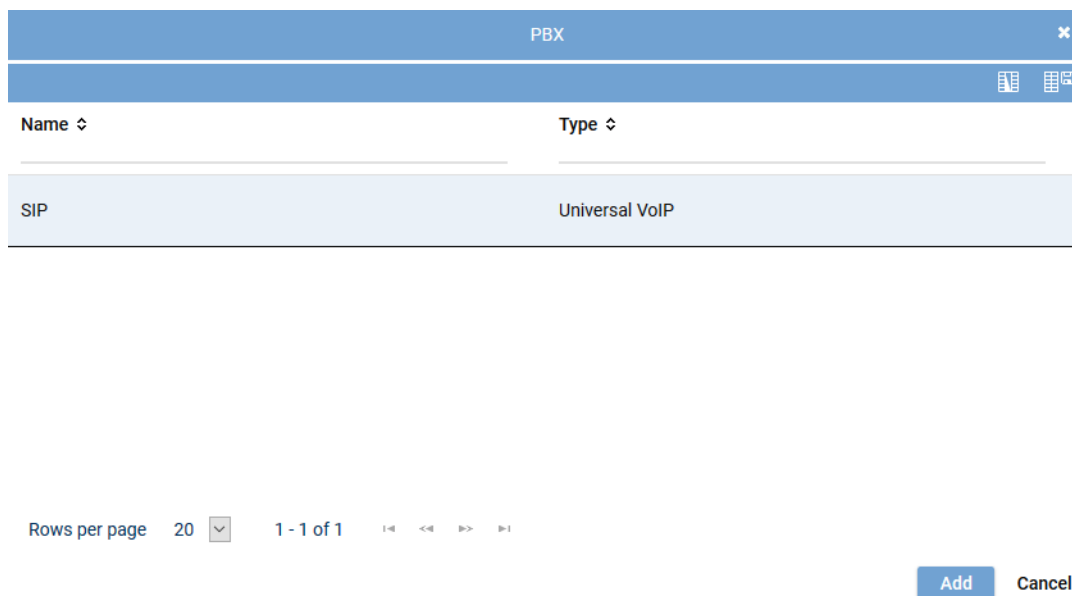
Fig. 191: Create integration type

- 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. 34: 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

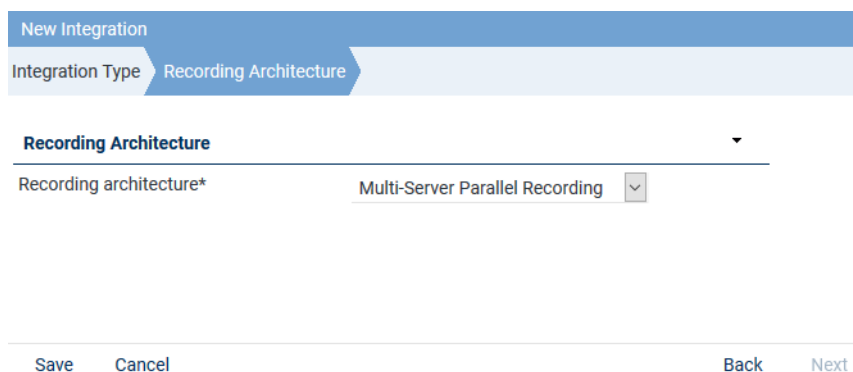
Add Cancel

Fig. 192: Select PBX

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

Assign recording architecture for Multi-Server Parallel Recording

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Parallel Recording

Save Cancel Back Next

Fig. 193: Assign recording architecture - Multi-Server Parallel

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




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

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



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see Duplicates in parallel recording architectures.

Configuration steps

1. To complete the configuration of the integration, click on the icon  in front of the name of the new integration.

⇒ The following configuration steps appear:







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

Fig. 194: Configuration steps of the integration

Configure recording architecture

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

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

Step: Configure Recording Architecture ✖

Details *


Recording architecture* Multi-Server Parallel Recording ▼

Save Cancel

Fig. 195: 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

- 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*
Transport protocol	UDP		
Port SIP signaling*	5060		
Activate SIP authentication	<input checked="" type="checkbox"/>		
User name for the SIP registration	123456		
Password for the SIP registration		
Activate SMS recording	<input type="checkbox"/>		

Save
Cancel

Fig. 196: Configuration step - Global recording settings

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

Parameter	Value/Description
<i>Transport protocol</i>	Select the deployed transport protocol for the SIP signaling between recording server and PBX from the drop-down list. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling on which the recording server waits for the signaling. Default value is 5060.
<i>Activate SIP authentication</i>	Activate this option if you would like to use SIP Digest Authentication.
<i>User name for the SIP registration</i>	Enter the user name for the SIP registration, e. g. 123456.
<i>Password for the SIP registration</i>	Enter the password if an authentication for SIP registration is supposed to be used.
<i>Activate SMS recording</i>	This functionality is not supported in this recording solution.

