

# EVOIPneo passive for Mitel MiVoice Connect



## Administration manual for system providers

10/21/2021

### Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (country-specific)

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

Copyright © 2021 ASC Technologies AG. All rights reserved.

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



## Contents

<b>1</b>	<b>General information .....</b>	<b>4</b>
<b>2</b>	<b>Introduction .....</b>	<b>5</b>
<b>3</b>	<b>System requirements.....</b>	<b>7</b>
3.1	Hardware components .....	7
3.1.1	Recorder .....	7
3.1.2	Additional requirements .....	7
3.2	Software components .....	7
3.3	Supported end devices .....	7
<b>4</b>	<b>Installation requirements .....</b>	<b>9</b>
4.1	Licenses .....	9
4.2	Information .....	9
<b>5</b>	<b>Overview of how to install and configure the product .....</b>	<b>10</b>
<b>6</b>	<b>Installation .....</b>	<b>11</b>
<b>7</b>	<b>Configuration.....</b>	<b>12</b>
7.1	System Configuration.....	12
7.1.1	Start application .....	12
7.1.2	Configure recording solution .....	13
7.1.2.1	Configure recording solution All-in-one Basic .....	13
7.1.3	Configure Recording Content Validation.....	55
7.1.4	Configure Recording Planner for DTMF control.....	57
7.1.4.1	Configure profile.....	58
7.1.4.2	Define DTMF sequences .....	59
<b>8</b>	<b>Troubleshooting.....</b>	<b>61</b>
	<b>List of figures .....</b>	<b>62</b>
	<b>List of tables .....</b>	<b>64</b>
	<b>Glossary.....</b>	<b>65</b>

## 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<sup>neo</sup> passive for Mitel MiVoice Connect provides the functionality which is necessary for the recording of unencrypted conversations in a SIP environment with a Mitel PBX.



This recording solutions allows recording data streams in stereo.

In stereo recording, the conversation directions are saved in separate files which can then be replayed separately. Stereo recording requires approximately twice as much storage capacity.

In this passive recording solution, the recording server is no active communication participant. The data packages are duplicated at the network switch and sent to a dedicated separate network card of the recording device via the monitor/mirror/[SPAN](#) port.

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



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

The following additional data is available:

- *Date and time*
- *Call duration*
- *Phone numbers*
- *Call direction*

Internal calls are not recorded.

The following options are available for recording control:

- [DTMF](#)
- [CLIENT<sup>command</sup>](#)  
Only if the internal phone number is called via the trunk (no collective phone numbers) and if the internal number is signaled on the trunk for outgoing calls, too, mapping of the agents and control by means of [CLIENT<sup>command</sup>](#) is possible.

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

## EVOIP<sub>neo</sub> passive for Mitel MiVoice Connect trunk/gateway side VoIP Recording

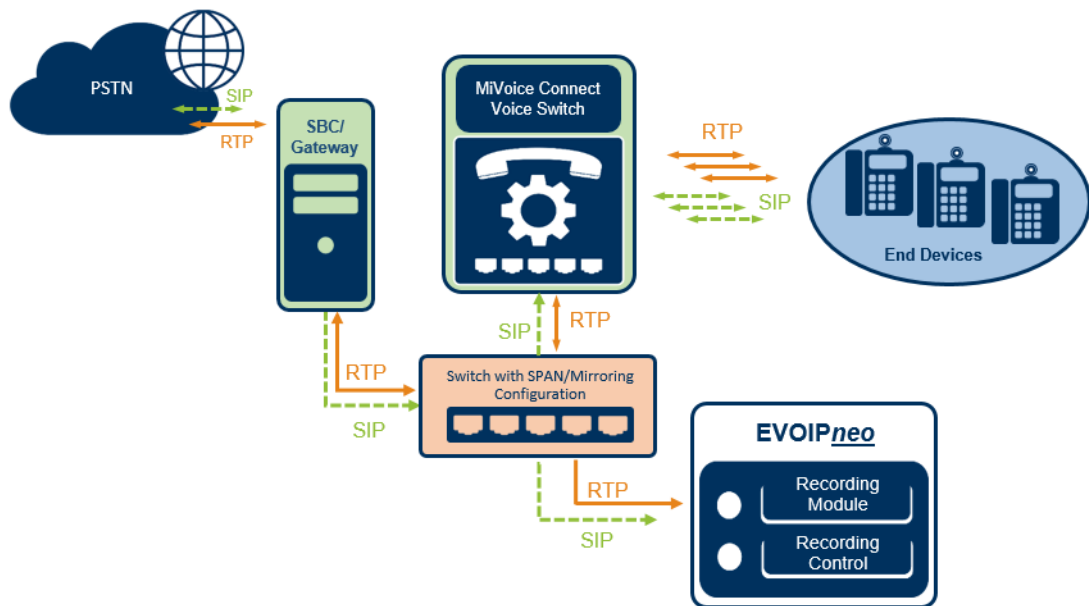


Fig. 1: Overview of the recording solution

### 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<sub>neo</sub> 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<sub>neo</sub> eco
- EVOLUTION<sub>neo</sub>
- EVOLUTION<sub>neo</sub> XXL



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

##### 3.1.2 Additional requirements

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



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

#### 3.2 Software components

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

#### 3.3 Supported end devices

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

The following RFC standards are supported:

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

- RFC 6068 (DTMF via SIP INFO) optional

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 <sup>neo</sup> Base license - passive	1 license per recording server
EVOIP <sup>neo</sup> passive for SIP	1 license per concurrent recording

Tab. 1: Licenses of ASC



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

#### 4.2 Information

Before starting the installation make sure that the following information is available:

- Name of the network interface in Windows which is supposed to be used for recording. The name is selected from a drop-down list during configuration.
- IP address of the recording server
- IP addresses of the Mitel MiVoice Connect Voice Switch

## 5

**Overview of how to install and configure the product**

The following steps have to be taken:

1. Install neo software
2. Configure PBX
  - 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 integration
    - Configure recording architecture  
Link the integration to the previously created recording architecture.
    - Configure recording servers  
Configuration of the parameters of the recording server, e. g. sniffer card

### 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.*

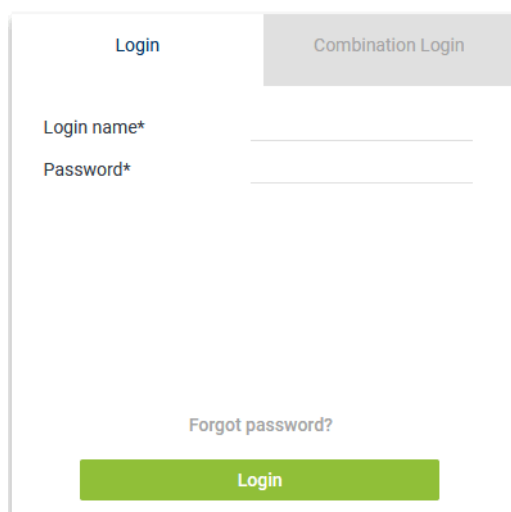


Fig. 2: System Configuration - web interface

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 $\geq 6.3$ , 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 $\geq 6.3$ , the changed password remains.
<i>neo</i> version $\geq 6.3$	
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.

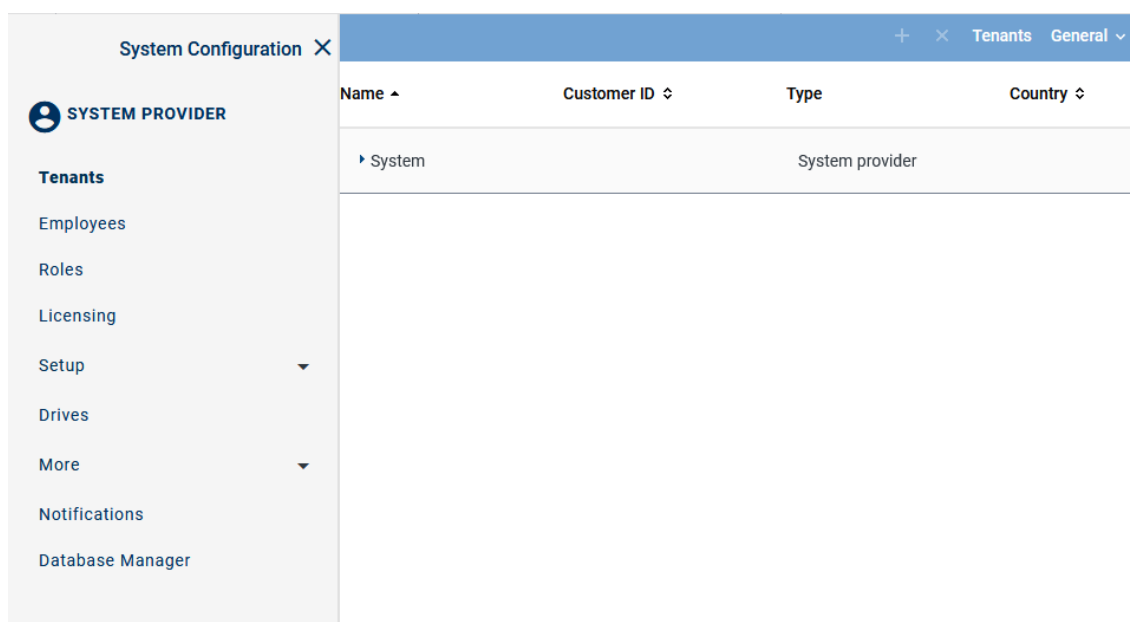


Fig. 3: System Configuration - main view:

