Video Communication Recording for SIP active

Administration manual

for system providers

10/16/2020

Product line *neo*, version 6.x

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

EVOIP*neo*

EVOLUTION*neo* / XXL / eco

EVO*flex* (country-specific)

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

Copyright © 2019 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.

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

Contents

1 General information ... 4

2 Introduction ... 5

3 System requirements ... 6

3.1 Hardware components ... 6

3.1.1 Recorder ... 6

3.2 Software components ... 6

3.3 External components ... 6

3.3.1 PBX ... 6

3.3.2 Supported PBXs and end devices ... 6

3.3.3 Additional requirements and restrictions ... 7

4 Installation requirements ... 8

4.1 Licenses ... 8

4.2 Information ... 8

5 Overview install and configure product ... 9

6 Installation ... 10

7 Configuration ... 11

7.1 System Configuration ... 11

7.1.1 Start application ... 11

7.1.2 Configure recording solution ... 12

7.1.2.1 Configure recording solution All-in-one Basic ... 12

List of figures ... 60

List of tables ... 62

Glossary ... 63

1 General information

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

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

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

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

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization of ASC.

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

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

2 Introduction

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

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

The recording solution Video Communications Recording for SIP active is based on the software EVOIP*neo* active for SIP which provides the functionality which is necessary for the active IP recording of unencrypted and encrypted video conversations in a SIP environment.

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

The recording server receives the conversation data which is supposed to be recorded as a mixed RTP data stream. The additional data is extracted from the SIP signaling.

The video conversations are encrypted in the ASC proprietary file format and stored on the recording server.

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

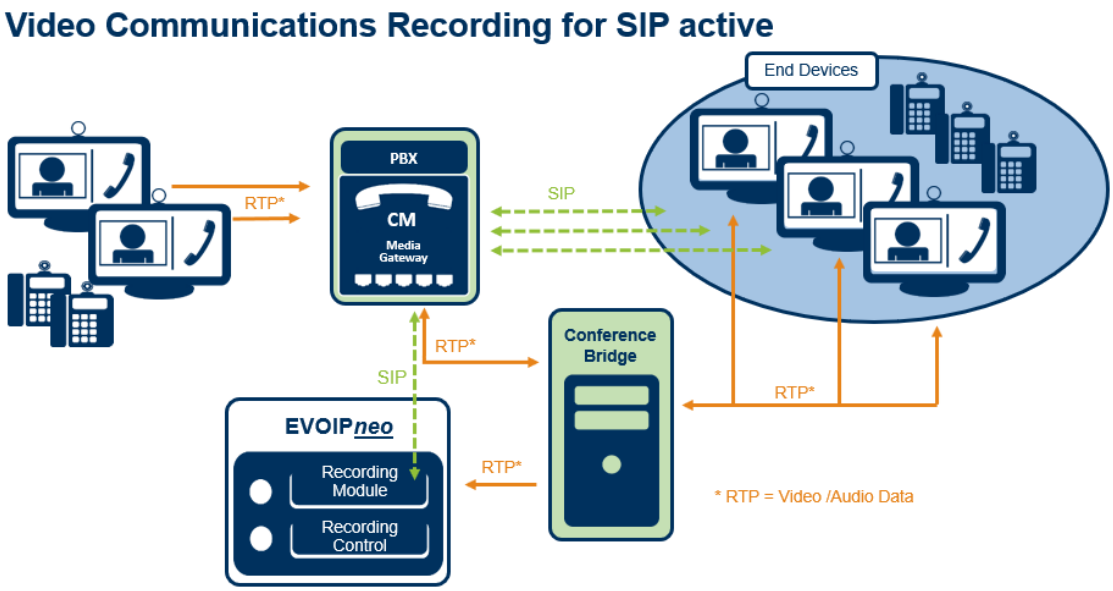

Fig. 1: Overview of the recording solution

3 System requirements

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

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

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

3.1 Hardware components

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

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

3.1.1 Recorder

For the recording solution you can use the following systems:

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

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

3.2 Software components

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

3.3 External components

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

3.3.1 PBX

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

3.3.2 Supported PBXs and end devices

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

The following RFC standards are supported:

- RFC 3261 (SIP)
- RFC 3550 (RTP)
- RFC 3665 (SIP Basic Call Flow Examples)
- RFC 3711 (SRTP)

- RFC 4566 (SDP Session Description Protocol)
- RFC 4568 (SDES)
- RFC 4733 (DTMF) optional

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

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

3.3.3 Additional requirements and restrictions

- Early Media must be deactivated.
- Voice Activity Detection (VAD) or silence suppression must be deactivated.
- The SIP authentication methods *basic* and *auth* are supported.

4 Installation requirements

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

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

4.1 Licenses

ASC

License name	Number
EVOIP*neo* Base license - active	1 license per recording server
EVOIP*neo* active for SIP	1 license per concurrent recording
Video Communications Recording for SIP active	1 license per agent to be recorded

Tab. 1: Licenses of ASC

4.2 Information

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

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

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

5 Overview install and configure product

The following steps have to be carried out:

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

       A server can be used for archiving, import, export, replay, data storage or for audio analysis.
   - Create PBX
     - A PBX configuration can either be created via the PBX module or via the configuration in the Integrations module.
   - Create, configure, and activate integration
     - Configure recording architecture
       Link the integration to the previously created recording architecture.
     - Global recording settings
       Configuration of port and transport protocol for SIP signaling
     - Configure recording servers
       Configuration of the parameters of the recording server, e. g. IP address, incoming port for RTP, and extensions.

Additional configuration steps for video recording

- Activate video support
  - For a working recording of video conversations, you have to activate the parameter for the support of video in the configuration file of the Recording module. See Activate video support.
- Configure employees
  - To be able to record the video conversations of agents, you have to configure the respective employees as agents in the Employees module and configure their *extension* or their *PBX Agent ID* in the agent data in the group field *Telephony* as well as activate the option *Video recording* in the group field *Miscellaneous Settings*.
    For this configuration you have to log in to the application System Configuration as 1st-tenant-admin.
- Configure Recording Planner
  - To be able to record the video conversations, you have to activate the option *Record video* in the Recording Planner module in the Quality Management module.
    For this configuration you have to log in to the application System Configuration as 1st-tenant-admin.
- Configure miscellaneous settings
  Optional configuration of participant information in an additional data field

6 Installation

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

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

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

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.

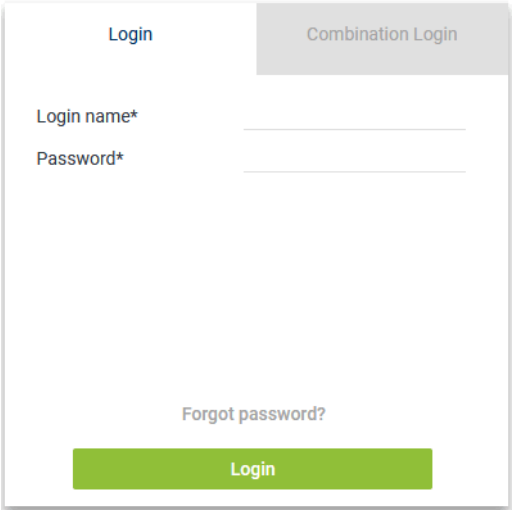

Fig. 2: System Configuration - web interface

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

Tab. 2: Login data - system provider

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

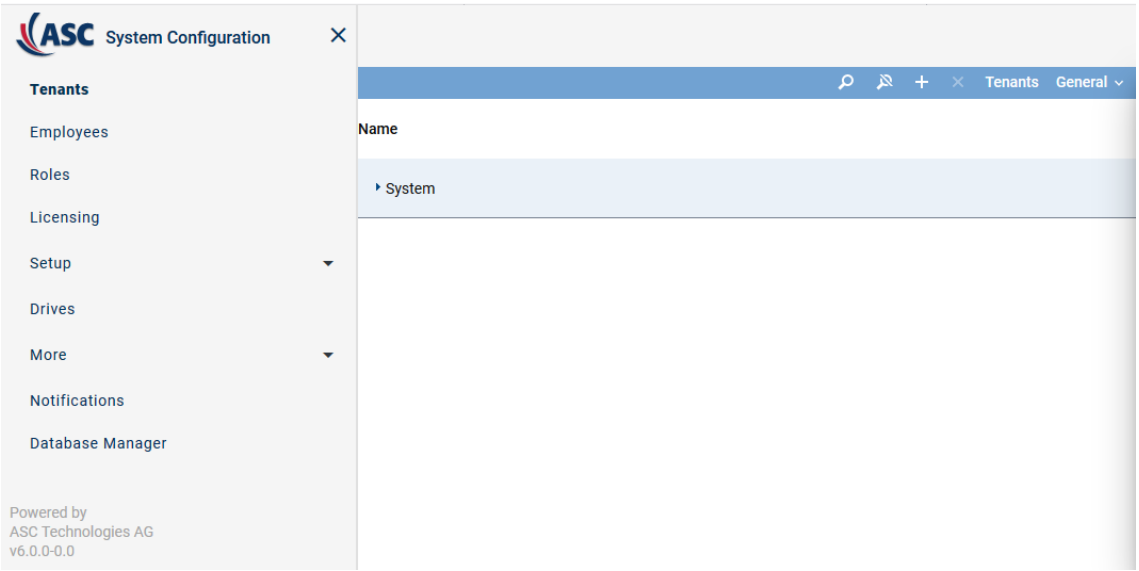

Fig. 3: System Configuration - main view:

7.1.2 Configure recording solution

Supported recording architectures

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

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

7.1.2.1 Configure recording solution All-in-one Basic

7.1.2.1.1 Create recording architecture

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

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

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

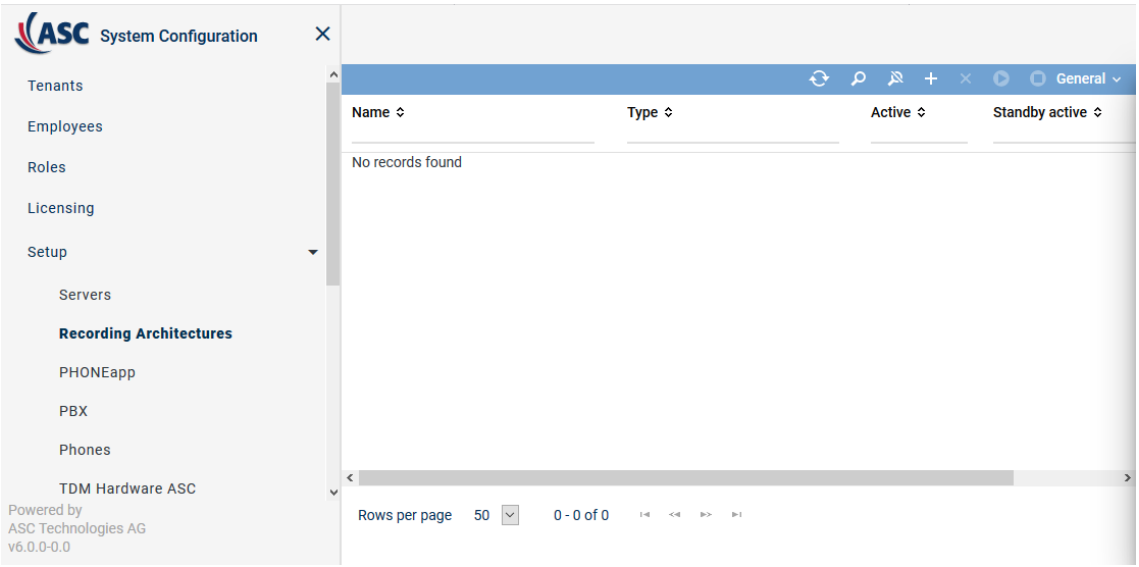

Fig. 4: Recording architectures - main view

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

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

Toolbar of the Recording Architectures module

The toolbar offers the following functions.