Tab. 35: Global recording settings



To make the registration on the SIP registrar or on the PBX work, SIP authentication as well as the PBX connection have to be activated.

The corresponding parameters have to be assigned to the correct values. In addition, the extensions of the recording server which are supposed to be registered must be configured.

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

Tab Device Groups

In parallel recording, you can configure connections to different PBXs.

- Select the tab Device Group 1 to configure the connection to PBX 1.

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. 197: 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. 198: 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.

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*.

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

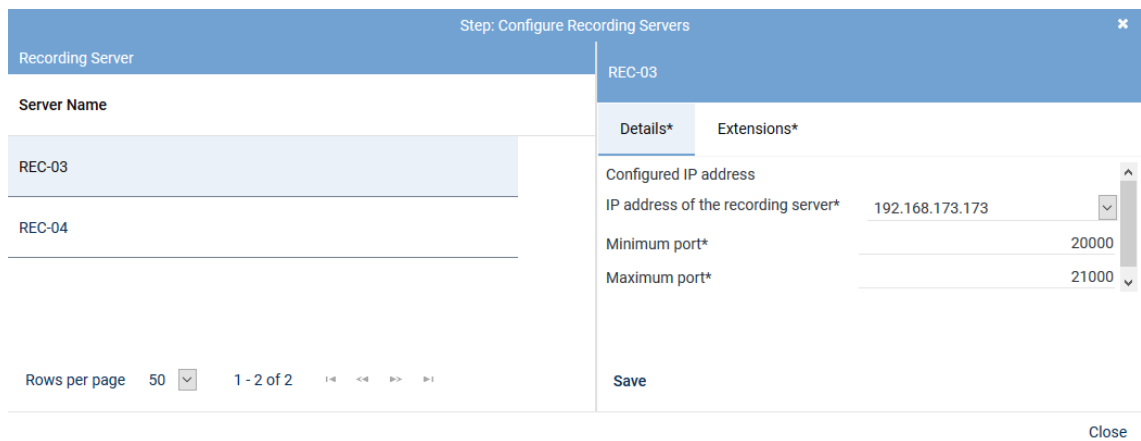


Fig. 199: Configuration step - Configure recording servers

- 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. 36: Configure recording servers



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



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

Configure add-on



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



Add-ons are not supported in this recording solution.


Configure miscellaneous settings





Configuring these settings is not required for this recording solution. Even without this configuration step, the integration has been configured comprehensively and can be activated.

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. 200: 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. 201: 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. 202: Deactivate integration

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

7.1.3

Duplicates in parallel recording architectures



In parallel recording architectures with synchronized recording control, no duplicates are created that could be deleted. Both recordings are merged in one package and thus cannot be deleted separately. Please note that as a result more storage capacity must be available for recording.

In parallel recording without synchronization, redundant recording data is created in the system. To avoid that identical conversations contained in the database are displayed twice in the replay applications (e. g. *POWERplay Web*), you can delete duplicates so that only one of the identical conversations remains.

Conversations are considered identical if they have the following characteristics:

- Identical start and end times

You can define a difference for start and end times so that conversations are still considered as duplicates despite of a certain difference, see [chapter "Configure duplicate detection", p. 171](#).

The start and end times of complete conversations as well as of individual recordings belonging to a conversation are checked.

- Identical conversation participants
- Identical additional data

Duplicate detection is configured in the Integrations module. There, you can select for each integration separately, when conversations are supposed to be considered as identical. Upon selecting an architecture based on parallel recording for an integration, the tab *Parallel Recording* becomes active where you can adjust the required settings, see [chapter "Configure duplicate detection"](#), p. 171.

The shorter one of the two identical recordings is deleted. To calculate the recording duration, the sum of all recording durations of all sections of a conversation are taken into account. The additional data as well as the audio data of the duplicate are deleted. On which of the two recording servers the duplicate is deleted depends on where the shorter conversation of the two has been saved. If the recording duration is identical, the recording which has been checked last is considered the duplicate.

Duplicate detection is carried out for all new recordings as soon as it has been activated but not retroactively. I. e. recordings which had already been saved when duplicate detection was activated are not checked.



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.