## 7.1.2 Configure recording solution

### 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:

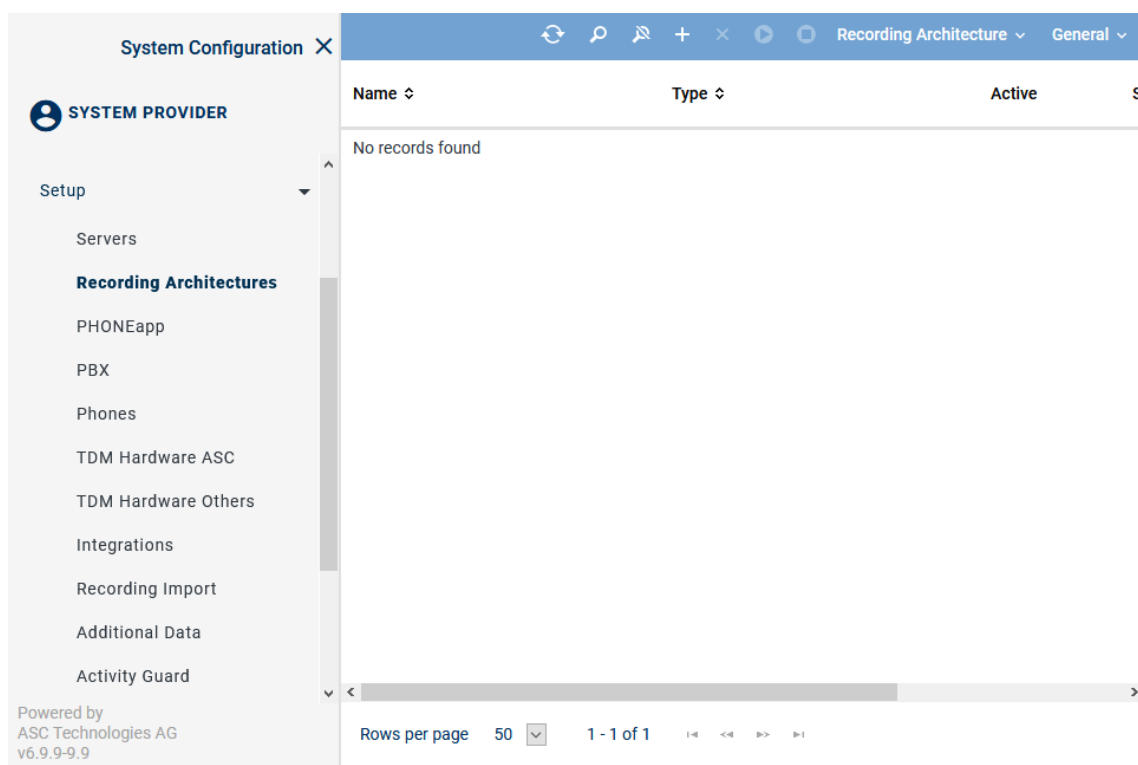




Fig. 4: Recording architectures - main view

<b>Name</b>	Name of the recording architecture
<b>Type</b>	Type of the recording architecture
<b>Active</b>	Shows whether the recording architecture has been activated and is ready to be used for the recording. <div> <span>✓</span> = 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.  <span>✗</span> = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div>
<b>Standby Active</b>	Shows whether the standby server is active for one or several recording components in the recording architecture. <div> <span>✓</span> = At least 1 standby server is active.  <span>✗</span> = No standby server is active or no standby server has been defined. </div>
<b>Creation Date</b>	Date on which the recording architecture was installed.
<b>Updated</b>	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

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

		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. <b>NOTICE!</b> 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. <b>NOTICE!</b> 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"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.




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

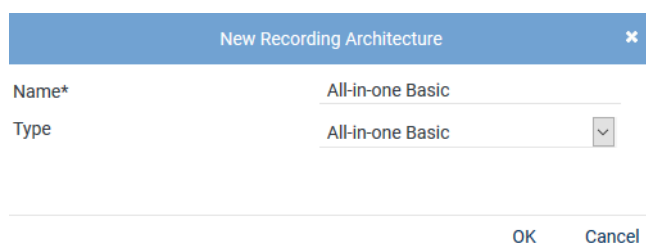
### Create recording architecture All-in-one Basic

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



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

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



New Recording Architecture

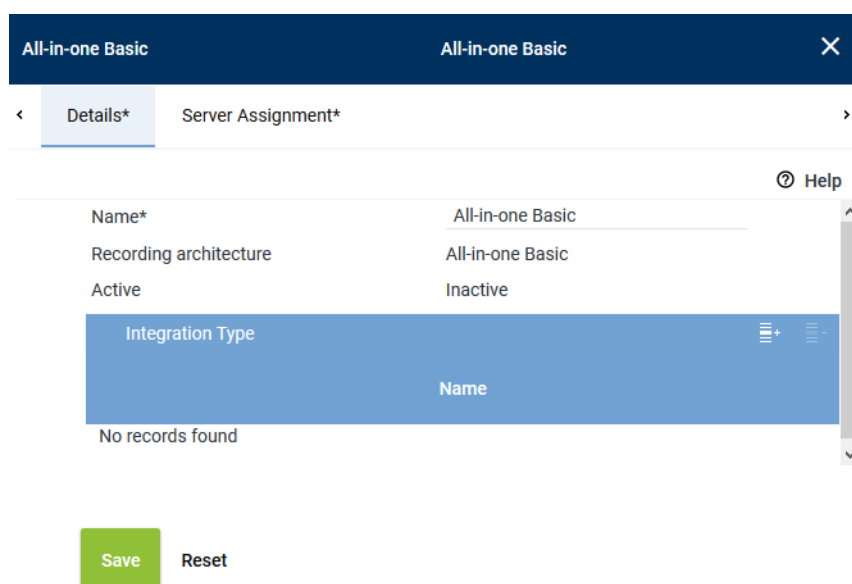
Name\* All-in-one Basic

Type All-in-one Basic

OK Cancel

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

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



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

< Details\* Server Assignment\* >

Help

Name\* All-in-one Basic

Recording architecture All-in-one Basic

Active Inactive


Integration Type

No records found

Save Reset

Fig. 7: Recording architecture - tab Details

### Add integration type

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



Integration Type

×

Name

SIP passive

Add

Cancel

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.



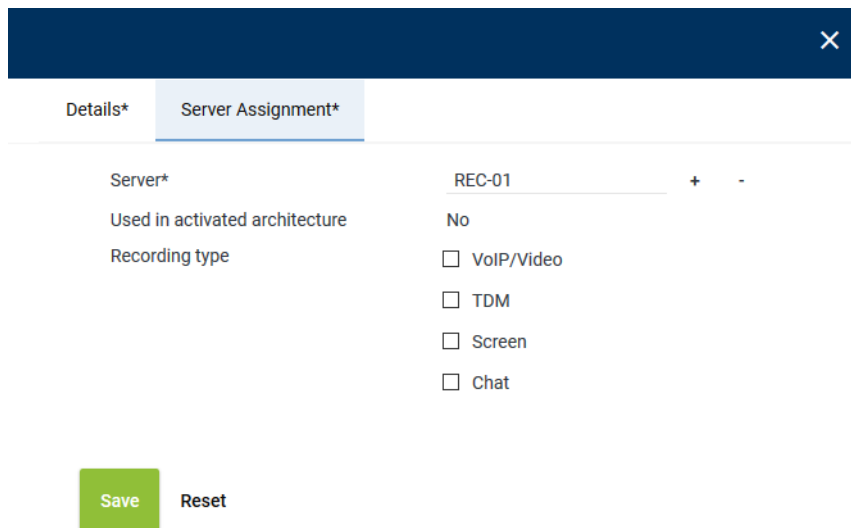
Any number of integration types can be assigned to a recording architecture.

2. Select *SIP passive* from the list of the available integration types and click on the button *Add*.

⇒ The name of the integration type now appears in the list in the detail view.

### **Assign server for All-in-one Basic**

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



Details\* Server Assignment\*

Server\* REC-01 + -

Used in activated architecture No

Recording type

☐ VoIP/Video

☐ TDM

☐ Screen

☐ Chat

Save Reset

Fig. 9: Recording architecture - tab Server Assignment

- 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

- 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.

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

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen




☐ Chat

Fig. 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.
3. To activate the recording architecture, click on the icon  (*Activate*).
  - ⇒ In the column *Active*, the icon  (*Active*) appears.





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

Fig. 12: Recording architecture - activate recording architecture

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



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



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

#### 7.1.2.1.2 Configure server

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

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

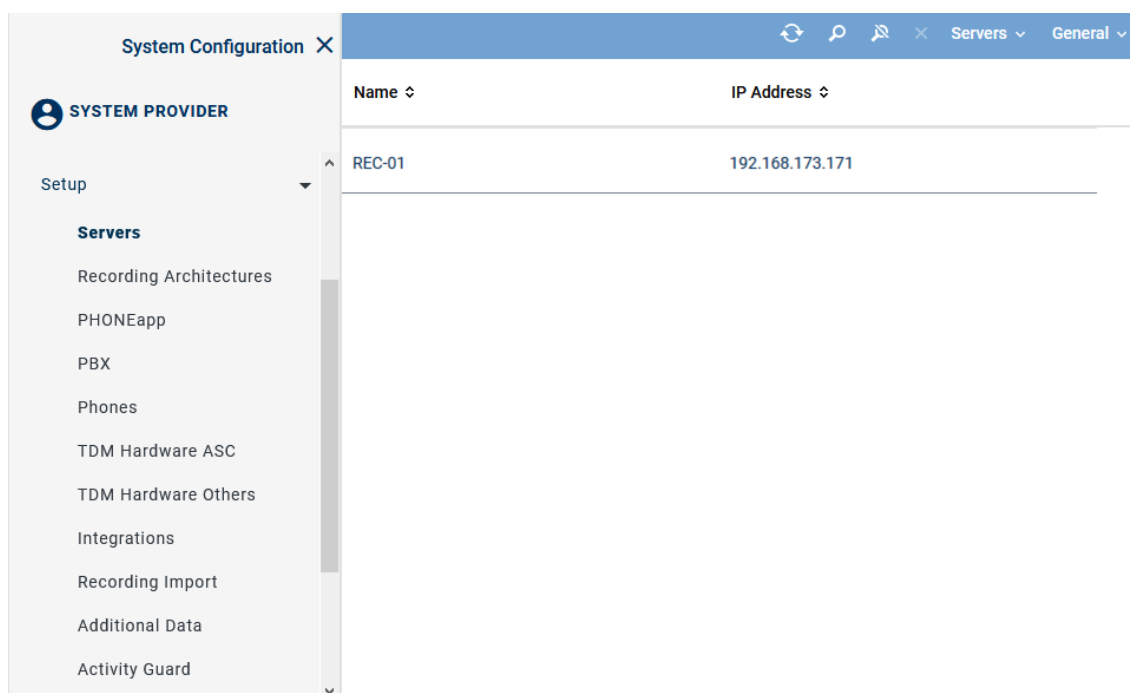


Fig. 13: Servers - main view

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 <a href="#">IP</a> 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.

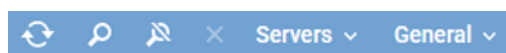







Fig. 14: Toolbar Servers module

	<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 <u>neo</u> system.