Fig. 5: Toolbar Recording Architectures module

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

+	*Create*	Creates a new recording architecture.
×	*Delete*	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. **NOTICE!** You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
▶	*Activate*	Activates the selected recording architecture.
◯	*Deactivate*	Deactivates the selected recording architecture. **NOTICE!** You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
Recording Architectures	*Standby management*	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	Save Table Configuration	Saves the current table configuration of the main view as default view of the user.
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

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

Create recording architecture All-in-one Basic

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

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

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

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

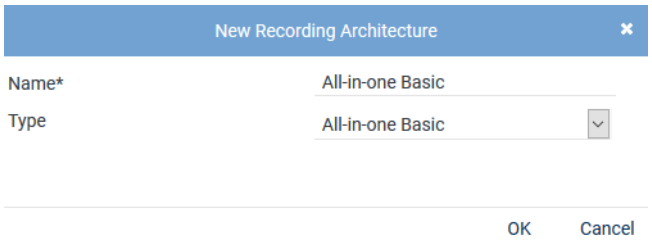

Fig. 6: Create recording architecture - All-in-one Basic Recording

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

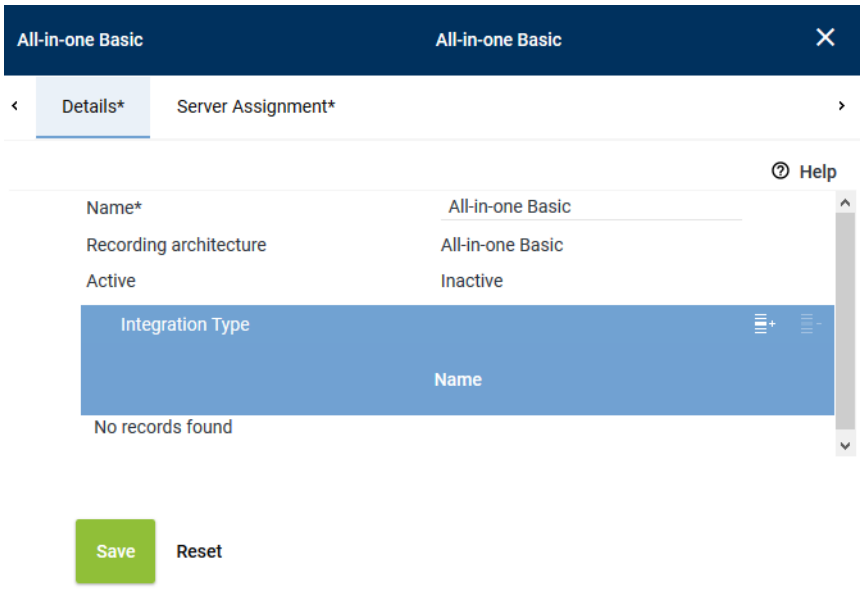

Fig. 7: Recording architecture - tab Details

Add integration type

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

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

Assign server for All-in-one Basic

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

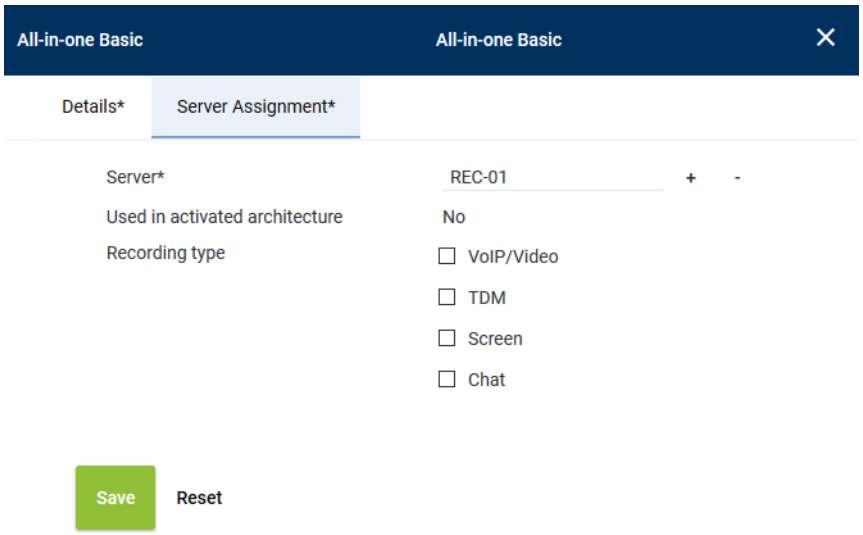

Fig. 9: Recording architecture - tab Server Assignment

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

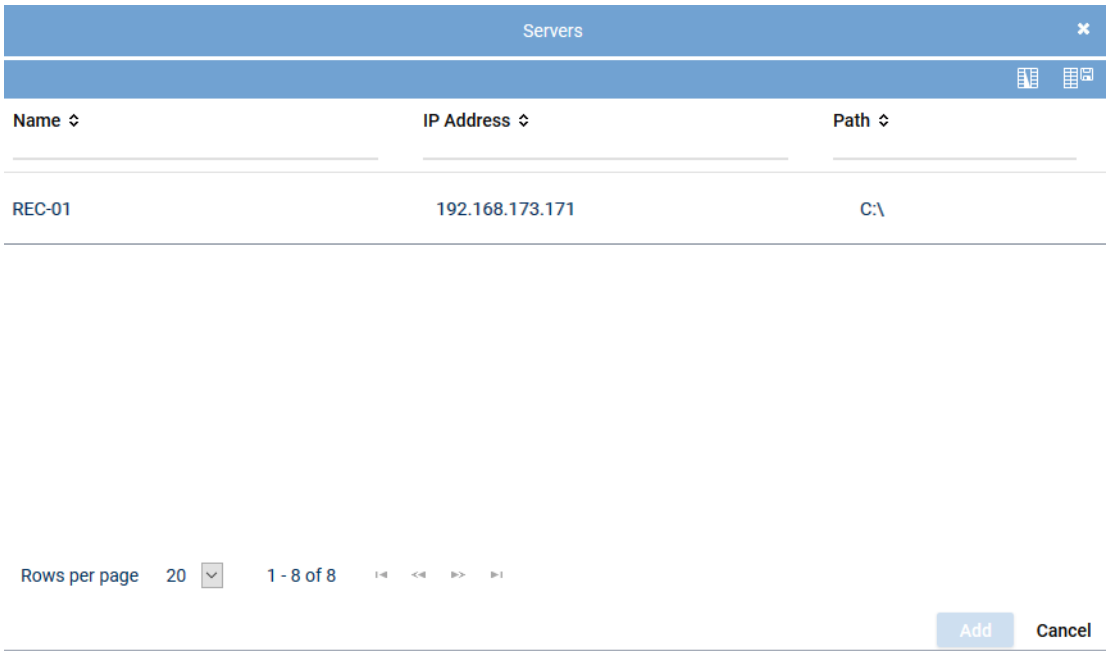

Fig. 10: Recording architecture - assign server

3. Select the respective server.

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

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

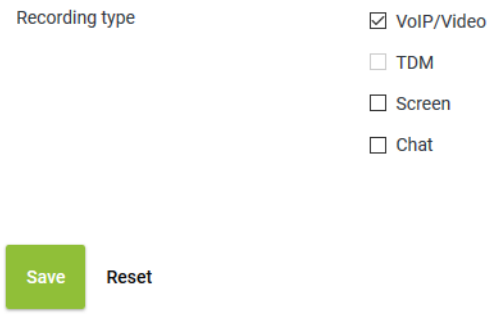

Fig. 11: Recording architecture - activate recording variant

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 toolbar becomes active.

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

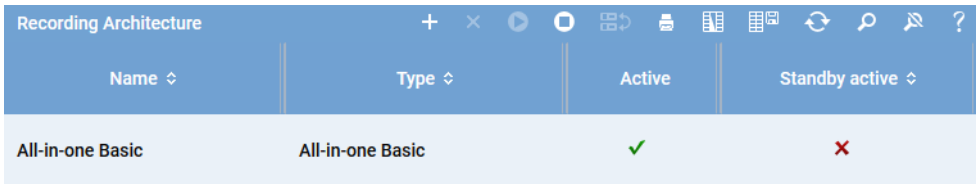

Fig. 12: Recording architecture - activate recording architecture

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.

ⓘ For updates, the recording architecture is stopped and deactivated. Once the update has been completed, check that the recording architecture has been activated again.

ⓘ 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:

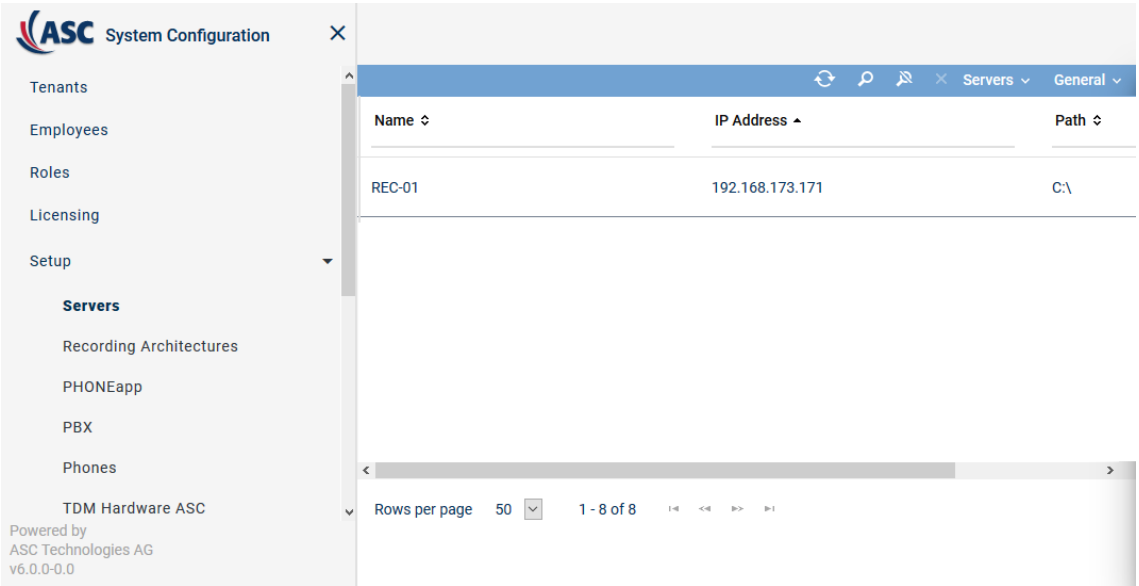

Fig. 13: Servers - main view

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

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

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

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

Toolbar of the Servers module

The toolbar offers the following functions.