7.1.3.1 Configure duplicate detection

In the Integrations module, you can select for each integration separately when 2 conversations are supposed to be considered as duplicates. Upon selecting an architecture based on parallel recording for an integration, the tab *Parallel Recording* becomes active where you can adjust 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. In the detail view, select the tab *Parallel Recording* 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. 203: Tab Parallel Recording (integration)

Delete duplicates...	<p>When activating this option, you can define by means of the displayed criteria when two recordings are supposed to be considered as duplicates.</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>
The start times differ in a maximum of	<p>Select the maximum difference for the start time. The start times of complete conversations as well as of individual recordings belonging to a conversation are checked.</p> <p>Example: <i>1.000 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 the two conversations do not differ for more than 1.000 milliseconds, then the conversations are considered as possible duplicates with regard to their start time.</p>
The end times differ in a maximum of	<p>Select the maximum difference for the end time. The end times of complete conversations as well as of individual recording sections of a conversation are checked.</p> <p>Example: <i>1.000 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 the two conversations do not differ for more than 1.000 milliseconds, then the conversations are considered as possible duplicates with regard to their end time.</p>

<i>Time after which conversations are to be checked at the earliest</i>	<p>Select the time period which is supposed to pass before a recording is supposed to be checked for duplicates.</p> <p>Example: <i>3 minutes</i></p> <p>If a conversation ended at 2:20 pm, i. e. the recording has been saved at 2:20 pm, then the recording is not checked for duplicates before 2:23 pm.</p>
<i>Interval in which the check is to take place</i>	<p>Select the interval in which the duplicate detection job is supposed to be carried out.</p> <p>Example: <i>2 minutes</i></p> <p>The job for duplicate detection starts again every 2 minutes to search for new recordings and possible duplicates and to delete duplicates.</p>
List <i>Additional data</i>	<p>Add all additional data which is supposed to be considered as criteria. When searching for duplicates, only those recordings containing an additional data type from the list are considered. If an additional data type is empty in both conversations, this is considered as identical and one conversation is deleted.</p> <p> = Add additional data to the list</p> <p> = Remove additional data from the list</p>

- To save the settings, click on the button **Save**.
- ⇒ Upon activating the option *Delete duplicates...*, the recordings are checked for duplicates and detected duplicates are deleted.

7.1.3.2 Additional data

7.1.3.2.1 Map additional data

In addition to the start and end times, you can use further additional data for duplicate detection.

- In the list *Additional Data*, click on the icon  (*Add*) to configure further additional data.


Additional Data 	
ID ↕	Displayed Name ↕

Fig. 204: Map additional data

- Select the required additional data from the list which are to serve to detect possible duplicates.
To select several entries or to revoke a selection, click on the respective line while holding the [Ctrl] key down.

Additional Data			
Displayed Name ↕	Available ↕	Editable ↕	External Recording Control
CallManager_SwitchCallId	✓	✓	✓
MLC Line	✓	✓	✓

Rows per page 20 1 - 20 of 21

Add Cancel

Fig. 205: Add additional data


NOTICE! The list only displays additional data which has been configured previously in the Additional Data module.



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*.

7.1.3.2.2 Add additional data assignment

- Select the tab *Parallel Recording*.
- Select the additional date that you would like to remove from the list *Additional Data*.
- Click on the icon  (*Delete*).

Additional Data	
ID ↕	Displayed Name
customCP01	CallManager_SwitchCallId

Fig. 206: Add additional data assignment

7.1.3.3 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.

7.1.4 Configure Recording Content Validation

Recording Content Validation is an easy and quick possibility to check the functionality of the recording system whenever required. The information is displayed in the Notifications module. Reports can be used to visualize the results.

Preconditions for validation:

- *The license Recording Content Validation must have been installed.*
- *Emotion detection must have been activated in the Servers module.*
- *The server for emotion detection must have been selected.*

Configuration in the Servers module

1. Go to the *Servers module*.
2. In the main view, select the server that you would like to configure.
3. Select the tab *Usage*.
4. Open the group field *Audio Analysis*.

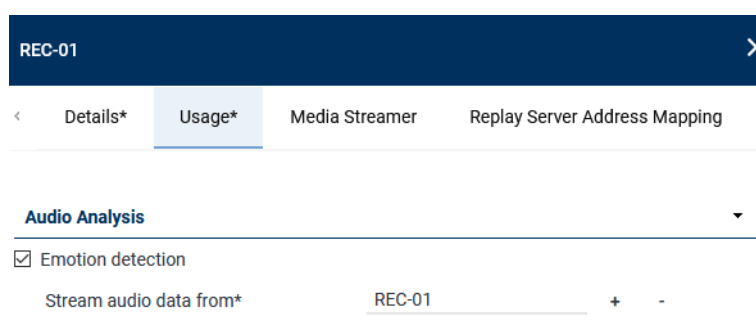


Fig. 207: Servers module - Activate emotion detection

5. Activate the function *Emotion detection*.
6. By clicking on the icon **+**, select the server that emotion detection runs on.
 - ⇒ This server will then appear in the list in the Integrations module in the tab *Recording Content Validation* to configure silence detection.