<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 21.</a>
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <a href="#">chapter "Administrate NTP server", p. 39.</a>
	<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"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Administrate server locations

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

#### Add server locations

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

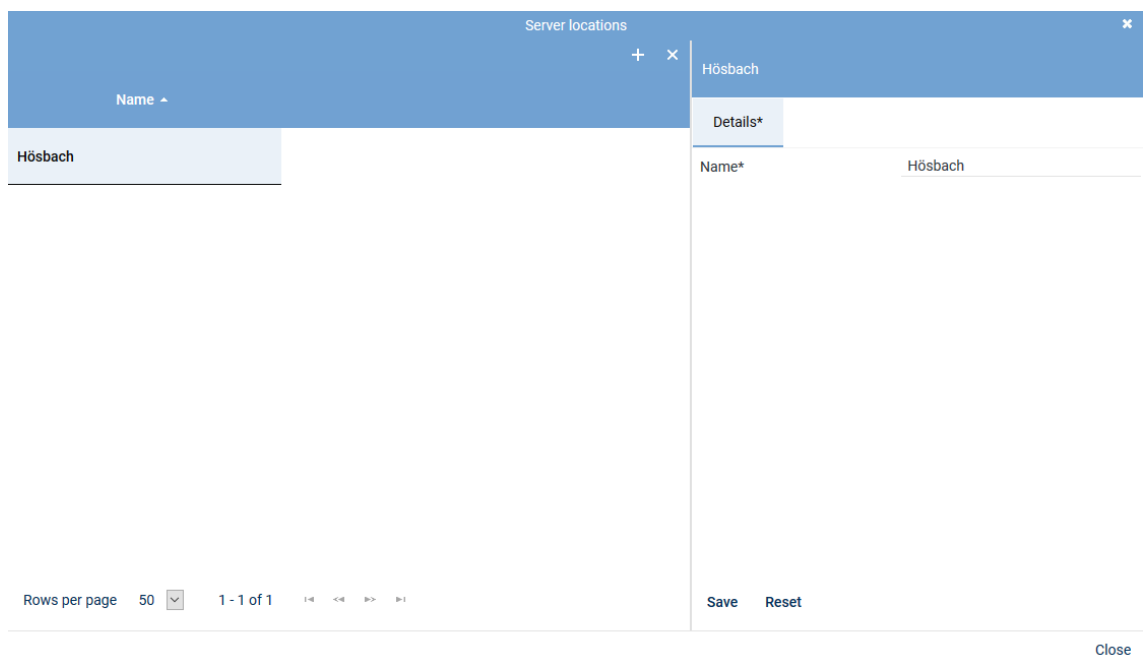



Fig. 15: Add server locations

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

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

### Delete server location



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

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

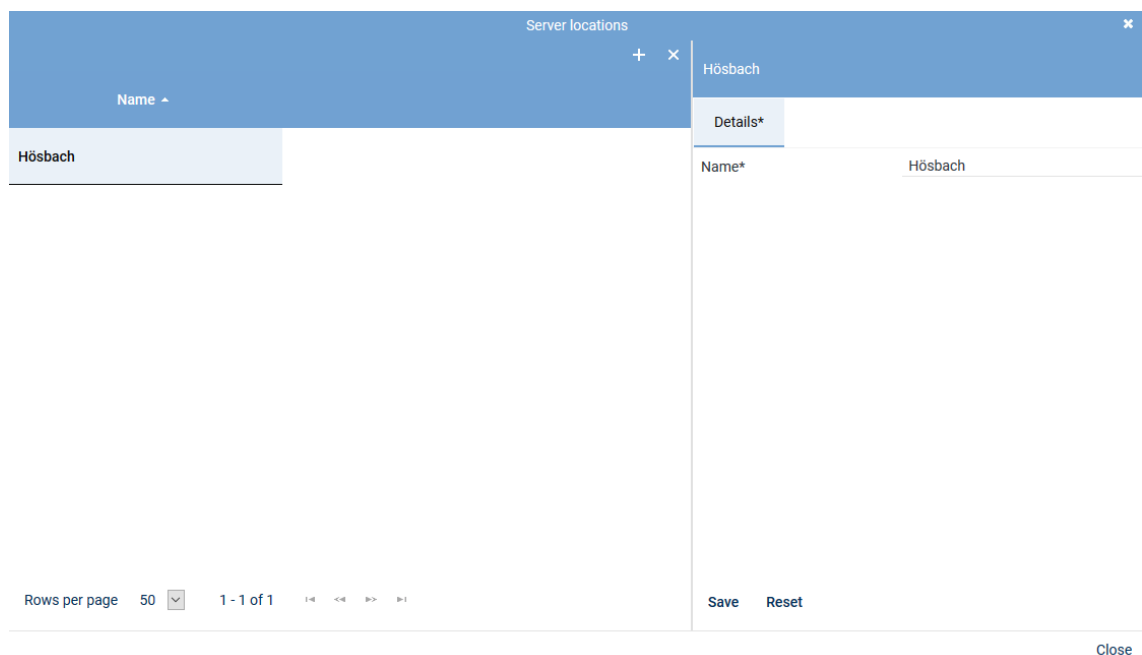



Fig. 16: Delete server location

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.

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

? Help

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

Save
Reset

Fig. 17: Servers - tab Details

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

### Tab Usage

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



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

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

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

Save
Reset

Fig. 18: Servers - tab usage

### Group field API Server

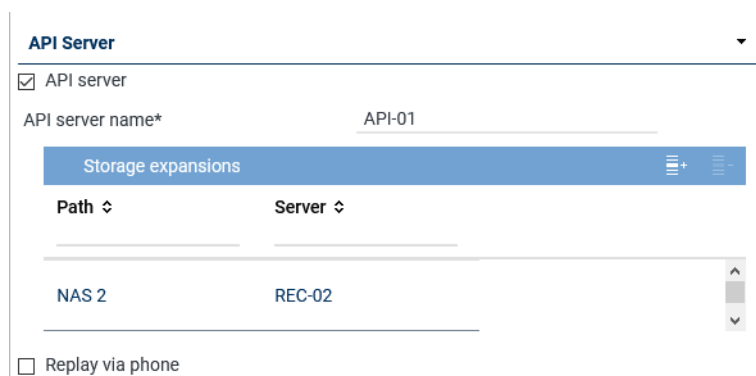




Fig. 19: Group field API Server

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

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


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

Parameter	Value/Description
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping", p. 34</a>.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List</i> <i>Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay", p. 25</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul>



Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.  <input type="checkbox"/> = Function has not been activated.</p> <p><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWERplay Pro</li> <li>• Application POWERplay Instant</li> <li>• Replay module</li> </ul> <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><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see <a href="#">chapter "Tab Media Streamer", p. 32</a>. 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

- 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>	<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"> <li>Click on the button <span>+</span> to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 3: Configure audio analysis

**Emotion Detection** ✕

📋

Name ↕

REC-01

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

Add Cancel

Fig. 22: 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. 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 CLIENT <i>command</i> or <i>API</i> recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> <li>Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.</li> </ul>
<i>neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 4: Configure recording control/key management

### Group field Data Processing

**Data Processing**

☒ Data storage

☐ Transfer data for replay

Target Server

Name

IP Address ↕

No records found

☒ Transfer data for data storage

Target Server

Name

IP Address ↕

No records found

Activate period of time

☒

Start

0:00

▼

End

4:00

▼

Receives data from

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 24: Group field Data Processing

EVOIP<sub>neo</sub> passive for Mitel MiVoice Connect - *neo* 6.x Rev. 12


27 / 66

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 29</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list", p. 29</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b></p> <p>For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>

Parameter	Value/Description
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <li><i>Replay server</i> From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers.</li> </ul> <p><b>NOTICE!</b> For the export from <i>neo</i> to <i>neo</i>, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <li><i>Recording architecture</i> From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.</li> </ul> <p><b>NOTICE!</b> If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.</p>

Tab. 5: Data storage

### Add target server to a list

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

Target Server	
Name ↕	IP Address ↕
RC-02	192.168.173.176
REC-04	192.168.173.174
RC-01	192.168.173.175
REC-02	192.168.173.172
CTI-01	192.168.173.177
REC-03	192.168.173.173
Rows per page 20 1 - 6 of 6	
<div>Add Cancel</div>	

Fig. 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*

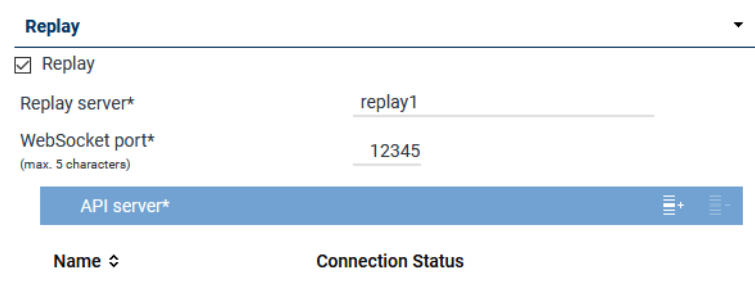




Fig. 26: Group field *Replay*

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 <a href="#">API server</a> 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 <a href="#">POWERplay Web</a> are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add <a href="#">API servers</a> 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 <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 31.</li> <li>By clicking on the icon  (Remove), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

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.

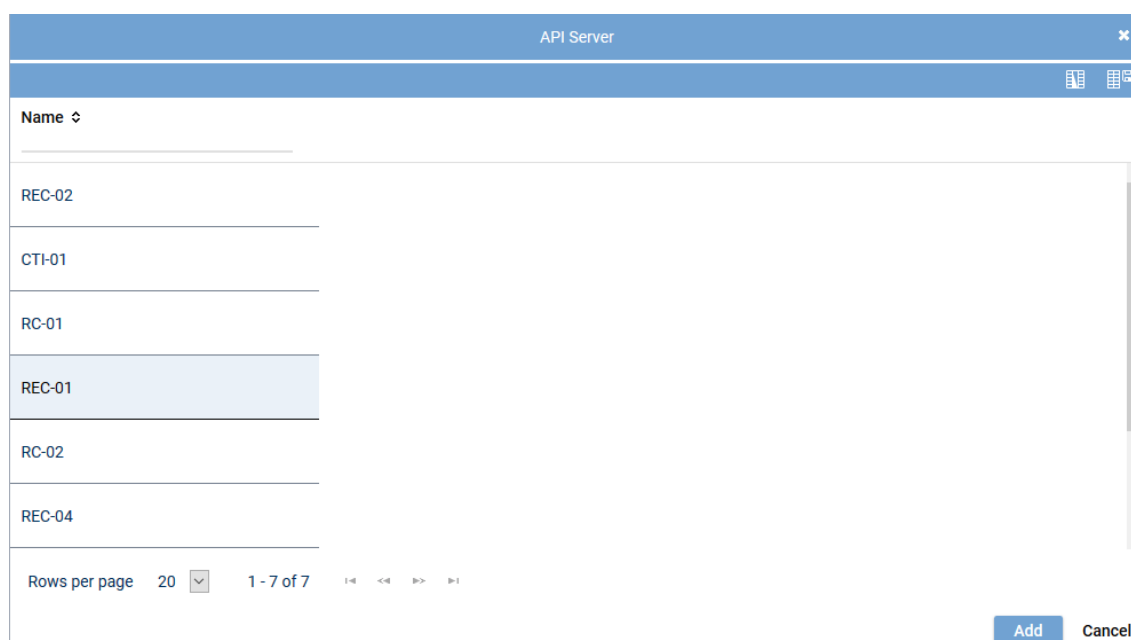


Fig. 27: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 24.

- 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. 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"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> <li>• <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

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.