Fig. 14: Toolbar Servers module

	Refresh	Refreshes the main view.
	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria. The icon is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all search filters so that all sets of data are displayed in the main view again.
	Delete	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the *neo* system.
Servers	*Administrate Server Locations*	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations", p. 19.
	Administrate NTP server	Opens a window in which you can administrate the servers for the time synchronization, see Administrate NTP server.
	Manage Synchronization Configurations	Opens a window in which you can manage the synchronization configurations.
General	*Adjust Table*	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*
	Save Table Configuration	Saves the current table configuration of the main view as default view of the user.
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

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

Administrate server locations

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

Add server locations

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

   ⇨ The window *Server Locations* appears.

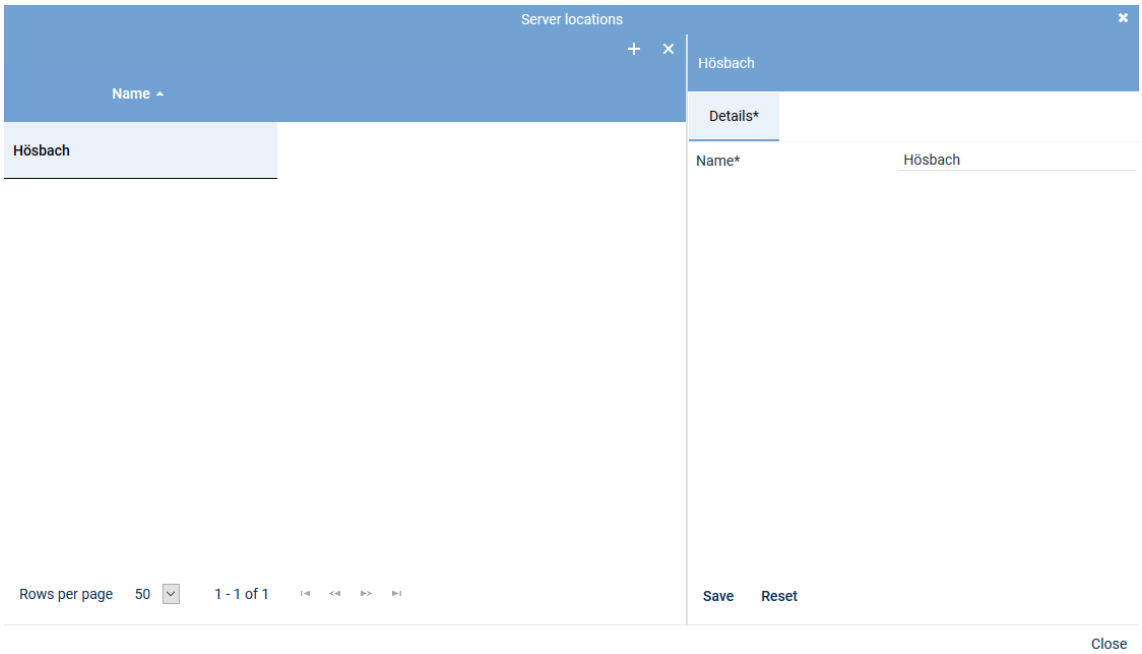

Fig. 15: Add server locations

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

Delete server location

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

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

   ⇨ The window *Server Locations* appears.
2. Select the location you would like to delete.

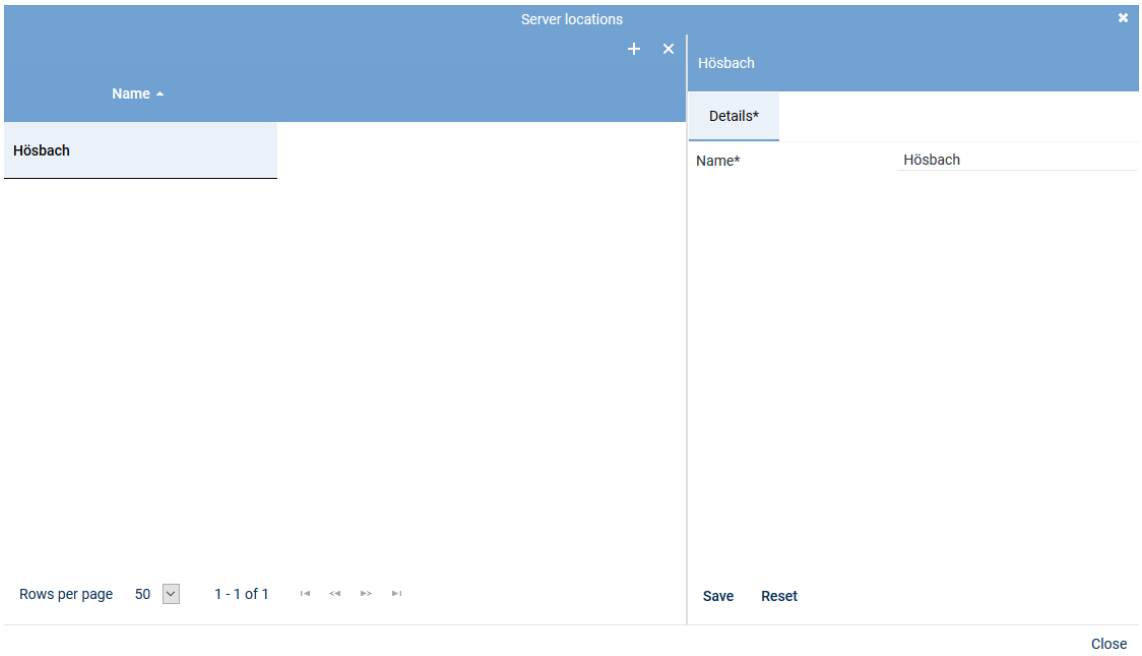

Fig. 16: Delete server location

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.

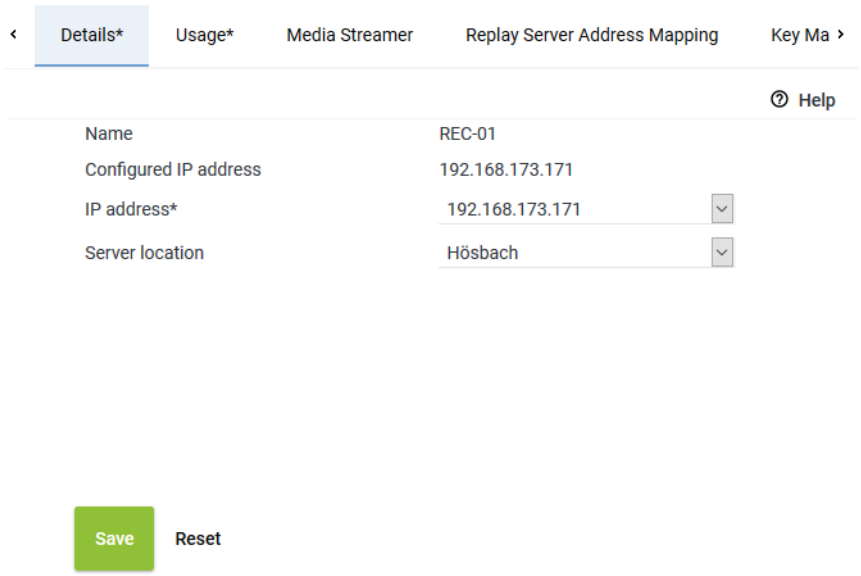

Fig. 17: Servers - tab Details

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

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

Tab Usage

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

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

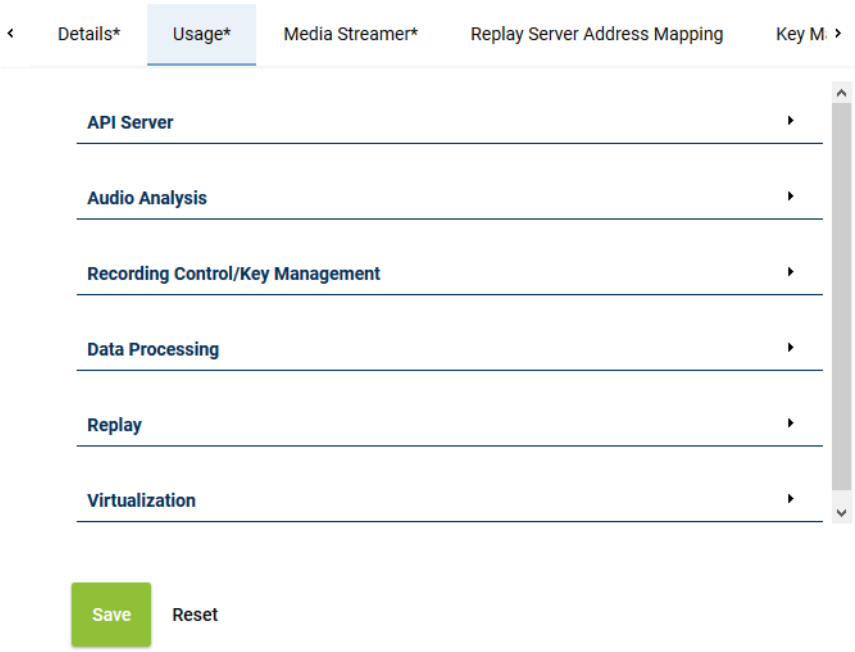

Fig. 18: Servers - tab usage

Group field API Server

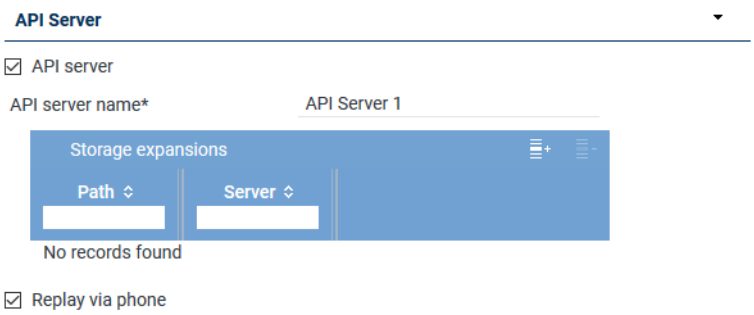

Fig. 19: Group field API Server

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

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

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

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

Parameter	Value/Description
API server	Tick the check box to start the API server. ☑ = Function has been activated. You have to complete the entry field *API server*. ☐ = Function has not been activated. In order to be able to reach the API server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab *Replay Server Address Mapping*, see chapter "Tab Replay Server Address Mapping", p. 32.
API server name	Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym. The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.
List *Storage expansions*	Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the storage expansions, see chapter "Add storage expansion for replay", p. 24. • By clicking on the icon *(Remove)*, you can remove the storage expansions from the list. If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
Replay via phone	Activate this function if you would like to use the functions *Replay via phone* or *Last Call Repeat*. ☑ = Function has been activated. ☐ = Function has not been activated. **NOTICE!** The function *Replay via phone* has been implemented in the following *neo* components: • Application POWER*play* Pro • Application POWER*play* Instant • Replay module In order to enable a client to use the functionality *Replay via phone*, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.