Configuration in the Integrations module

1. In the main view, select the integration for which you would like to check the validity of recording.
2. Select the tab *Recording Content Validation*.

The following criteria are available to check the correct functionality of the recording system and the validity of recording content:

- *Packet loss detection*
- *Silence detection*

×

< Details*
Recording Content Validation
>

Activate packet loss detection ☒

Activate decryption error detection ☐

☒ Activate silence detection

Minimum duration* ms

Threshold value* dB

Silence percentage* %

Weighting*

Emotion detection*

Save

Reset

Fig. 208: Create integration - tab Recording Content Validation

Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost. NOTICE! Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	NOTICE! This check is not required in this recording solution.
Activate silence detection	<input checked="" type="checkbox"/> Activate the check box to check whether the recording contain sections of silence and under which conditions sections are recognized as silence. NOTICE! A high percentage of silence sections can indicate a technical problem such as a connection interruption.
<i>Minimum duration</i>	Enter the minimum duration of silence after which a notification is supposed to be issued. Default value is 30000 ms (30 seconds).
<i>Threshold value</i>	Enter a threshold value of the audio level in dB under which the section is supposed to be considered a silence section. Default value is -60 dB.
<i>Silence percentage</i>	Enter the percentage of silence in a recording which is supposed to trigger a notification. Default value is 90 %.
<i>Weighting</i>	Enter the extent to which the audio curve (samples) is supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 1-10000 can be recommended.
<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.

3. Select the respective server from the list of available servers.

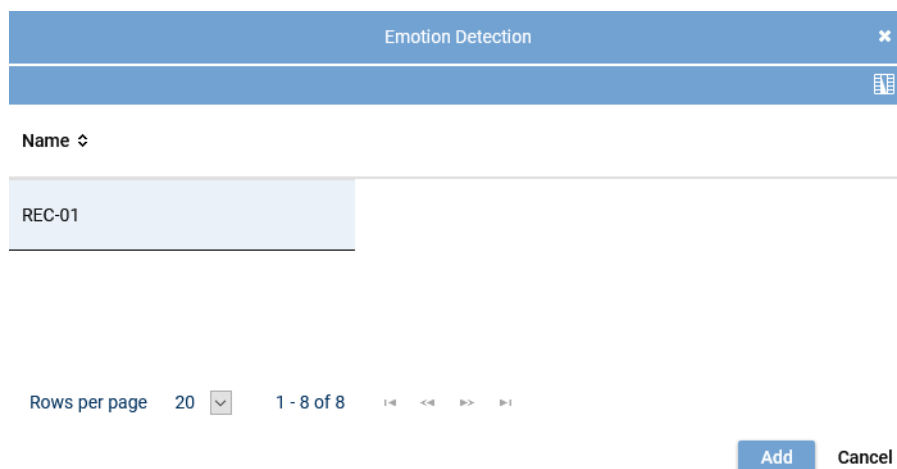


Fig. 209: Select server for emotion detection

4. Click on the button *Add* to apply the selected server.
5. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

Configuration in the Notifications module

To issue notifications in case of an error, the corresponding notifications must be configured in the Notifications module.



For basic information about the Notifications module refer to the administration manual for tenants *Notifications module*.

Configuration in the application INSIGHT_{neo}

To issue a report visualizing the errors occurred, a report must be created in the application INSIGHT_{neo}.



For information about using the Report Templates module and the Report Instances module refer to the respective INSIGHT_{neo} user manuals.

7.1.5 Adjust neo configuration file

Some parameters cannot be configured via the graphic interface but have to be adjusted in the configuration files.

7.1.5.1 Adjust Recording module

The configuration files for the recording module can be found in the following directory:
C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingModule

A separate configuration file is created for each configured integration. Customer-specific adjustments of the parameters have to be carried out in the respective integration configuration file. Upon starting, the basic file *basic.recorder.properties* is read out. After that, the integration configuration file is read out. The values in the integration configuration file have a higher priority and will be the ones being used in the end.