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. 29: Servers module - tab Media Streamer

2. Enter the following parameters:

<b>PBX</b>	<p><b>PBX</b> that the Media Streamer is supposed to be mapped to.</p> <p>Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a <b>PBX</b> via the blue bar <b>PBX</b>, see <a href="#">chapter "Create PBX"</a>, p. 40.</p>
<b>Extension</b>	<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 <b>8000</b>.</p>
<b>Media streamer IP address</b>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <b>SIP</b> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <b>169.254.254.100</b> in the drop-down list.</p>
<b>Minimum port</b>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<b>Maximum port</b>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p>

	<p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p> <p><b>NOTICE! The port range must not have less than 64 ports.</b></p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the <b>SIP</b> communication.</p> <p><b>TCP</b> = unencrypted  <b>UDP</b> = unencrypted  <b>TLS</b> = encrypted</p> <p>If an external analog gateway has been integrated, select <b>UDP</b> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the <b>SIP</b> communication.</p> <p>Port for data exchange: <b>5062</b></p>
<i>User name</i>	Enter the user name for the authentication on the <b>SIP</b> server.
<i>Password</i>	Enter the password for the authentication on the <b>SIP</b> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <b>SIP</b> registrar of the <b>PBX</b>.</p> <p>If an external analog gateway has been integrated, enter the IP address <b>169.254.254.101</b>.</p>
<i>PBX port</i>	<p>Enter the port of the <b>SIP</b> registrar of the <b>PBX</b>.</p> <p>If an external analog gateway has been integrated, enter the value <b>5060</b>.</p>
<i>Registration required</i>	<p>Select whether the <b>SIP</b> extension has to be registered with the <b>SIP</b> registrar of the <b>PBX</b>.</p> <p><input checked="" type="checkbox"/> = <b>SIP</b> extension has to be registered.  <input type="checkbox"/> = <b>SIP</b> extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <b>Registration required</b>.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

### Tab Replay Server Address Mapping

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

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



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




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

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



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

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



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

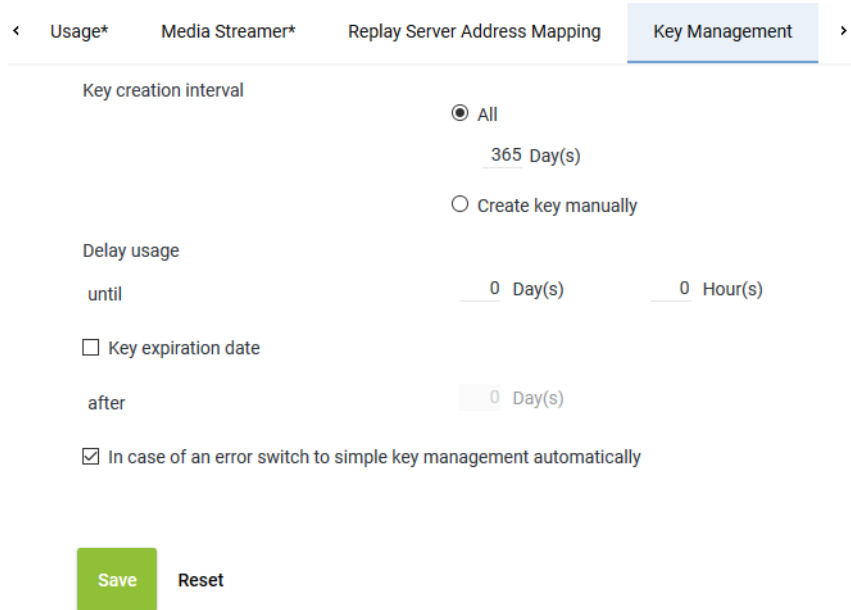


For information about the configuration refer to the administration manual for tenants *User management tenant*.

### Tab Key Management

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

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



The screenshot shows the 'Key Management' tab selected in a navigation bar. Below the navigation bar, there are several configuration options:

- Key creation interval:** A radio button is selected for 'All', with a value of '365 Day(s)' displayed. There is also an option for 'Create key manually'.
- Delay usage:** A section with two input fields: 'until' (set to '0 Day(s)') and '0 Hour(s)'.
- Key expiration date:** A checkbox is unchecked, with an 'after' field set to '0 Day(s)'.
- Automatic switch:** A checkbox is checked, labeled 'In case of an error switch to simple key management automatically'.
- Buttons:** At the bottom left, there are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 31: Servers module - tab Key Management

<b>Key creation interval</b>	<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"> <li>• <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</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</li> </ul>
<b>Delay usage</b>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<b>Key expiration date</b>	<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><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
In case of an error ... automatically	<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.

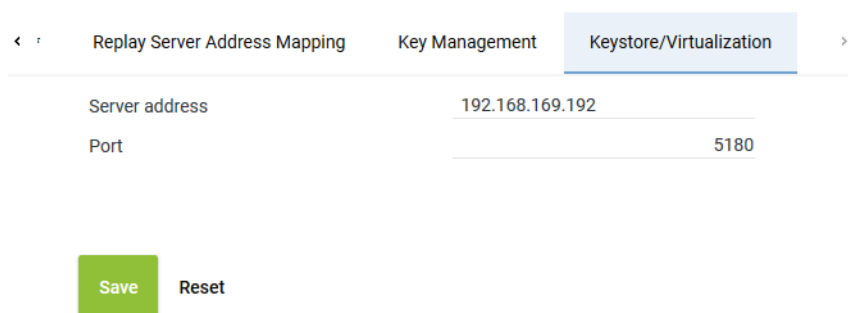
- *Trusted Virtualization License*

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.



Replay Server Address Mapping    Key Management    **Keystore/Virtualization**

Server address    192.168.169.192

Port    5180

**Save**    Reset

Fig. 32: Servers module - tab Keystore/Virtualization

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



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

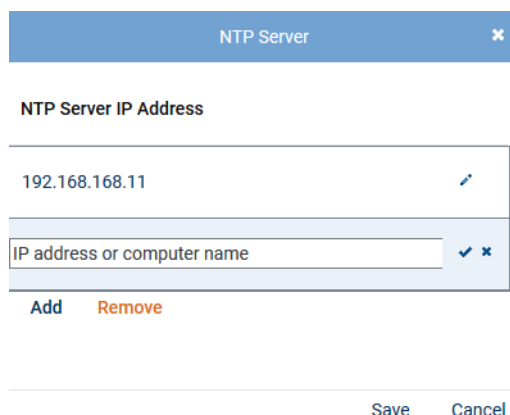
1. To save the settings, click on the button *Save*.  
To discard the settings, click on the button *Reset*.

### Administrate NTP server

The recording system works with an **NTP**-based time synchronization. The function *Administrate NTP server* allows defining several **NTP** servers. Every server in the system identifies all **NTP** servers configured within the system and can use any **NTP** server for time synchronization. That way, every server can connect immediately to another **NTP** server if its current **NTP** server connection breaks down.

### Add NTP server




1. Select the menu item *Servers > Administrate NTP Server* in the toolbar of the main view.  
⇒ The window *NTP Server* appears.



The screenshot shows a window titled "NTP Server" with a close button (X). Below the title bar, there is a section labeled "NTP Server IP Address". It contains a text field with the value "192.168.168.11" and an edit icon (pencil). Below this is a dropdown menu with the text "IP address or computer name" and check/cancel icons. At the bottom of the window, there are "Add" and "Remove" buttons, and at the very bottom, "Save" and "Cancel" buttons.

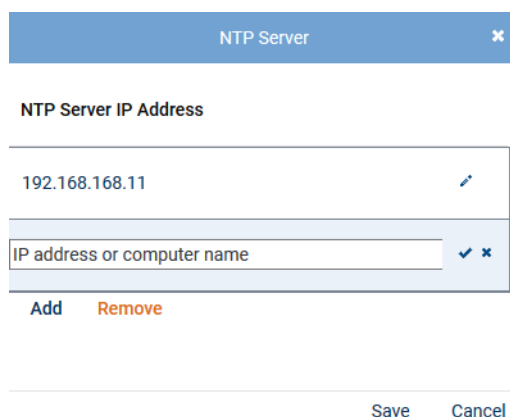
Fig. 33: Add NTP server

The list displays all NTP servers that have been configured during the installation.

2. To add a server, click on the button *Add*.
3. In the newly added row, click on the icon  (*Edit*).
4. Enter the **IP** address or the name of the **NTP** server in the entry field.
5. To save the entry in the row, click on the icon  (*Save*).  
To discard the entry in the row, click on the icon  (*Discard*).
6. To save all changes in the list, click on the button *Save*.  
To discard the changes and close the window, click on the button *Cancel*.




### Edit IP address

1. Select the menu item *Servers > Administrate NTP Server* in the toolbar of the main view.  
⇒ The window *NTP Server* appears.



This screenshot is identical to the one in Figure 33, showing the "NTP Server" window with the "Add" button and the "NTP Server IP Address" field containing "192.168.168.11".

Fig. 34: Edit IP address

2. Click on the icon  (*Edit*) in the row with the **IP** address that you would like to edit.
3. Change the entry in the entry field.
4. To save the change, click on the icon  (*Save*).  
To discard the change, click on the icon  (*Discard*).
5. To save the changes, click on the button *Save*.  
To discard the changes and close the window, click on the button *Cancel*.

### Remove NTP server

1. Select the menu item *Servers > Administrate NTP Server* in the toolbar of the main view.  
⇒ The window *NTP Server* appears.

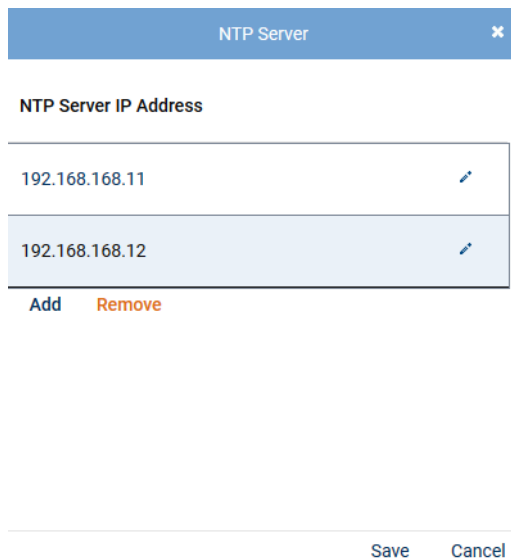


Fig. 35: Remove NTP server

2. In the list, select the **NTP** server that you would like to remove.
3. Click on the button *Remove*.  
⇒ The NTP server is removed from the list.
4. To save the change, click on the button *Save*.  
To discard the change and close the window, click on the button *Cancel*.