Parameter	Value/Description
	NOTICE! In the tab *Media Streamer*, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 31. To be able to do so, at least 1 PBX must have been configured in the system.

Add storage expansion for replay

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

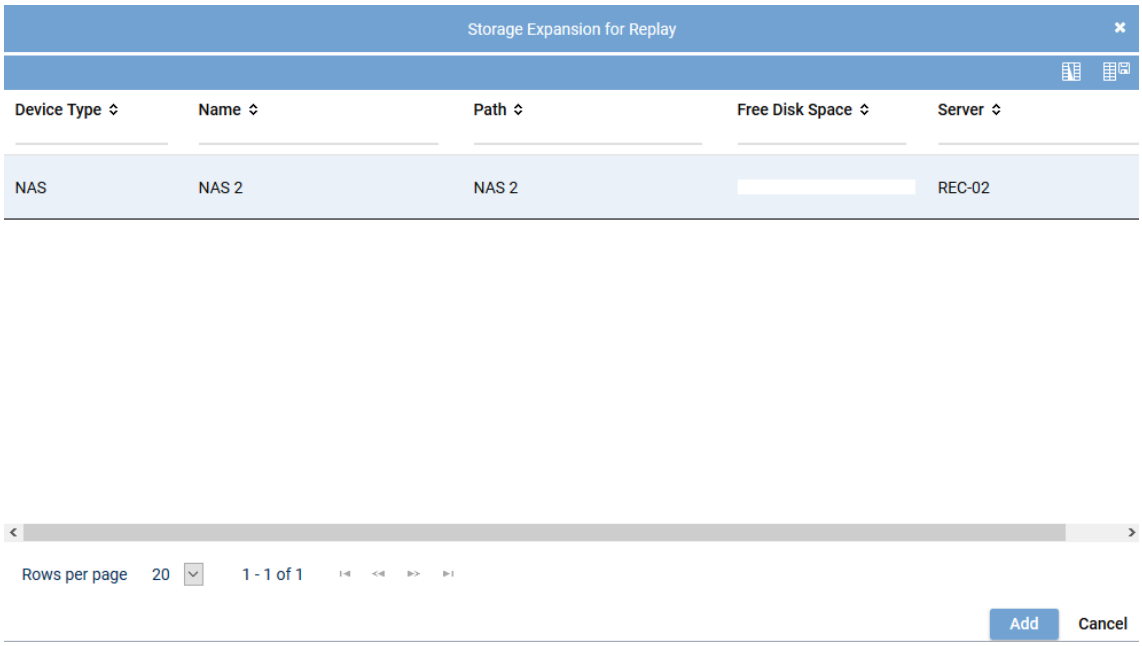

Fig. 20: Select storage expansion

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

Group field Audio analysis

Fig. 21: Group field Audio analysis

Parameter	Value/Description
Emotion detection	Activate this check box to activate emotion detection for audio analysis. ☑ = Function has been activated. Tenants can use the function emotion detection. ☐ = Function has not been activated.

Tab. 3: Configure audio analysis

Group field Recording Control/Key Management

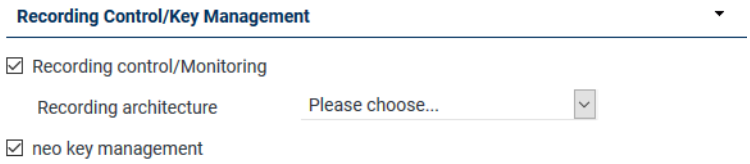

Fig. 22: Group field Recording Control/Key Management

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

Tab. 4: Configure recording control/key management

Group field Data Processing

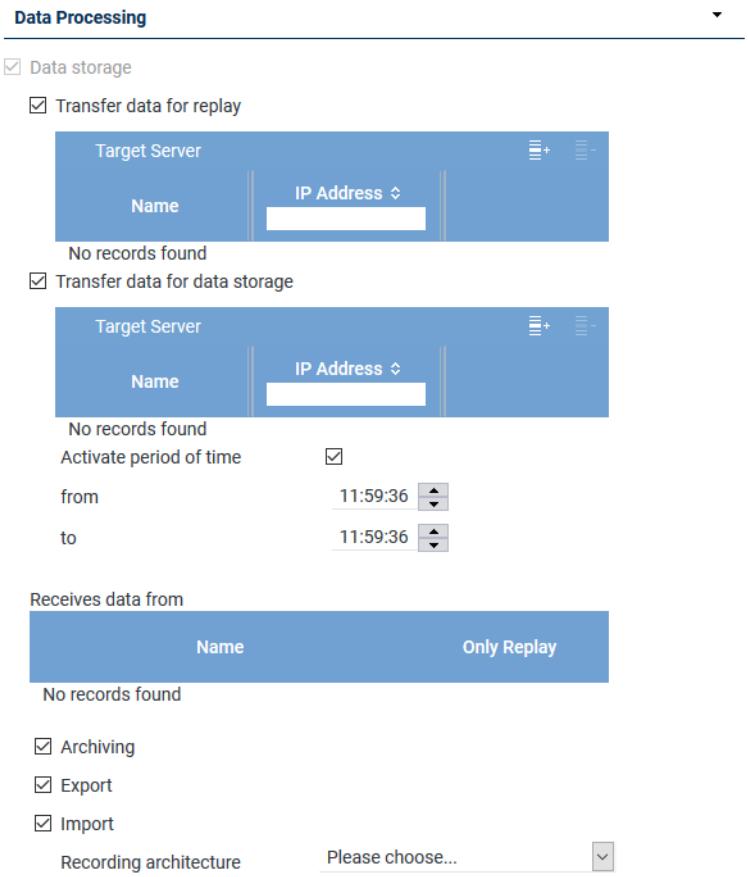

Fig. 23: Group field Data Processing

Parameter	Value/Description
Data storage	Activate the check box to allow the modification of the additional functions of data processing.
Transfer data for replay	Activate the check box if you would like to transfer data only for replay to another server. If the function has been activated, you can select a server from the list *Target Server* to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed. • By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 27. • By clicking on the icon *(Remove)*, you can remove the target server from the list. **NOTICE!** Only those servers are displayed on which an API server and a replay server have been configured.
Transfer data for data storage	Activate the check box if you would like to transfer data for storage to another server. If the function has been activated, you can select a server from the list *Target Server* to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function *Data Storage* has been activated. The data is copied to the target server and stored there.

Parameter	Value/Description
	• By clicking on the icon *(Add)*, you can add the target server, see chapter "Add target server to a list", p. 27. • By clicking on the icon *(Remove)*, you can remove the target server from the list. **NOTICE!** Only those servers are displayed on which the function *Data Storage* has been activated. If the function has been activated, you can activate the transfer for a certain period of time. • Activate period of time ☑ = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from − to. • Active period of time ☐ = Function has not been activated. **NOTICE!** In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.
Receives data from	This table contains those servers which transfer data to this server. In the column *Name*, the name of the server appears from which data has been transferred. In the column *Only Replay*, the purpose of the transfer is displayed: ✓ = Data is transferred only for replay. ✗ = Data is transferred for data storage.
Archiving	Activate the check box *Archiving* if you would like to use the server for archiving purposes.
Export	Activate the check box *Export* to allow the export from this server.
Import	Activate the check box *Import* so that the imported data can be stored on this server. • Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. **NOTICE!** If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.

Tab. 5: Configure data storage

Add target server to a list

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

Fig. 24: 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

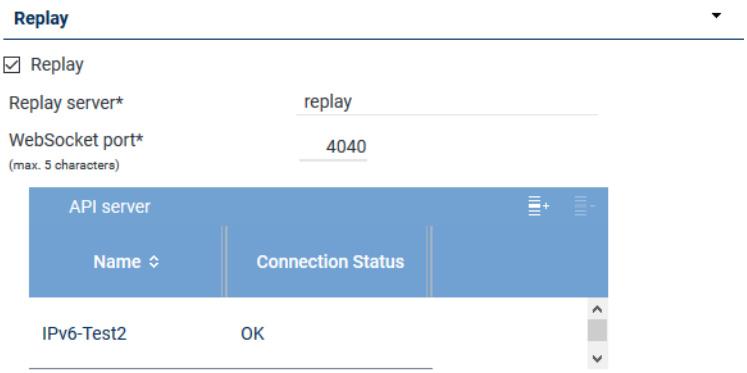

Fig. 25: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated *Replay Feature*. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes. Activate the check box *Replay* to be able to use the replay function of the players and the phones. ☑ = Function has been activated. You have to complete the entry field *Replay server*. ☐ = Function has not been activated.

Parameter	Value/Description
Replay server	If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field *Replay server*. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms. The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address. In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab *Replay Server Address Mapping*. For further details about the configuration refer to the administration manual *Configuration of servers and recording architectures*.
WebSocket port (maximum of 5 characters)	Enter the port via which the data to be replayed in POWER*play* Web are supposed to be transmitted.
List API server	Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here. If the function *Replay* has been activated, you can adjust the following settings: • By clicking on the icon *(Add)*, you can add the API server, see chapter "Add API server to a list", p. 29. • By clicking on the icon *(Remove)*, you can remove selected API servers from the list.