If you have configured several integrations of the same integration type, you have to make the adjustments for each integration separately. To determine which file belongs to which integration, you can open the configuration file and for instance compare the area of assigned extensions. Under no circumstances change the original name of the file since you will not be able to start the integration again.

Configured integrations which have not been activated have the addition *inactive* in front of the file name. The file is not deleted even if the integration in the application System Configuration is deleted. If a deactivated integration is activated again, the addition *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`.

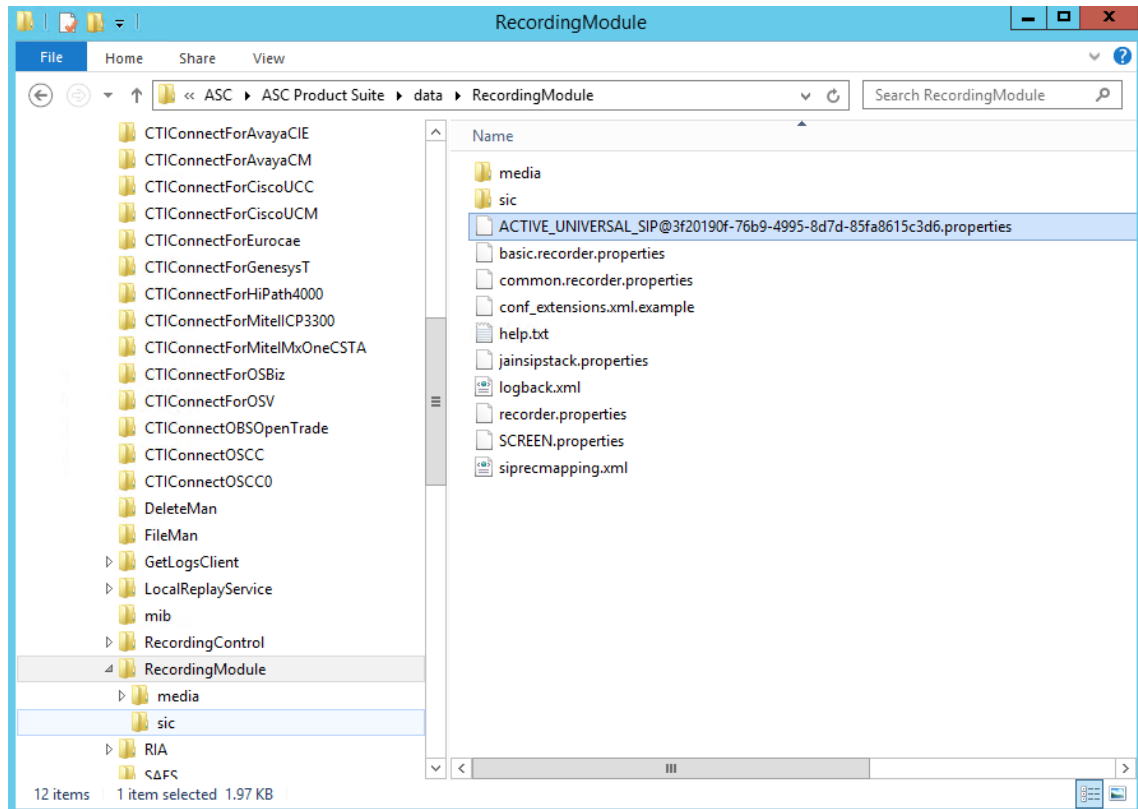


Fig. 210: Path to the configuration file

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`

Tagging for parallel recording

For parallel recording, you can configure a tagging to be able to see which server is recording. You can use the additional data field **customCP30** for this purpose.

1. Search for the entry `simStaticTagging=`.
2. On the **first** recording server, enter **Core A** for the tagging of the additional data field **customCP30**.
 - `simStaticTagging="customCP30=Core A"`
3. Change to the other recording servers.
4. Open the files `ACTIVE_UNIVERSAL_SIP@<UUID>.properties` in the Editor there, too.

5. Search for the entry `simStaticTagging=`.
6. For the tagging of the additional data field **customCP30** enter the corresponding value **Core xy** for each recording server.
7. Save the changes in the configuration files.
8. Restart the service *ASC RecordingModule* on every recording server to apply the changes.

7.1.5.2 Copy ASC.ScenarioConfig.Noetica.xml

ASC delivers customized templates for the configuration files of the Recording Control module.