#### 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:



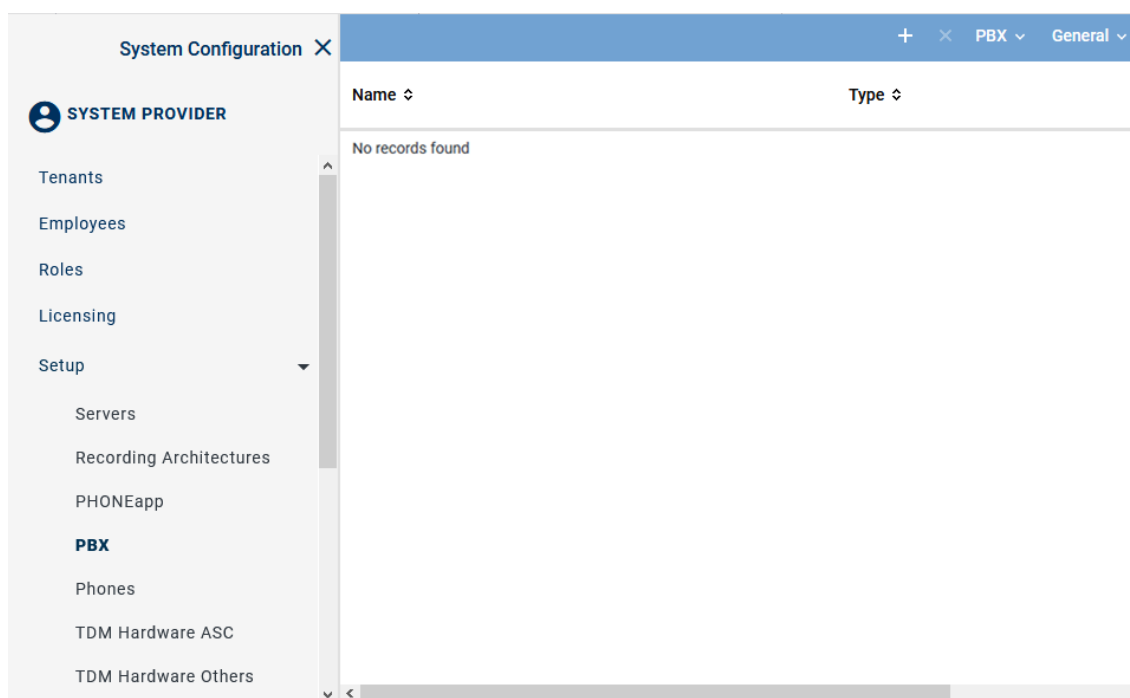


Fig. 36: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

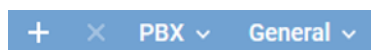




Fig. 37: Toolbar PBX module

	<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"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

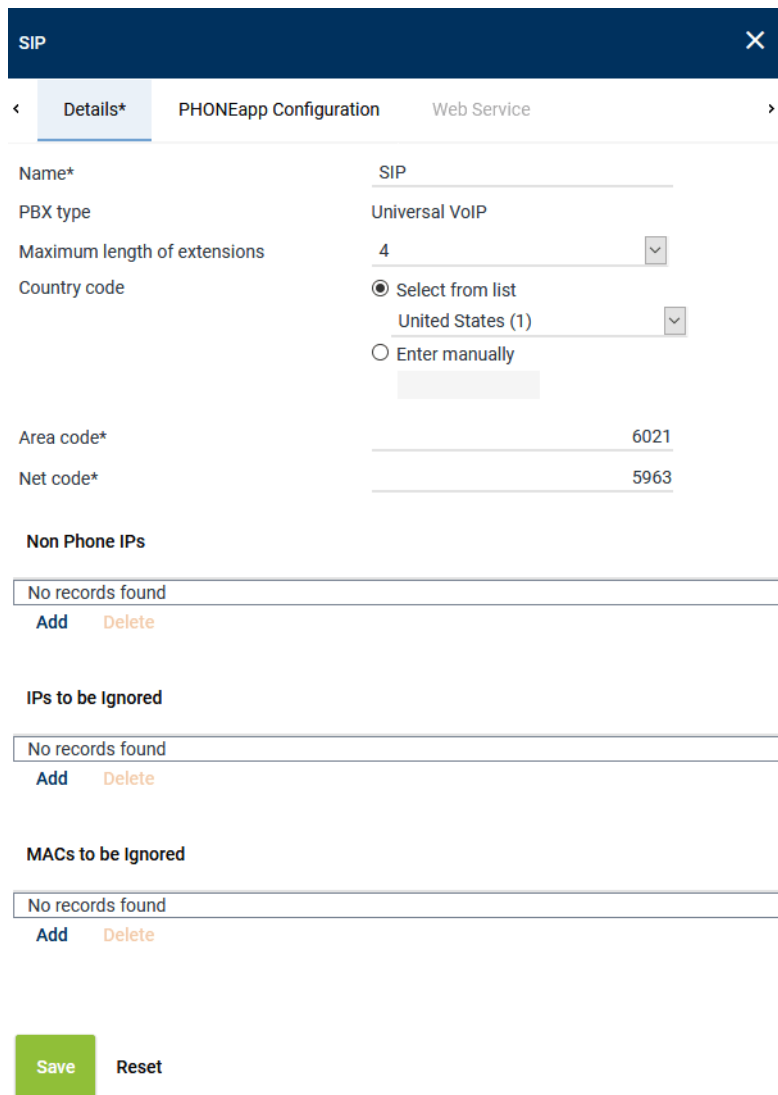


For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

### Create new PBX

1. Click on the icon  (*Create*) in the toolbar of the main view of the PBX module.

⇒ In the detail view, the tab *Details* appears.



**SIP** [X]

< **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. 38: 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 <b>PBX</b> 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"> <li><i>Select from list</i> Select the country code from the drop-down list.</li> <li><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.</li> </ul>
<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

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

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

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

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



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

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

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

#### 7.1.2.1.4 Assign recording resources

##### Resources for tenants

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

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

### Assign extensions to tenants

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

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

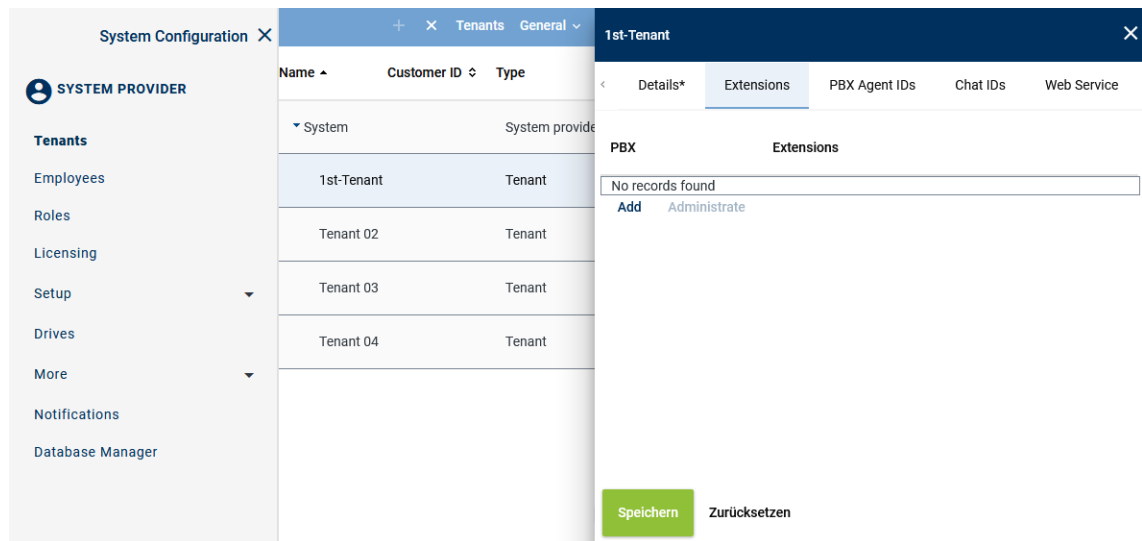


Fig. 39: Tenants - main view - tab Extensions

### 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:

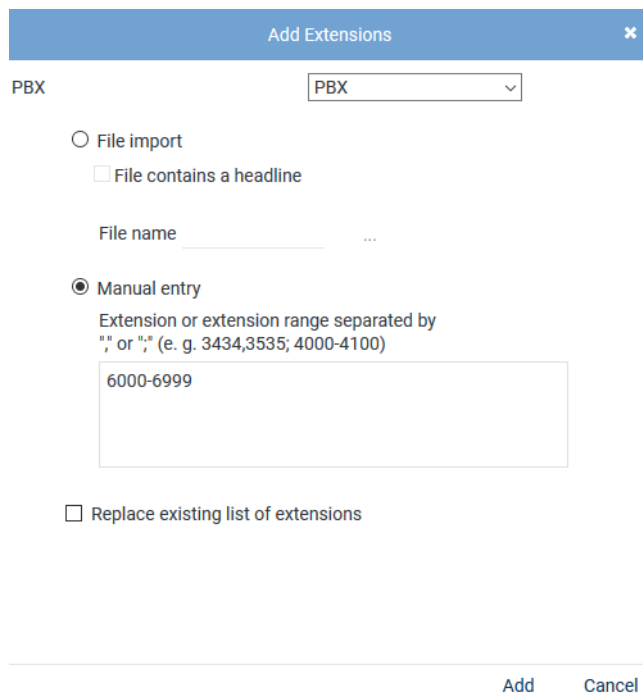




Fig. 40: Assign extensions to tenants

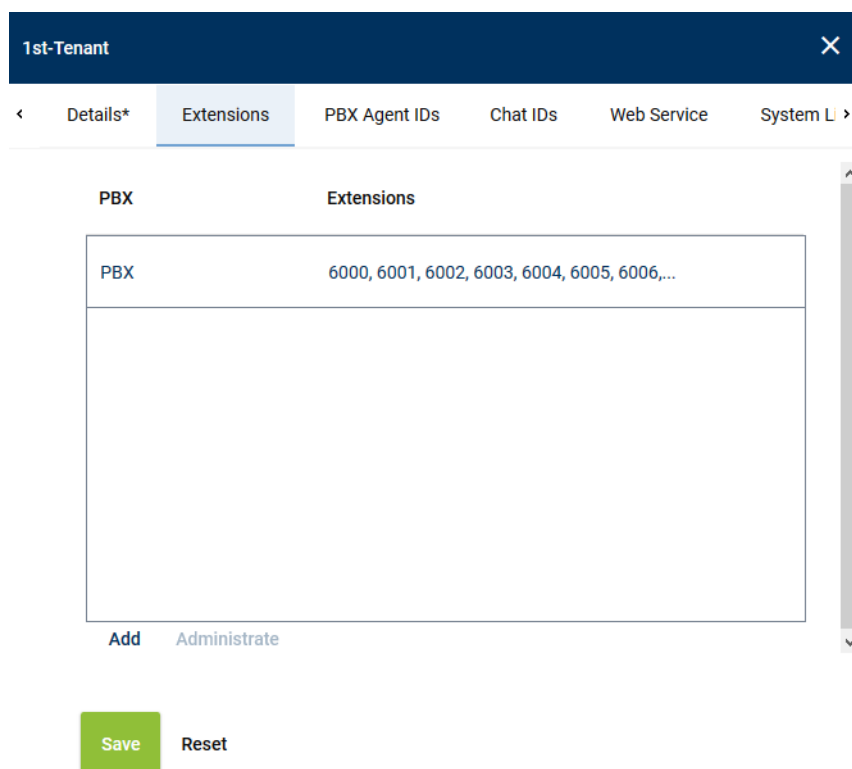
4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported:</p> <ul style="list-style-type: none"> <li>• <i>ZIP</i></li> <li>• <i>TXT</i></li> <li>• <i>CSV</i></li> </ul> <p><b>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.</b></p> <p><i>File contains a headline</i></p> <p>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.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button  behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  <i>Upload File</i>.</li> </ul>
<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><b>NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.</b></p> <p><b>NOTICE! Wildcards cannot be used!</b></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