Tab. 6: Configure replay

Search and replay functions

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

Add API server to a list

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

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

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

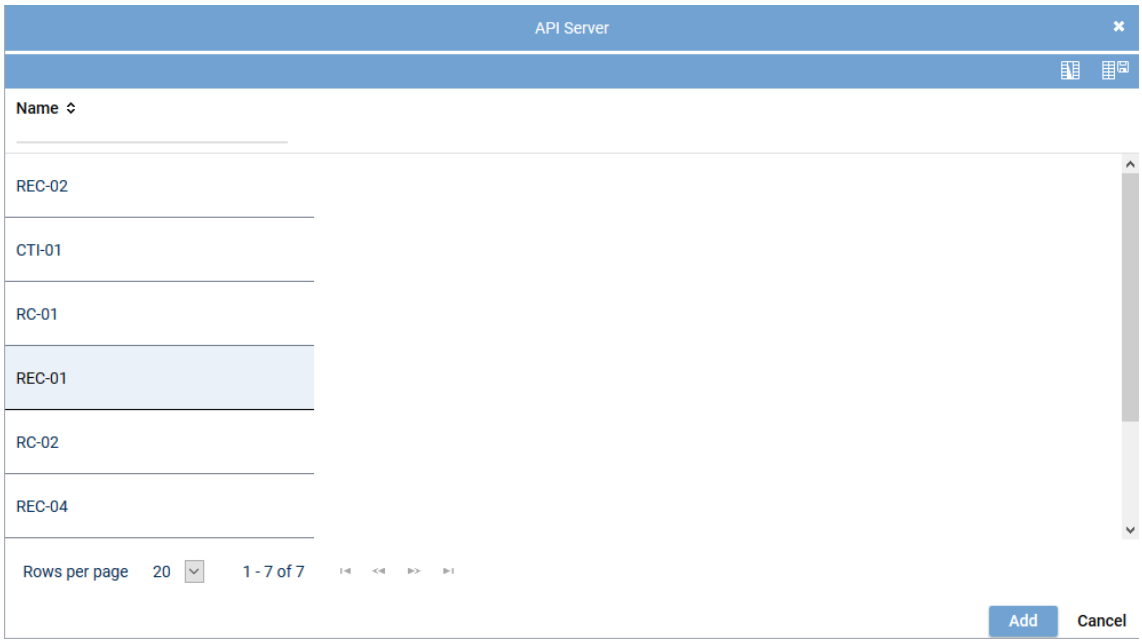

Fig. 26: Select server

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

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

Group field Virtualization

Fig. 27: Group field Virtualization

Parameter	Value/Description
VM support	Activate the check box *VM support* to be able to use the licensing for several VM installations. This function can only be activated if the system has been installed in a VMware and no *TRUSTED_VIRTUALIZATION* license has been imported to the system. When activating the function *VM support*, you have to configure the respective settings in the tab *Keystore/VM Licensing*. For further details about the configuration of this function refer to the administration manual *Configuration of servers and recording architectures*.

Tab. 7: Configure virtualization

For the *virtualization* without Internet connection, a dongle is required which contains the system information. The application *Dongle Manager*, required to read the dongle, has to be installed on the server that the dongle has been connected to.

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

Tab Media Streamer

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

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

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

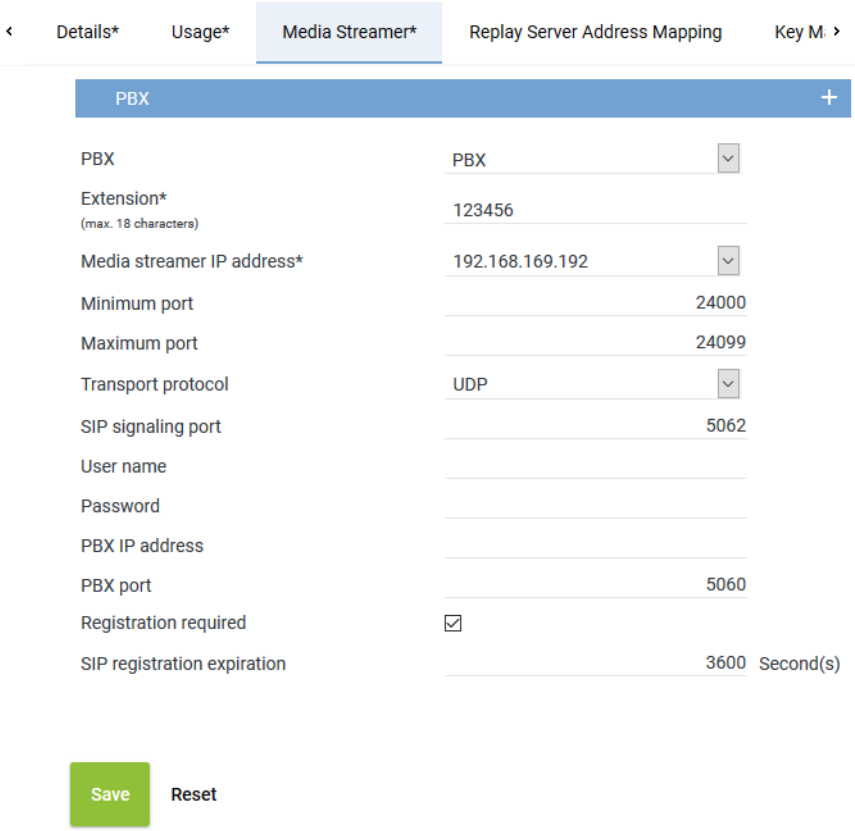

Fig. 28: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	PBX that the Media Streamer is supposed to be mapped to. Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system. If no PBX has been created in the system yet, you can create a PBX via the blue bar *PBX*, see chapter "Create PBX", p. 36.
Extension	Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing. If an external analog gateway has been integrated, enter the value *8000*.
Media streamer IP address	IP address which is supposed to be used for the exchange of the audio data and for the SIP communication. Select an IP address from the drop-down list. In the drop-down list, all IP addresses of the server are displayed. If an external analog gateway has been integrated, select the IP address *169.254.254.100* in the drop-down list.

Minimum port	Enter the minimum port which is supposed to be used for the audio data exchange.
Maximum port	Enter the maximum port which is supposed to be used for the audio data exchange. A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.
Transport protocol	Select the transport protocol type you would like to use for the SIP communication from the drop-down list. TCP = unencrypted UDP = unencrypted TLS = encrypted If an external analog gateway has been integrated, select *UDP* in the drop-down list.
SIP signaling port	Enter the port for the SIP communication. Port for data exchange: *5062*
User name	Enter the user name for the authentication on the SIP server.
Password	Enter the password for the authentication on the SIP server.
PBX IP address	Enter the IP address of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the IP address *169.254.254.101*.
PBX port	Enter the port of the SIP registrar of the PBX. If an external analog gateway has been integrated, enter the value *5060*.
Registration required	Select whether the SIP extension has to be registered with the SIP registrar of the PBX. ☑ = SIP extension has to be registered. ☐ = SIP extension does not have to be registered. If an external analog gateway has been integrated, deactivate the check box *Registration required*.
SIP registration expiration	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

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

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

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

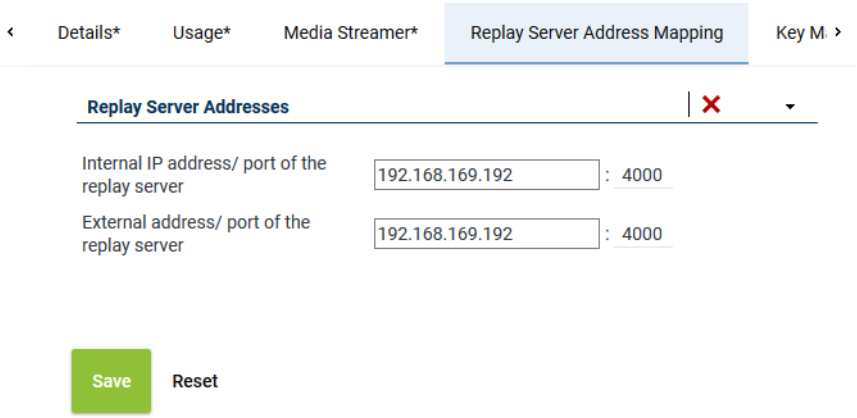

Fig. 29: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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

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

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

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

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

Tab Key Management

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

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

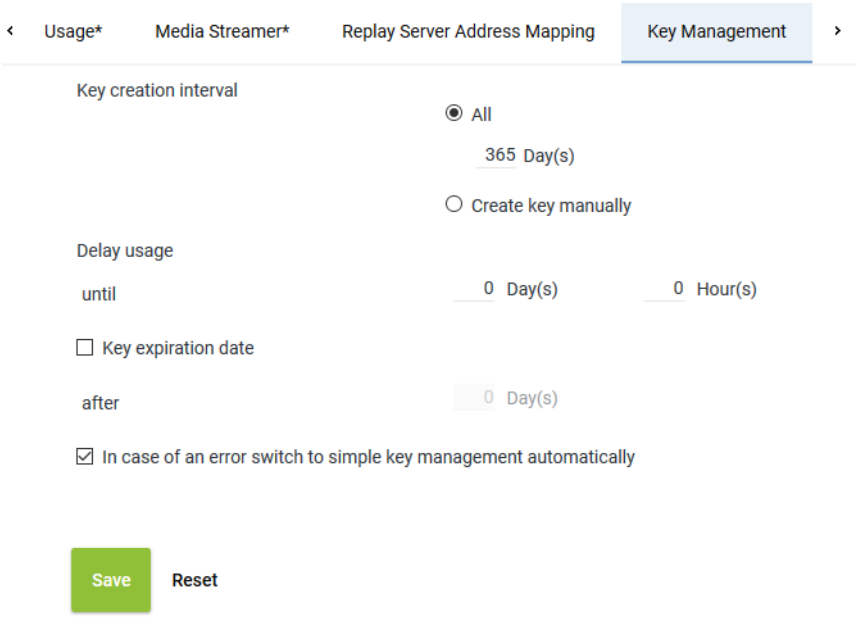

Fig. 30: Servers module - tab Key Management

Key creation interval	Select whether a key is supposed to be generated automatically or manually. Select one of the following options: • *All* Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days • *Create key manually* Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.
Delay usage	If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.
Key expiration date	Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here. ☐ = Key never becomes invalid. ☑ = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.

	CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.
In case of an error ... automatically	Select whether simple key management is supposed to be used if the *neo* key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the *neo* key management has been activated but does not work. ☑ = In case of an error, simple key management is used as replacement. ☐ = In case of an error, no recording takes place as long as the *neo* key management has been activated. In this case, disable key management in the tab *Usage*.

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

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

Tab Keystore/Virtualization

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

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

If your system has been installed in a virtual environment, the application Dongle Manager must have been installed and started locally outside the VM so that the access to the dongle works. The dongle must have been connected to the server on which the VM has been installed.

For detailed information about neo key management refer to the administration manual *Encryption of recordings*.