1. Change to the path
C:\Program Files (x86)\ASC\ASC Product Suite\data\RecordingControl
2. Copy the file called **ASC.ScenarioConfig.Noetica.xml** and rename it to **ASC.Scenario-Config.xml**.



```

1 <ScenarioConfig>
2 <!--
3   Noetica
4 -->
5 <GeneralSettings
6   automaticMonitoringType="true"
7 />
8 <Scenario
9   type="PBX_UNIVERSAL_VOIP"
10  subtype="IP_UNIVERSAL_PORT_BASED"
11  tag="CUSTOMERPBX"
12  recordingOnlyConnect="false"
13  staticConfigNeeded="false"
14  staticConfigTXOnly="true"
15  recordingDeviceMode="PBXPHONEID"
16  detectConferenceOnHoldEnd="false"
17  ignoreTransferID="false"
18  allowsRIAParticipantMerging="false"
19  allowsRMParticipantMerging="false"
20  streamRequestType="RTP"
21  streamRequestCount="-1"
22  streamHolderType="RTP_ACTIVE"
23  streamHolderMode="KEEPER"
24 />
25 </ScenarioConfig>
26

```

3. Restart the *Recording Control Service*.

The behavior of the integration is controlled by the parameters in this file. As soon as this file has been saved in the indicated directory upon starting, the integration will use this configuration.

Mixed operation with other port-based recordings is not possible. Recording does not start unless the **API** transmits the command to start a recording. Even if **RTP** data can be found at one of the configured ports, it will not be recorded. Recording cannot be started with other ASC clients either.

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.

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.....	5
Fig. 2	System Configuration - web interface	11
Fig. 3	System Configuration - main view:.....	12
Fig. 4	Recording architectures - main view	13
Fig. 5	Toolbar Recording Architectures module.....	13
Fig. 6	Create recording architecture - All-in-one Basic Recording	14
Fig. 7	Recording architecture - tab Details.....	15
Fig. 8	Select integration type.....	16
Fig. 9	Recording architecture - tab Server Assignment	16
Fig. 10	Recording architecture - assign server	17
Fig. 11	Recording architecture - activate recording variant.....	17
Fig. 12	Recording architecture - activate recording architecture.....	18
Fig. 13	Servers - main view.....	18
Fig. 14	Toolbar Servers module.....	19
Fig. 15	Add server locations.....	20
Fig. 16	Delete server location	21
Fig. 17	Servers - tab Details.....	21
Fig. 18	Servers - tab usage	22
Fig. 19	Group field API Server	22
Fig. 20	Select storage expansion	24
Fig. 21	Group field Audio Analysis	24
Fig. 22	Select server for emotion detection.....	25
Fig. 23	Group field Recording Control/Key Management	25
Fig. 24	Group field Data Processing	26
Fig. 25	Select server	28
Fig. 26	Group field Replay	28
Fig. 27	Select server	30
Fig. 28	Group field Virtualization	30
Fig. 29	Servers module - tab Media Streamer	31
Fig. 30	Servers Module - tab Replay Server Address Mapping	33
Fig. 31	Servers module - tab Key Management.....	34
Fig. 32	Servers module - tab Keystore/Virtualization	36
Fig. 33	Create new PBX.....	37
Fig. 34	Toolbar PBX module	37
Fig. 35	Create new PBX - tab Details	38
Fig. 36	Tenants - main view - tab Extensions	40
Fig. 37	Assign extensions to tenants	40
Fig. 38	Remove extensions.....	42
Fig. 39	Select extensions	42
Fig. 40	Additional Data module main view	43
Fig. 41	Configure additional data	44

Fig. 42	Additional data - configure availability	44
Fig. 43	Integrations - main view	45
Fig. 44	Toolbar Integrations module	45
Fig. 45	Create integration type	46
Fig. 46	Select PBX	47
Fig. 47	Assign recording architecture - All-in-one Basic	47
Fig. 48	Configuration steps of the integration	48
Fig. 49	Configuration step - Configure Recording Architecture	48
Fig. 50	Configuration step - Global recording settings	49
Fig. 51	Configuration step - Configure recording servers	50
Fig. 52	Activate integration	51
Fig. 53	Activated integration	52
Fig. 54	Deactivate integration	52
Fig. 55	Recording architectures - main view	53
Fig. 56	Toolbar Recording Architectures module	53
Fig. 57	Create recording architecture - All-in-one Parallel Recording	54
Fig. 58	Recording architecture - tab Details - All-in-one Parallel Recording	55
Fig. 59	Select integration type	56
Fig. 60	Recording Architecture - tab Server Assignment	57
Fig. 61	Recording Architecture - assign server - example	57
Fig. 62	Recording Architecture - activate recording type	58
Fig. 63	Activate recording architecture	58
Fig. 64	Servers - main view	59
Fig. 65	Toolbar Servers module	59
Fig. 66	Add server locations	60
Fig. 67	Delete server location	61
Fig. 68	Servers - tab Details	62
Fig. 69	Servers - tab usage	62
Fig. 70	Group field API Server	63
Fig. 71	Select storage expansion	64
Fig. 72	Group field Audio Analysis	65
Fig. 73	Select server for emotion detection	65
Fig. 74	Group field Recording Control/Key Management	65
Fig. 75	Group field Data Processing	66
Fig. 76	Select server	68
Fig. 77	Group field Replay	69
Fig. 78	Select server	70
Fig. 79	Group field Virtualization	71
Fig. 80	Servers module - tab Media Streamer	72
Fig. 81	Servers Module - tab Replay Server Address Mapping	73
Fig. 82	Servers module - tab Key Management	74
Fig. 83	Servers module - tab Keystore/Virtualization	76