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



1st-Tenant

< Details\* Extensions PBX Agent IDs Chat IDs Web Service System L >

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

Add Administrate

Save Reset

Fig. 41: Remove extensions

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



Administrate Extensions

6993
6994
6995
6996
6997
6998
6999

Remove Cancel

Fig. 42: Select extensions

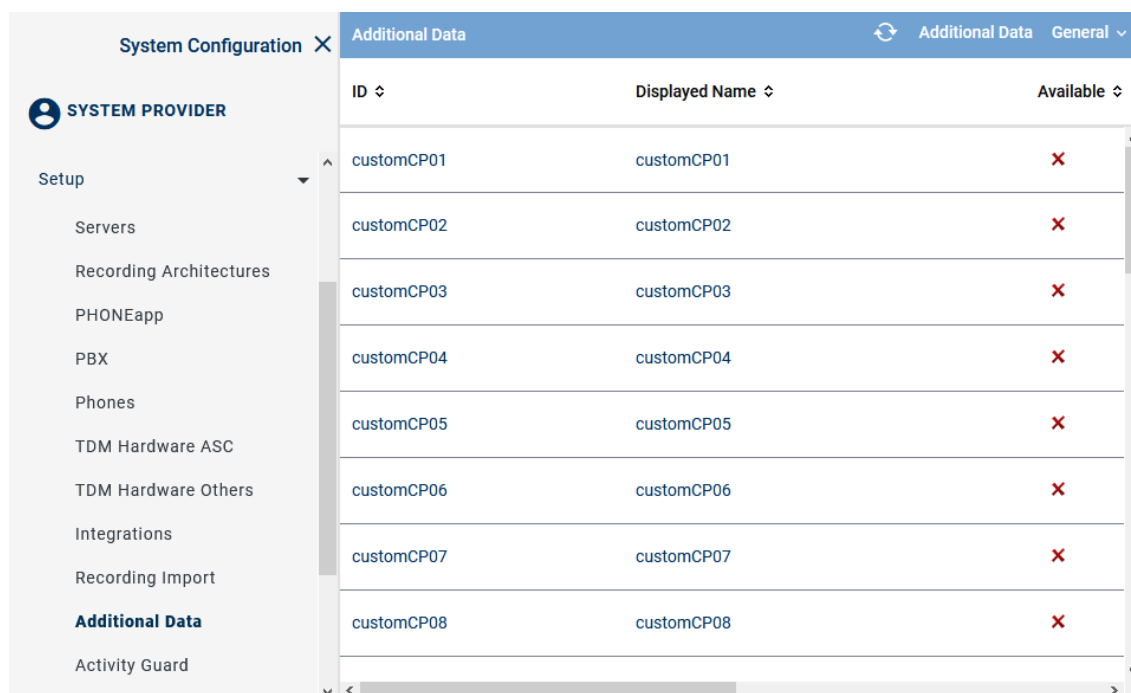
4. To remove the selected extensions, click on the button *Remove*.  
To cancel the process and close the window, click on the button *Cancel*.

### 7.1.2.1.5 Configure additional data

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

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

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



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

Fig. 43: Additional Data module main view

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

### Change display name







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

Fig. 44: Configure additional data

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

### Availability

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

Save
Reset

Fig. 45: Additional data - configure availability

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



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



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

#### 7.1.2.1.6 Create integration for All-in-one Basic

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

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

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

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



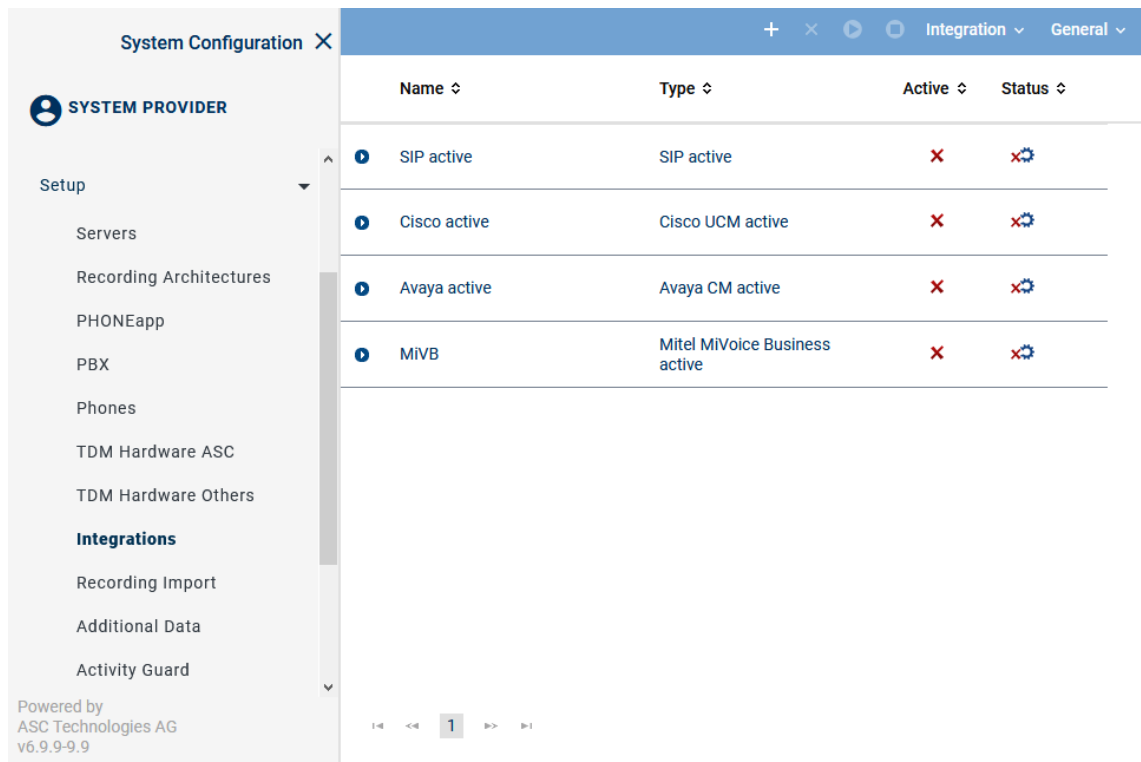


Fig. 46: Integrations - main view

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

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

### Toolbar of the Integrations module

The toolbar offers the following functions.




Fig. 47: Toolbar Integrations module

	<b>Create</b>	Opens the detail view so that you can create a new integration.
	<b>Delete</b>	Deletes the selected integration. The integration can only be deleted if it has been deactivated.
	<b>Activate</b>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<b>Deactivate</b>	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.

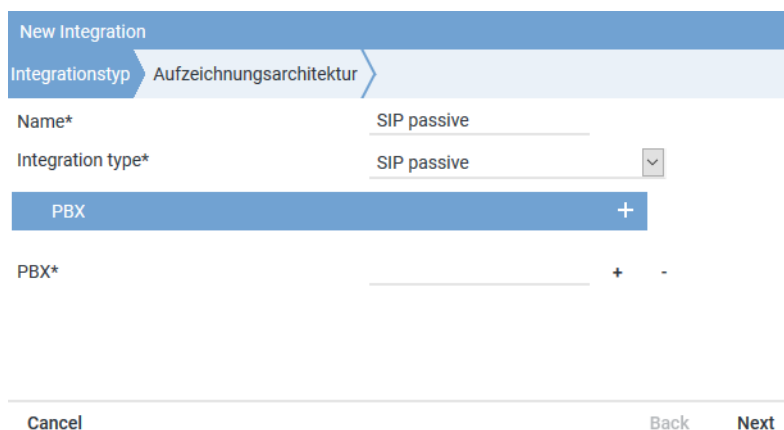



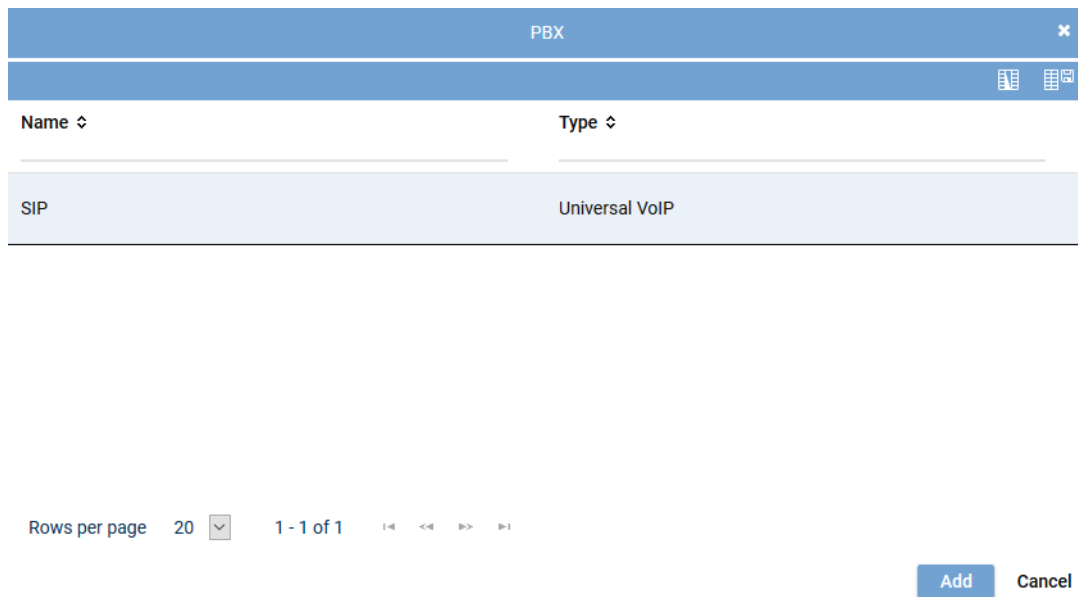
Fig. 48: Create integration type

- Enter the following parameters:

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

Tab. 9: 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. 49: Integrations - select PBX

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

### Assign recording architecture for All-in-one Basic

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



New Integration

Integration Type | Recording Architecture

**Recording Architecture**

Recording architecture\* | All-in-one Basic

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

Fig. 50: 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 passive		SIP passive	X	
Step		Configuration		
Configure recording architecture		✓		
Configure recording servers		X		
Configure add-on		✓		
Configure miscellaneous settings		✓		

Fig. 51: 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. 52: Configuration step - Configure Recording Architecture

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

### Configure recording servers

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

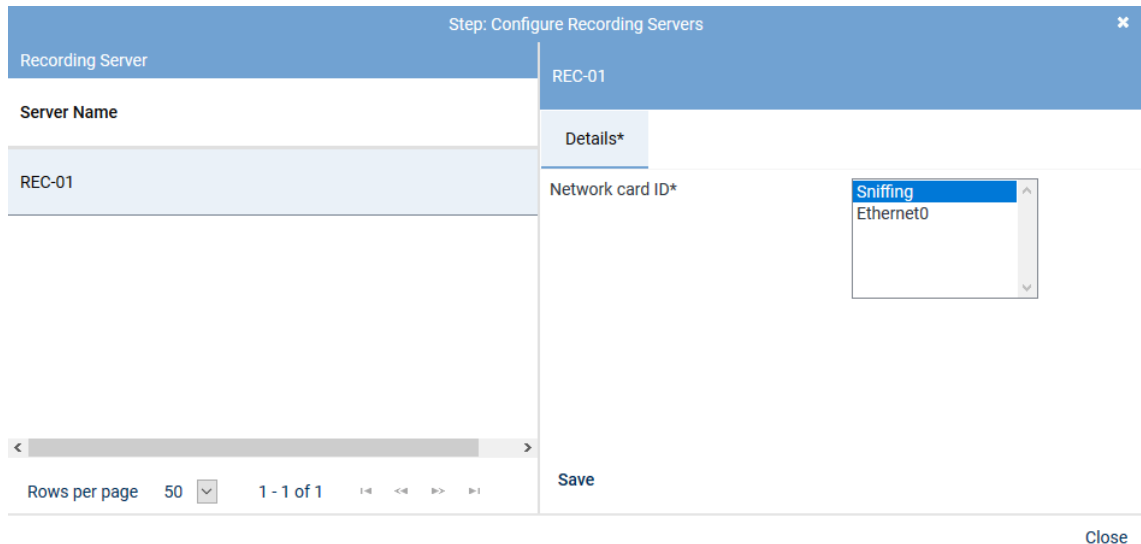


Fig. 53: Configuration step - Configure recording servers

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

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

Tab. 10: Configure recording servers



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

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



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



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

### Configure add-on



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

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



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



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


### Configure 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*.














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

Fig. 54: 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 passive	SIP passive	 

Fig. 55: Activated integration



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



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






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

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

### Deactivate/Delete integration

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

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







+ ×   Integration ▾ General ▾			
Name ▾	Type ▾	Active ▾	Status ▾
 SIP passive	SIP passive		

Fig. 56: Deactivate integration

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

### 7.1.3 Configure Recording Content Validation

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

Preconditions for validation:

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

#### Configuration in the Servers module

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

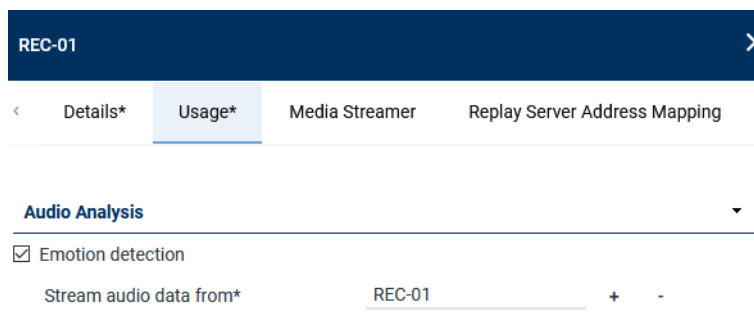



Fig. 57: Servers module - Activate emotion detection

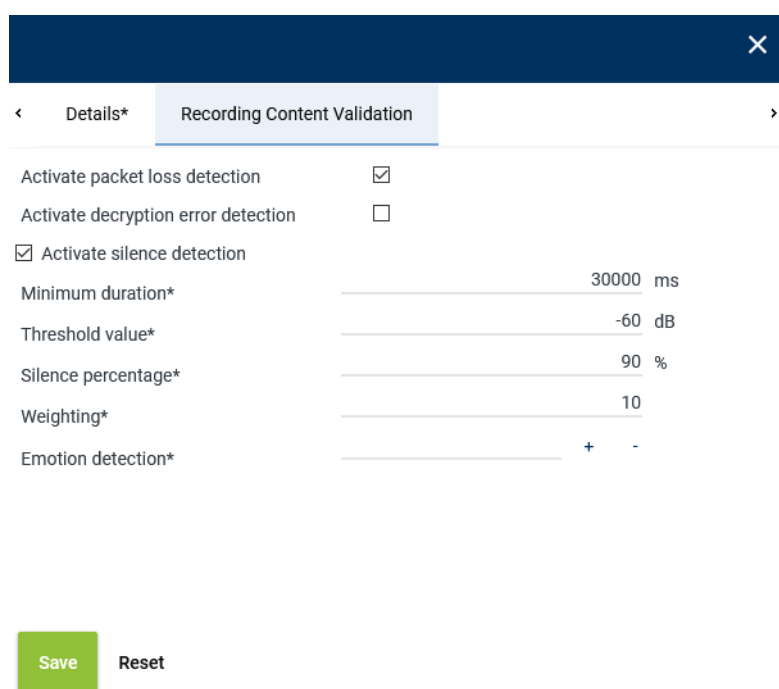
- Activate the function *Emotion detection*.
- By clicking on the icon , select the server that emotion detection runs on.
  - ⇒ This server will then appear in the list in the Integrations module in the tab *Recording Content Validation* to configure silence detection.

### Configuration in the Integrations module

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\* 30000 ms

Threshold value\* -60 dB

Silence percentage\* 90 %

Weighting\* 10


Emotion detection\* + -

Save Reset

Fig. 58: Create integration - tab Recording Content Validation

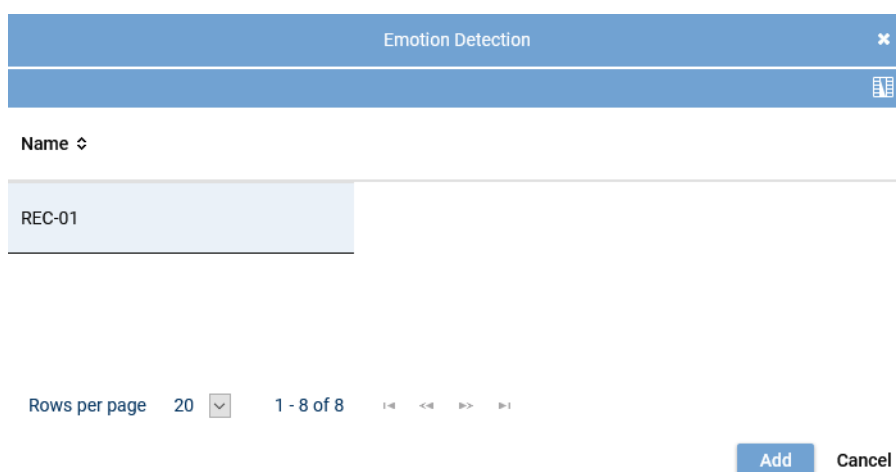
Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost. <b>NOTICE!</b> Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	<b>NOTICE!</b> 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. <b>NOTICE!</b> 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.



Emotion Detection

Name ▾

REC-01

Rows per page 20 ▾ 1 - 8 of 8

Add Cancel

Fig. 59: 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<sub>neo</sub>

To issue a report visualizing the errors occurred, a report must be created in the application INSIGHT<sub>neo</sub>.



For information about using the Report Templates module and the Report Instances module refer to the respective INSIGHT<sub>neo</sub> user manuals.

#### 7.1.4 Configure Recording Planner for DTMF control



The following configuration has to be carried out as the administrator of the tenant.

For external recording control by means of **DTMF**, you must configure the **DTMF** sequences in the Recording Planner module.

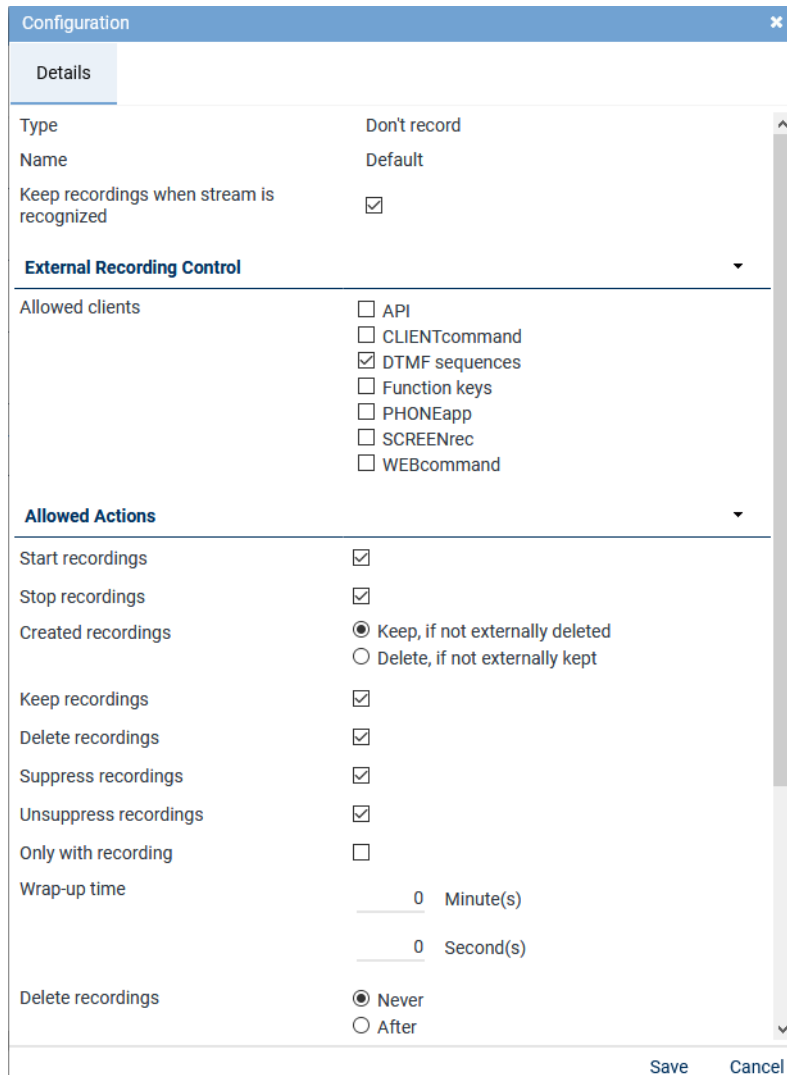


For information about the configuration of recording plans refer to the administration manual for tenants *System Configuration - Recording Planner*.