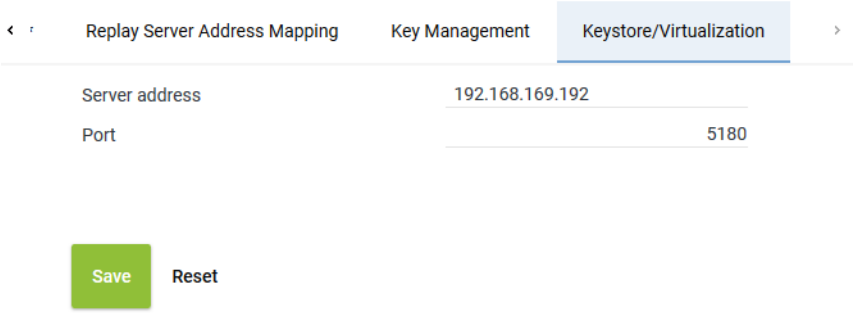

Fig. 31: Servers module - tab Keystore/Virtualization

Server address	Enter the address of the server for this connection. • If you use the neo key management as well as the virtualization: IP address of the server that the service *DongleMan* has been installed on. • If you use only virtualization, you can authenticate the VM via the ASC License Management System, too. In this case, enter the following address: *licensing.asc.de*

	• If you use only the ASC key management: IP address of the server with the master password database
Port	Enter the port for the connection. Default value: *5180*

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

7.1.2.1.3 Create PBX

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

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

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

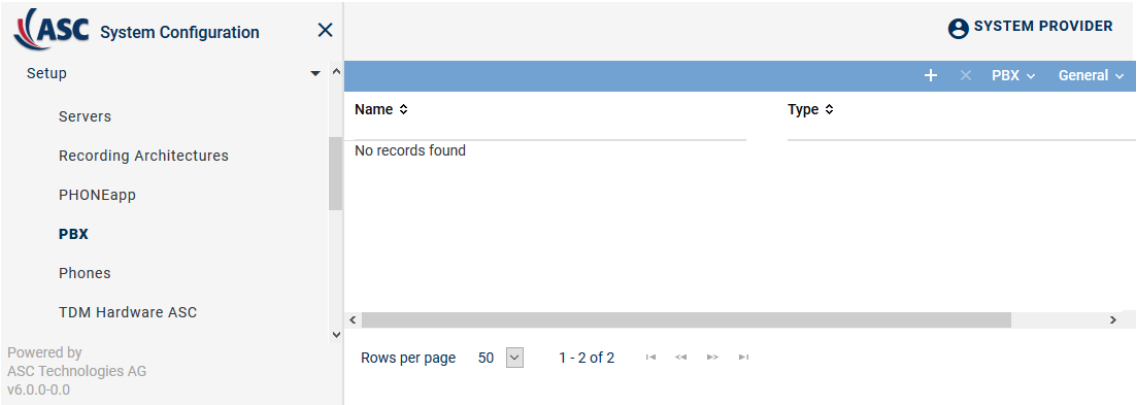

Fig. 32: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.

Fig. 33: Toolbar PBX module

+	*Create*	In the detail view, you can enter the parameters of the new PBX.
×	*Delete*	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
PBX	*Phone Configuration*	Opens a window in which you can create and configure phones.
	Administrate Unused Extensions	Opens a window in which you can delete extensions that are not used in any configuration.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • *Displayed information* • *Order of the displayed columns* • *Number of rows per page*

	Save Table Configuration	Saves the current table configuration of the main view as default view of the user.
	General Help	Opens the online help.
	Module Help	Opens the module-specific online help.

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

Create new PBX

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

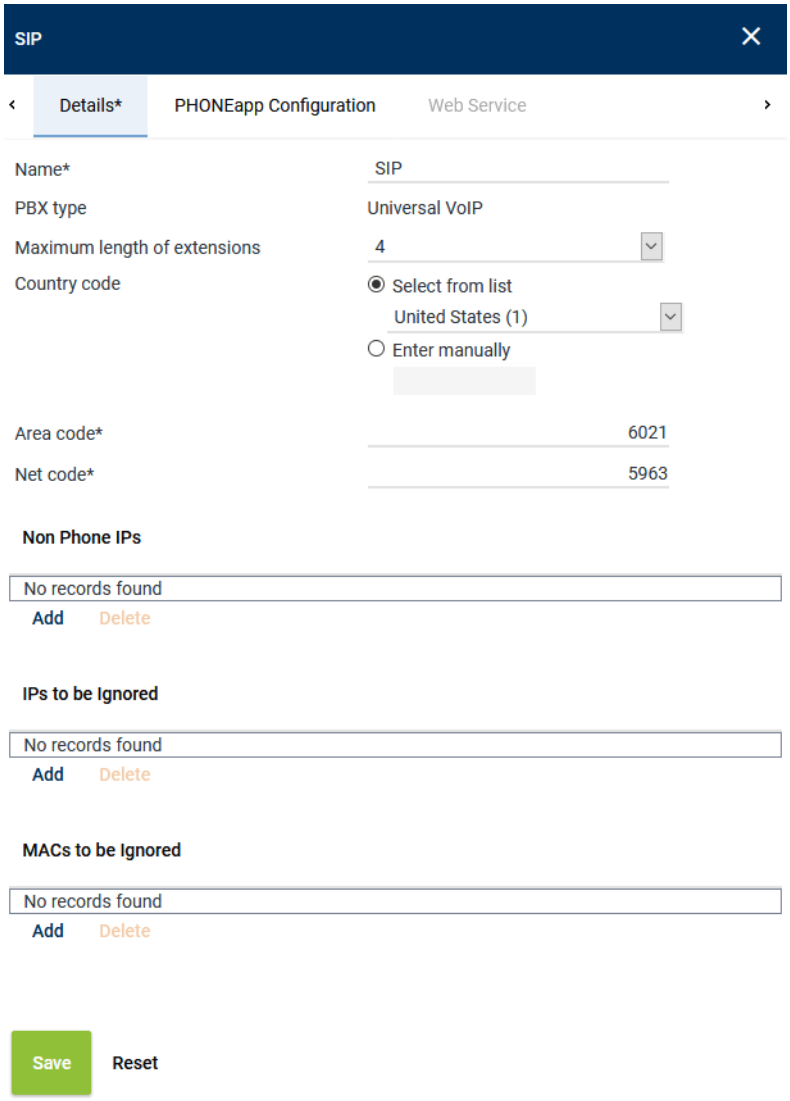

Fig. 34: Create new PBX - tab Details

2. Set the following parameters in the detail view:

Parameter	Value/Description
Name	This *name* serves as the identifier of this PBX.
PBX type	Select the type of the PBX from the drop-down list.
Maximum length of the extensions	Enter the number of digits of the extensions, e. g. *4*.
Country code	Select the option for the country code:

Parameter	Value/Description
	• *Select from list* Select the country code from the drop-down list. • *Enter manually* If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka *094*.
Area code	Enter the area code without the preceding *0*, e. g. *6021*.
Net code	Enter the net code, e. g. *5963*. Do not enter an extension here.

Tab. 8: Create PBX

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

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

Tab. 9: PBX parameters with complete phone number

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

7.1.2.1.4 Assign recording resources

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

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities.

Assign extensions to tenants

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

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

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

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

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

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

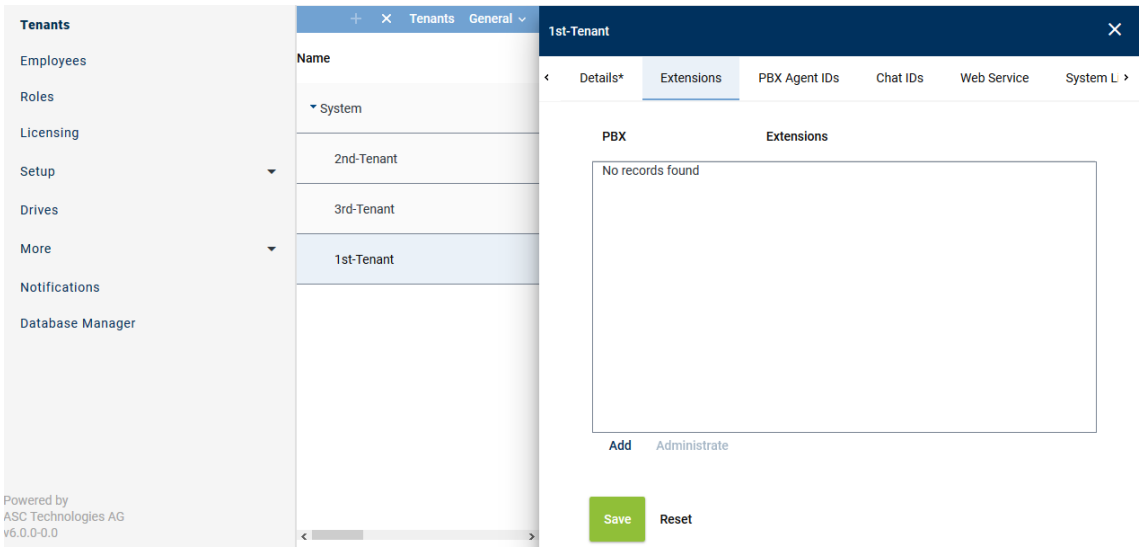

Fig. 35: Tenants - main view - tab Extensions

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:

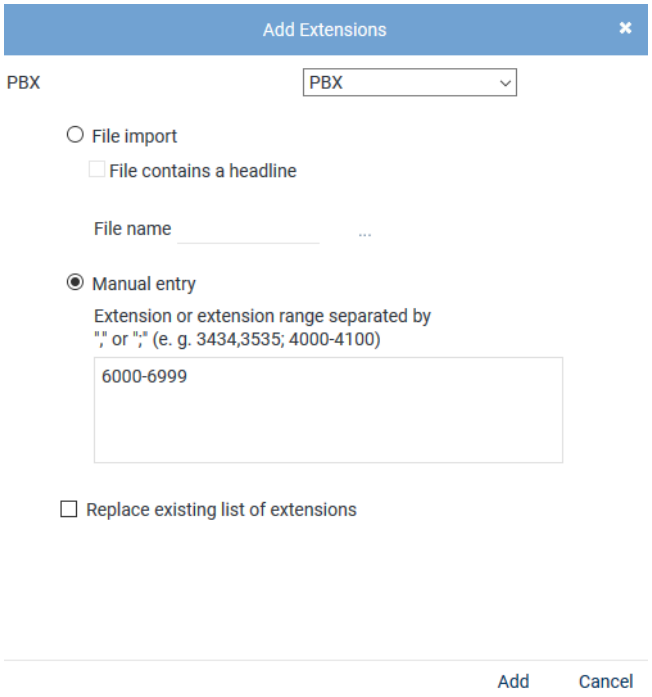

Fig. 36: Assign extensions to tenants

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

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT*

	• *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually. To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