Fig. 84	Tenants - main view - tab Extensions	77
Fig. 85	Assign extensions to tenants	78
Fig. 86	Remove extensions.....	80
Fig. 87	Select extensions	80
Fig. 88	Additional Data module main view	81
Fig. 89	Configure additional data	82
Fig. 90	Additional data - configure availability	82
Fig. 91	Integrations - main view	83
Fig. 92	Toolbar Integrations module	83
Fig. 93	Create integration type	84
Fig. 94	Select PBX	85
Fig. 95	Assign recording architecture - All-in-one Parallel	85
Fig. 96	Configuration steps of the integration	86
Fig. 97	Configuration step - Configure Recording Architecture.....	86
Fig. 98	Configuration step - Global recording settings	87
Fig. 99	Configure device group 1	88
Fig. 100	Configure device group 2	88
Fig. 101	Configuration step - Configure recording servers	89
Fig. 102	Activate integration.....	90
Fig. 103	Activated integration.....	91
Fig. 104	Deactivate integration	91
Fig. 105	Recording architectures - main view	92
Fig. 106	Toolbar Recording Architectures module.....	92
Fig. 107	Create recording architecture - Multi-Server Recording.....	93
Fig. 108	Recording architecture - tab Details - Multi-Server Recording	94
Fig. 109	Select integration type.....	95
Fig. 110	Recording architecture - tab Server Assignment	96
Fig. 111	Recording architecture - assign server - example.....	96
Fig. 112	Add recording server	97
Fig. 113	Recording architecture - activate recording architecture.....	98
Fig. 114	Servers - main view.....	99
Fig. 115	Toolbar Servers module.....	99
Fig. 116	Add server locations.....	100
Fig. 117	Delete server location	101
Fig. 118	Servers - tab Details.....	102
Fig. 119	Servers - tab usage	102
Fig. 120	Group field API Server	103
Fig. 121	Select storage expansion.....	104
Fig. 122	Group field Audio Analysis	105
Fig. 123	Select server for emotion detection.....	105
Fig. 124	Group field Recording Control/Key Management	105
Fig. 125	Group field Data Processing	106

Fig. 126	Select server	108
Fig. 127	Group field Replay	109
Fig. 128	Select server	110
Fig. 129	Group field Virtualization	111
Fig. 130	Servers module - tab Media Streamer	112
Fig. 131	Servers Module - tab Replay Server Address Mapping	113
Fig. 132	Servers module - tab Key Management.....	114
Fig. 133	Servers module - tab Keystore/Virtualization	116
Fig. 134	Tenants - main view - tab Extensions	117
Fig. 135	Assign extensions to tenants	118
Fig. 136	Remove extensions.....	120
Fig. 137	Select extensions	120
Fig. 138	Additional Data module main view	121
Fig. 139	Configure additional data	122
Fig. 140	Additional data - configure availability	122
Fig. 141	Integrations - main view	123
Fig. 142	Toolbar Integrations module	123
Fig. 143	Create integration type	124
Fig. 144	Select PBX	125
Fig. 145	Assign recording architecture - Multi-Server Recording.....	125
Fig. 146	Configuration steps of the integration	126
Fig. 147	Configuration step - Configure Recording Architecture.....	126
Fig. 148	Configuration step - Global recording settings	127
Fig. 149	Configuration step - Configure recording servers	128
Fig. 150	Activate integration.....	129
Fig. 151	Activated integration.....	130
Fig. 152	Deactivate integration	130
Fig. 153	Recording architectures - main view	131
Fig. 154	Toolbar Recording Architectures module.....	131
Fig. 155	Create recording architecture - Multi-Server Parallel Recording.....	132
Fig. 156	Recording architecture - tab Details - Multi-Server Parallel Recording	133
Fig. 157	Select integration type.....	134
Fig. 158	Recording architecture - server assignment device group 1	135
Fig. 159	Recording architecture - assign server - example.....	135
Fig. 160	Add recording server	136
Fig. 161	Recording architecture - activate recording architecture - example	137
Fig. 162	Servers - main view.....	138
Fig. 163	Toolbar Servers module.....	138
Fig. 164	Add server locations.....	139
Fig. 165	Delete server location	140
Fig. 166	Servers - tab Details.....	141
Fig. 167	Servers - tab usage	141