#### 7.1.4.1

#### Configure profile

- Select the menu item in which you have created your recording plans:
  - *Compliance*
  - *Quality Management*
- Open the existing profile and select the create action node.
  - ⇒ The detail view opens.



The screenshot shows a 'Configuration' window with a 'Details' tab. The configuration is as follows:

Type	Don't record
Name	Default
Keep recordings when stream is recognized	<input checked="" type="checkbox"/>
<b>External Recording Control</b>	
Allowed clients	<input type="checkbox"/> API <input type="checkbox"/> CLIENTcommand <input checked="" type="checkbox"/> DTMF sequences <input type="checkbox"/> Function keys <input type="checkbox"/> PHONEapp <input type="checkbox"/> SCREENrec <input type="checkbox"/> WEBcommand
<b>Allowed Actions</b>	
Start recordings	<input checked="" type="checkbox"/>
Stop recordings	<input checked="" type="checkbox"/>
Created recordings	<input checked="" type="radio"/> Keep, if not externally deleted <input type="radio"/> Delete, if not externally kept
Keep recordings	<input checked="" type="checkbox"/>
Delete recordings	<input checked="" type="checkbox"/>
Suppress recordings	<input checked="" type="checkbox"/>
Unsuppress recordings	<input checked="" type="checkbox"/>
Only with recording	<input type="checkbox"/>
Wrap-up time	0 Minute(s) 0 Second(s)
Delete recordings	<input checked="" type="radio"/> Never <input type="radio"/> After

Buttons: Save, Cancel

Fig. 60: Recording Planner - activate DTMF function



An action node can only be edited as long as the profile has not been activated.

- Activate the following parameters:

#### General parameters

*Keep recordings when stream is recognized*

Activate the check box if only those recordings are supposed to be kept for which an audio stream could be recognized.

### Group field External Recording Control

- Under *Allowed clients*, activate DTMF control:

<i>Allows clients</i>	DTMF control
-----------------------	--------------

### Group field Allowed Actions

- Activate the following options:

<i>Start/Stop recordings</i>	Allows manually starting and stopping recordings for all clients activated under <i>External Recording Control</i> .
<i>Created recordings</i> <i>Keep, if not externally deleted</i> or <i>Delete, if not externally kept</i>	Select one of the two options. Created recordings can be kept or deleted by default if no external control interferes.
<i>Delete/Keep recordings</i>	Allows deleting or keeping recorded conversations by manual control by means of function keys.
<i>Suppress/Unsuppress recordings (optional)</i>	Allows suppressing a recording of a running conversations without having to stop it. This function is available for all recording formats.

- Click on the button **Save**.
- Activate the profile.

#### 7.1.4.2 Define DTMF sequences

For recording control by means of **DTMF**, you must configure the sequences.

- Select the menu item *Recording Planner > DTMF Sequences* in the toolbar.
- Define the character combinations for the commands.

DTMF Sequences ×

Start recording	*111#
Stop recording	*222#
Keep recording	*555#
Delete recording	*666#
Suppress recordings of all participants	*333#
Unsuppress recording of all participants	*444#
Suppress recordings of internal participants	*3331#
Unsuppress recording of internal participants	*4441#
Suppress recordings of external participants	*3332#
Unsuppress recording of external participants	*4442#

Save
Cancel

Fig. 61: Define DTMF sequences

A **DTMF** sequence is any sequence of the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, \*,

The following commands are available:

- *Start recording*
- *Stop recording*
- *Keep recording*
- *Delete recording*
- *Suppress recordings of all participants*
- *Unsuppress recordings of all participants*
- *Suppress recordings of internal participants*
- *Unsuppress recordings of internal participants*
- *Suppress recordings of external participants*
- *Unsuppress recordings of external participants*



---

Ensure that the configured sequences are not used for other functions already.

---

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

## 8 Troubleshooting



Before initiating any troubleshooting measures, verify that the recording solution has been configured according to the description in the manual and check whether an up-to-date hotfix version with bug fixes is available.

**If no calls or additional data have been recorded check:**

- whether the correct network device has been selected in System Configuration, see [chapter "Configure server", p. 19](#)
- the correct configuration of the SPAN port

**When opening a ticket, include the following information:**

- Log files with test calls  
**NOTICE!** Before creating any log files, adjust the settings of the log levels in the Log Level module in System Monitoring as described below, see user manual *System Monitoring*.
- detailed description of the issue and of the scenarios of the test calls which have been made
- extension, MAC IP address of the affected device
- manufacturer, type, and software version of the PBX
- Wireshark traces of the recording network interface

**Log level settings**

Module	Log level
RECORDING_CONTROL	DEBUG
RECORDING_MODULE_MANAGER	DEBUG
API_SERVER	DEBUG
FILE_MANAGER	DEBUG

## List of figures

Fig. 1	Overview of the recording solution.....	6
Fig. 2	System Configuration - web interface .....	12
Fig. 3	System Configuration - main view:.....	13
Fig. 4	Recording architectures - main view .....	14
Fig. 5	Toolbar Recording Architectures module.....	14
Fig. 6	Create recording architecture - All-in-one Basic Recording .....	16
Fig. 7	Recording architecture - tab Details.....	16
Fig. 8	Select integration type.....	17
Fig. 9	Recording architecture - tab Server Assignment .....	18
Fig. 10	Recording architecture - assign server .....	18
Fig. 11	Recording architecture - activate recording variant.....	19
Fig. 12	Recording architecture - activate recording architecture.....	19
Fig. 13	Servers - main view.....	20
Fig. 14	Toolbar Servers module.....	20
Fig. 15	Add server locations.....	21
Fig. 16	Delete server location .....	22
Fig. 17	Servers - tab Details.....	23
Fig. 18	Servers - tab usage.....	23
Fig. 19	Group field API Server .....	24
Fig. 20	Select storage expansion.....	25
Fig. 21	Group field Audio Analysis.....	26
Fig. 22	Select server for emotion detection.....	26
Fig. 23	Group field Recording Control/Key Management .....	26
Fig. 24	Group field Data Processing .....	27
Fig. 25	Select server .....	29
Fig. 26	Group field Replay .....	30
Fig. 27	Select server .....	31
Fig. 28	Group field Virtualization .....	32
Fig. 29	Servers module - tab Media Streamer .....	33
Fig. 30	Servers Module - tab Replay Server Address Mapping.....	35
Fig. 31	Servers module - tab Key Management.....	36
Fig. 32	Servers module - tab Keystore/Virtualization .....	38
Fig. 33	Add NTP server.....	39
Fig. 34	Edit IP address.....	39
Fig. 35	Remove NTP server.....	40
Fig. 36	PBX module - main view .....	41
Fig. 37	Toolbar PBX module .....	41
Fig. 38	Create new PBX - tab Details .....	42
Fig. 39	Tenants - main view - tab Extensions .....	44
Fig. 40	Assign extensions to tenants .....	44
Fig. 41	Remove extensions.....	46

Fig. 42	Select extensions .....	46
Fig. 43	Additional Data module main view .....	47
Fig. 44	Configure additional data .....	47
Fig. 45	Additional data - configure availability .....	48
Fig. 46	Integrations - main view .....	49
Fig. 47	Toolbar Integrations module .....	49
Fig. 48	Create integration type .....	50
Fig. 49	Integrations - select PBX.....	51
Fig. 50	Assign recording architecture - All-in-one Basic .....	51
Fig. 51	Configuration steps of the integration .....	52
Fig. 52	Configuration step - Configure Recording Architecture.....	52
Fig. 53	Configuration step - Configure recording servers .....	53
Fig. 54	Activate integration.....	54
Fig. 55	Activated integration.....	54
Fig. 56	Deactivate integration .....	55
Fig. 57	Servers module - Activate emotion detection.....	55
Fig. 58	Create integration - tab Recording Content Validation.....	56
Fig. 59	Select server for emotion detection.....	57
Fig. 60	Recording Planner - activate DTMF function .....	58
Fig. 61	Define DTMF sequences .....	59

**List of tables**

Tab. 1	Licenses of ASC.....	9
Tab. 2	Login data - system provider.....	12
Tab. 3	Configure audio analysis.....	26
Tab. 4	Configure recording control/key management .....	27
Tab. 5	Data storage.....	28
Tab. 6	Configure replay.....	30
Tab. 7	Configure virtualization.....	32
Tab. 8	Create PBX .....	42
Tab. 9	Create integration type.....	50
Tab. 10	Configure recording servers.....	53



## Glossary

### API

Application Programming Interface

### API server

Server on which the API service runs. (API=Application Programming Interface)

### DNS

Domain Name System is a worldwide directory service which administrates the name domain of the Internet. Its main task is to answer the queries regarding name resolutions. (Source: Wikipedia 5th April 2017)

### DTMF

Dialed Dual Tone Multi Frequency keys represent dialing signals on the analog connecting cable of the telephone. This is a method to transmit the phone number to the telephone network or to a PBX.

### IP

Internet Protocol, basic protocol for Internet communication

### LCR

Last Conversation Repeat

### Monitor/Mirror/SPAN Port

Port mirroring is used to copy a network package, which passes a switch port, to another switch port.

### NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

### PBX

Private Branch Exchange

### RTP

Real-time Transport Protocol is a protocol to continuously transmit audio and video files via the IP protocol within the network.

### SDP

The Session Description Protocol describes properties of multimedia data streams. It serves to manage communication sessions and is used together with SIP and H.323 for instance within the IP telephony to deal codecs, transport protocols and addresses as well as for the transmission of meta data. (Source: Wikipedia 4th May 2017)

### SIP

Session Initiation Protocol

---

**SSL**

Secure Socket Layer

---

**TCP**

Transmission Control Protocol, controlled connection establishment, secure data transmission, controlled connection termination

---

**TDM**

Time Division Multiplexing is an umbrella term for time-slot-oriented interfaces, ITU G.703 defined. The term is used ASC-wide representative for conventional telephony.

---

**TLS**

Transport Layer Security, former name Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

---

**UDP**

User Datagram Protocol UDP is a minimal, connectionless network protocol which belongs to the core members of the Internet protocol suite. Its purpose is to make sure that data transmitted via the Internet reach the designated application. There is no destination check.

---

**URL**

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)

---

**VM**

Virtual machine

---

**VoIP**

Voice over IP

---