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

Remove extensions

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

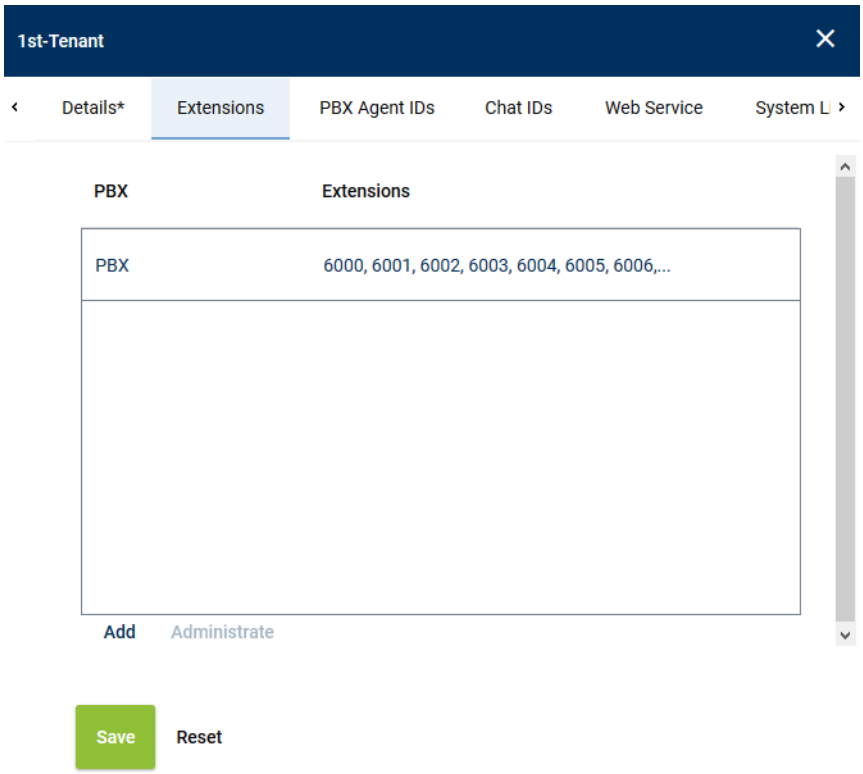

Fig. 37: Remove extensions

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

Fig. 38: Select extensions

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

Assign PBX Agent IDs to tenants

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

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

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

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

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

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

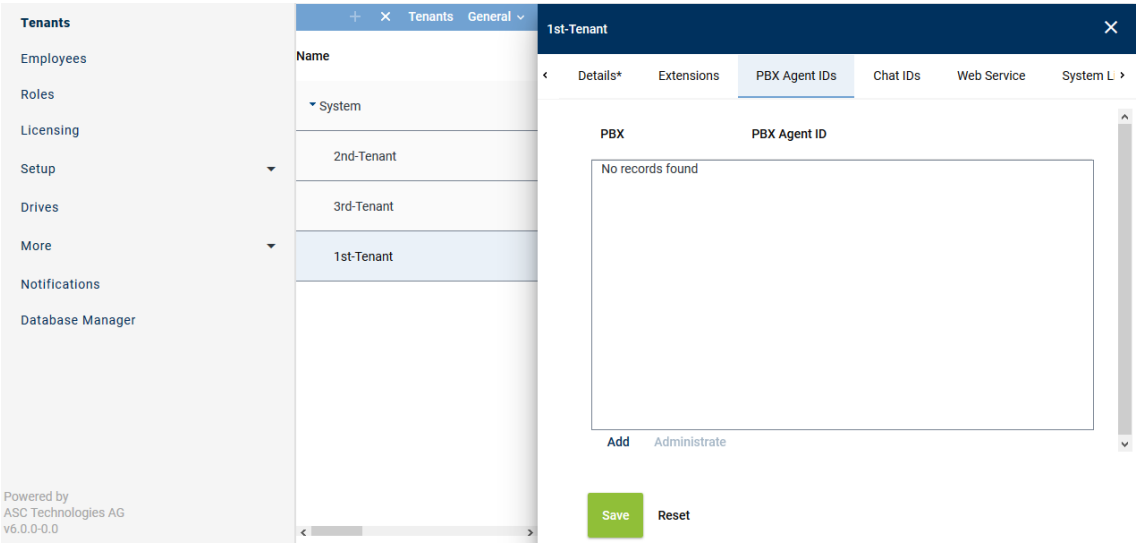

Fig. 39: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

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

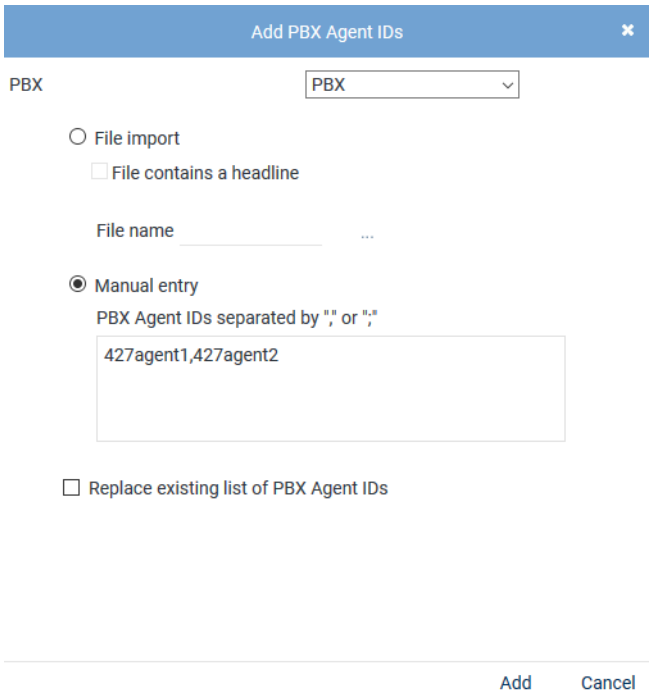

Fig. 40: Assign PBX Agent IDs to tenants

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

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

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

Remove PBX Agent ID

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

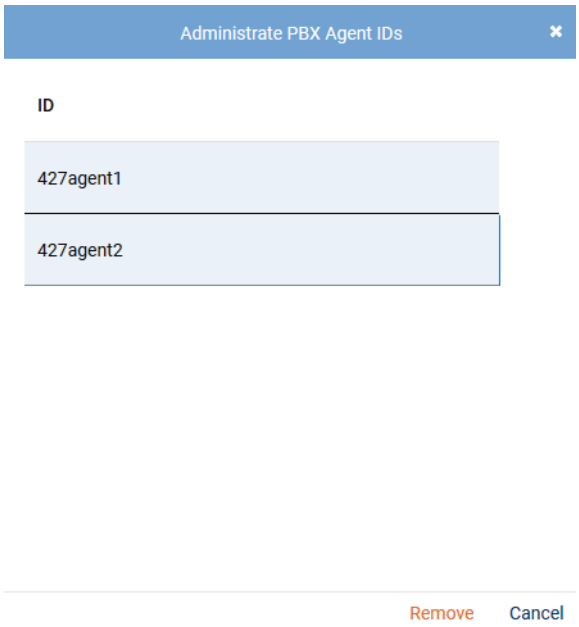

Fig. 41: Select PBX Agent IDs

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

Assign chat IDs to tenants

For chat recording, chat identifiers are used for the assignment. The assignment to the respective tenant can be done in the Tenants module.

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

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

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

The manual assignment of chat IDs is not possible until a chat system has been created in the PBX module since the assignment is PBX-related.

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

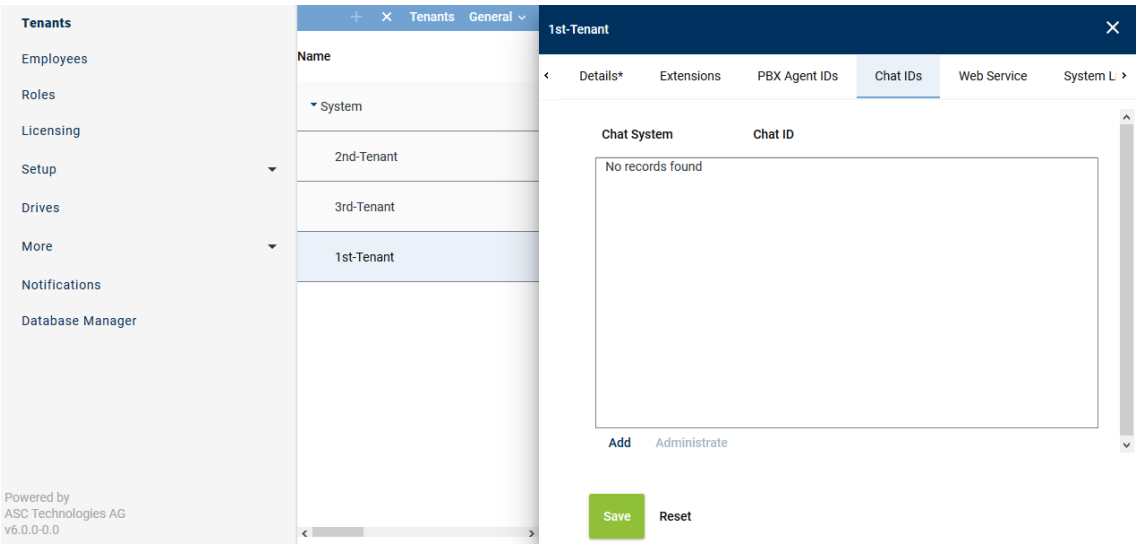

Fig. 42: Tenants - main view - tab Chat Identifier

Add chat ID

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

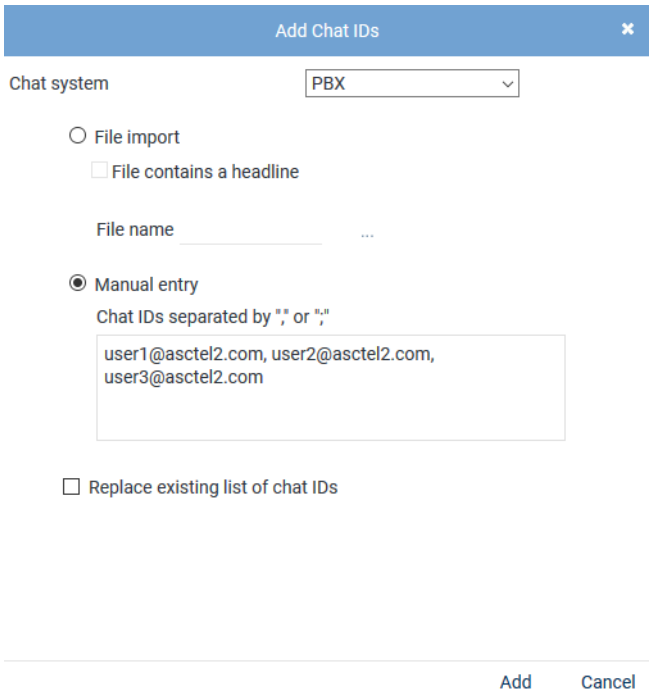

Fig. 43: Assign chat IDs to tenants

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

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

	Activate this option so that this structed is recognized correctly when importing the file. The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears. Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *(Upload file)*.
Manual entry	Select this option to enter chat IDs manually. You can separate the individual chat IDs by means of the delimiters displayed in the screenshot. The chat address must be identical to the entries in the Agent data in the Employees module and must contain the name of the corresponding domain. The configuration must be identical to the entries in the Skype for Business Monitor. **NOTICE! Wildcards cannot be used!**
Replace existing list of chat IDs	Activate the check box to overwrite existing chat IDs.