Fig. 168	Group field API Server	142
Fig. 169	Select storage expansion.....	143
Fig. 170	Group field Audio Analysis	144
Fig. 171	Select server for emotion detection.....	144
Fig. 172	Group field Recording Control/Key Management	144
Fig. 173	Group field Data Processing	145
Fig. 174	Select server	147
Fig. 175	Group field Replay	148
Fig. 176	Select server	149
Fig. 177	Group field Virtualization	150
Fig. 178	Servers module - tab Media Streamer	151
Fig. 179	Servers Module - tab Replay Server Address Mapping	152
Fig. 180	Servers module - tab Key Management.....	153
Fig. 181	Servers module - tab Keystore/Virtualization	155
Fig. 182	Tenants - main view - tab Extensions	156
Fig. 183	Assign extensions to tenants	157
Fig. 184	Remove extensions.....	159
Fig. 185	Select extensions	159
Fig. 186	Additional Data module main view	160
Fig. 187	Configure additional data	161
Fig. 188	Additional data - configure availability	161
Fig. 189	Integrations - main view	162
Fig. 190	Toolbar Integrations module	162
Fig. 191	Create integration type.....	163
Fig. 192	Select PBX.....	164
Fig. 193	Assign recording architecture - Multi-Server Parallel	164
Fig. 194	Configuration steps of the integration	165
Fig. 195	Configuration step - Configure Recording Architecture.....	165
Fig. 196	Configuration step - Global recording settings	166
Fig. 197	Configure device group 1	167
Fig. 198	Configure device group 2	167
Fig. 199	Configuration step - Configure recording servers	168
Fig. 200	Activate integration.....	169
Fig. 201	Activated integration.....	170
Fig. 202	Deactivate integration	170
Fig. 203	Tab Parallel Recording (integration)	172
Fig. 204	Map additional data	173
Fig. 205	Add additional data	174
Fig. 206	Add additional data assignment	174
Fig. 207	Servers module - Activate emotion detection.....	175
Fig. 208	Create integration - tab Recording Content Validation.....	176
Fig. 209	Select server for emotion detection.....	177

Fig. 210 Path to the configuration file.....	178
--	-----

List of tables

Tab. 1	Licenses of ASC.....	8
Tab. 2	Login data - system provider.....	11
Tab. 3	Configure audio analysis.....	24
Tab. 4	Configure recording control/key management	25
Tab. 5	Configure data storage.....	26
Tab. 6	Configure replay.....	28
Tab. 7	Configure virtualization.....	30
Tab. 8	Create PBX	38
Tab. 9	PBX parameters with complete phone number.....	39
Tab. 10	Create integration type.....	46
Tab. 11	Global recording settings	49
Tab. 12	Configure recording servers.....	50
Tab. 13	Configure audio analysis.....	65
Tab. 14	Configure recording control/key management	66
Tab. 15	Configure data storage.....	67
Tab. 16	Configure replay.....	69
Tab. 17	Configure virtualization.....	71
Tab. 18	Create integration type.....	84
Tab. 19	Global recording settings	87
Tab. 20	Configure recording servers.....	89
Tab. 21	Configure audio analysis.....	105
Tab. 22	Configure recording control/key management	106
Tab. 23	Configure data storage.....	107
Tab. 24	Configure replay.....	109
Tab. 25	Configure virtualization.....	111
Tab. 26	Create integration type.....	124
Tab. 27	Global recording settings	127
Tab. 28	Configure recording servers.....	128
Tab. 29	Configure audio analysis.....	144
Tab. 30	Configure recording control/key management	145
Tab. 31	Configure data storage.....	146
Tab. 32	Configure replay.....	148
Tab. 33	Configure virtualization.....	150
Tab. 34	Create integration type.....	163
Tab. 35	Global recording settings	166
Tab. 36	Configure recording servers.....	168

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)

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

NVP

Noetica Voice platform is a platform for communication via VoIP.

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

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

SRTP

Secure real-time protocol

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