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

Remove chat ID

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

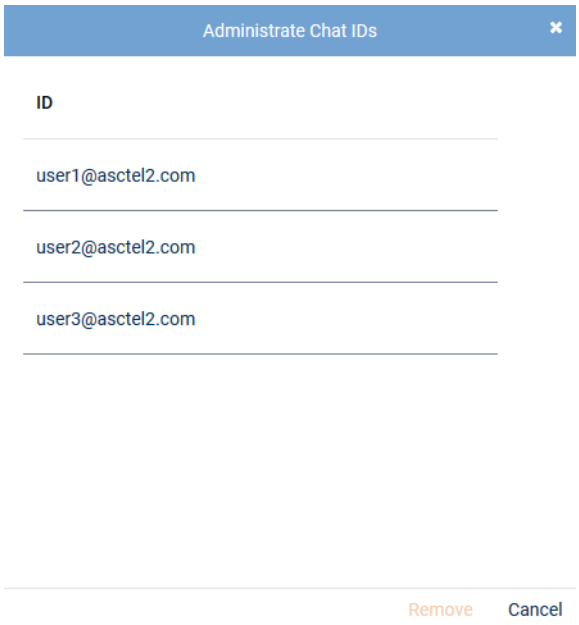

Fig. 44: Select chat IDs

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

7.1.2.1.5 Create integration for All-in-one Basic

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

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

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

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

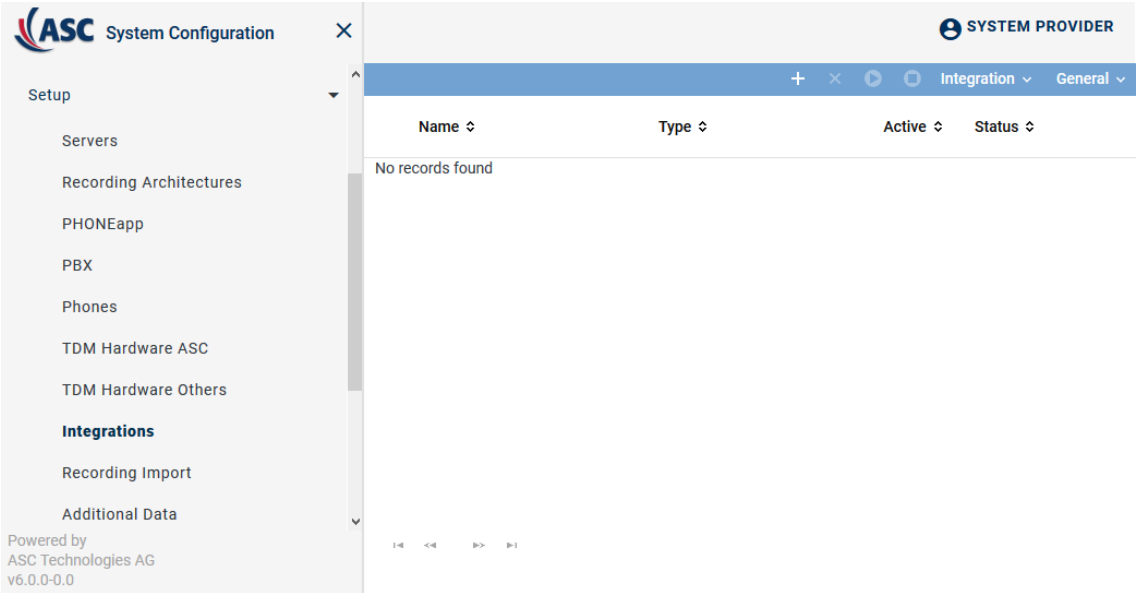

Fig. 45: Integrations - main view

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

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

Toolbar of the Integrations module

The toolbar offers the following functions.

Fig. 46: Toolbar Integrations module

+	*Create*	Opens the detail view so that you can create a new integration.
×	*Delete*	Deletes the selected integration. The integration can only be deleted if it has been deactivates.
	Activate	Activates the selected integration. The integration can only be activated if it has been configured completely.
	Deactivate	Deactivates the selected integration. This stops running recordings.
Integration	*Import Grammar*	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
General	*General Help*	Opens the online help.
	Module Help	Opens the module-specific online help.

Assign integration type

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

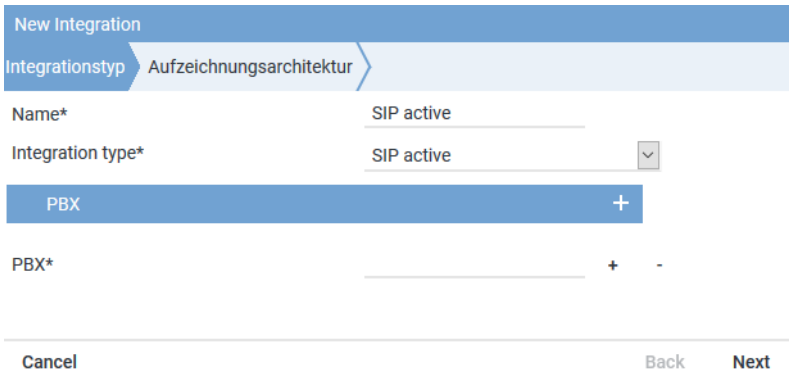

Fig. 47: Create integration type

2. Enter the following parameters:

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

Tab. 10: Create integration type

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

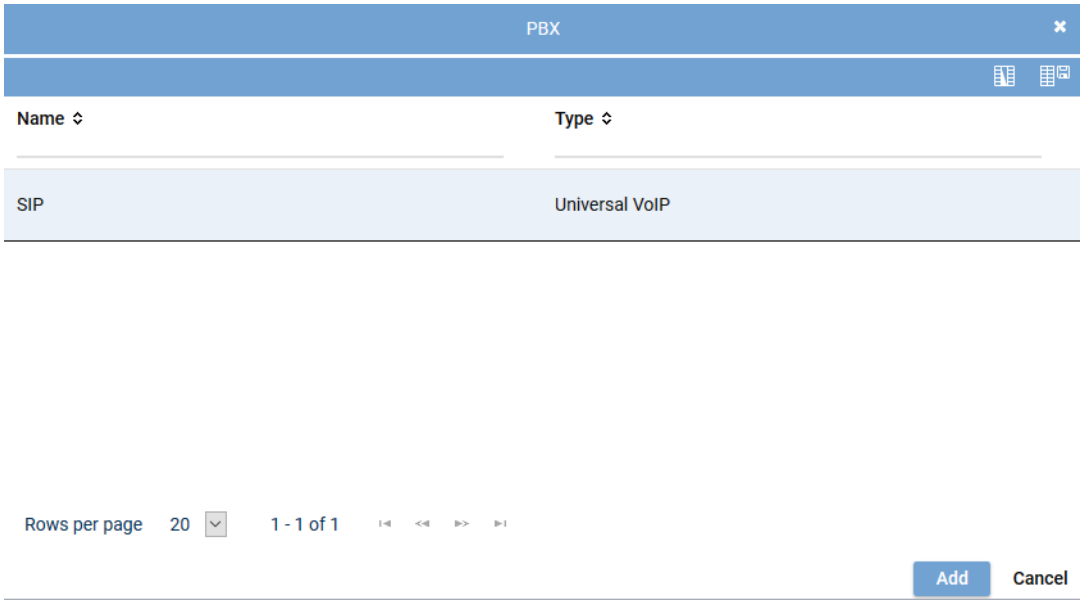

Fig. 48: Select PBX

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

Assign recording architecture for All-in-one Basic

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

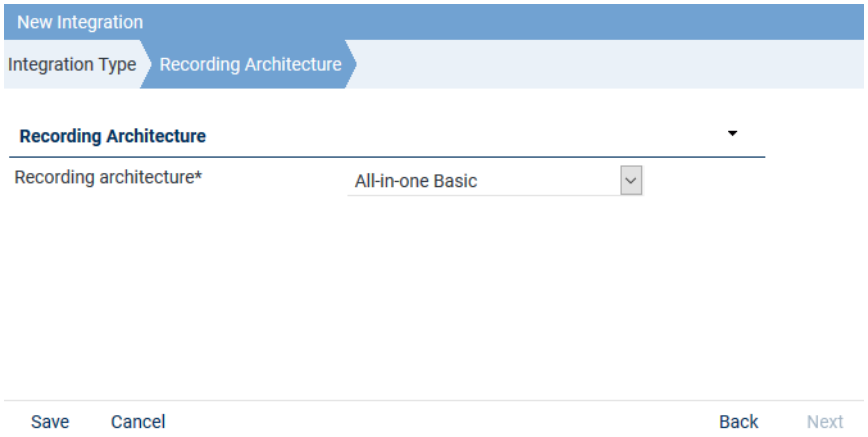

Fig. 49: Assign recording architecture - All-in-one Basic

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

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

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

Configuration steps

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

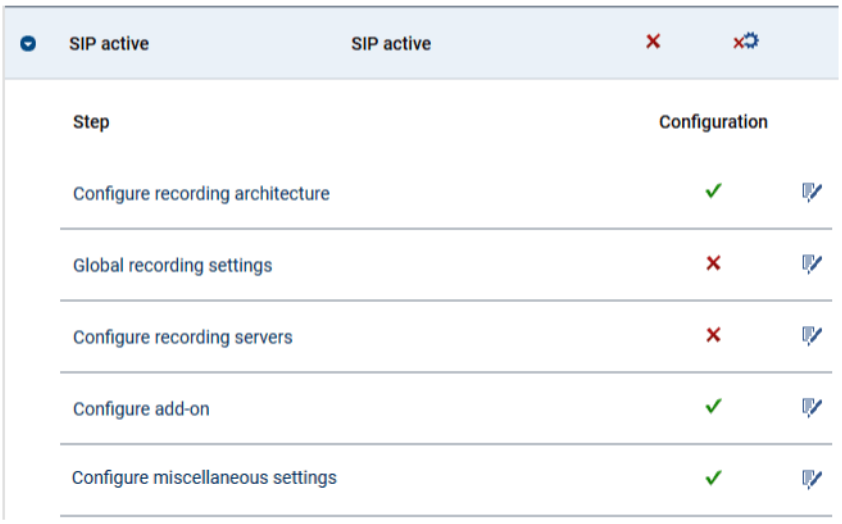

Fig. 50: Configuration steps of the integration

Configure recording architecture

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

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

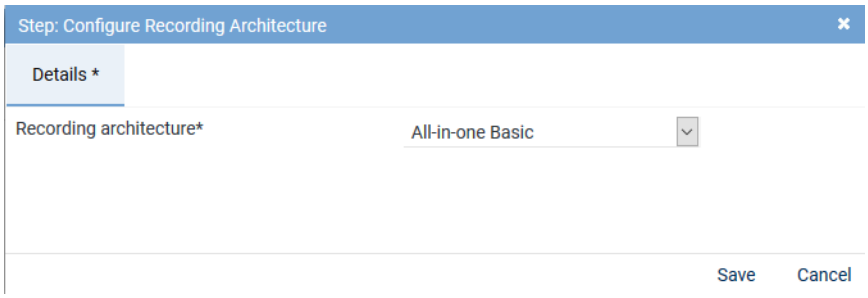

Fig. 51: Configuration step - Configure Recording Architecture

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

Global recording settings for All-in-one Basic

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

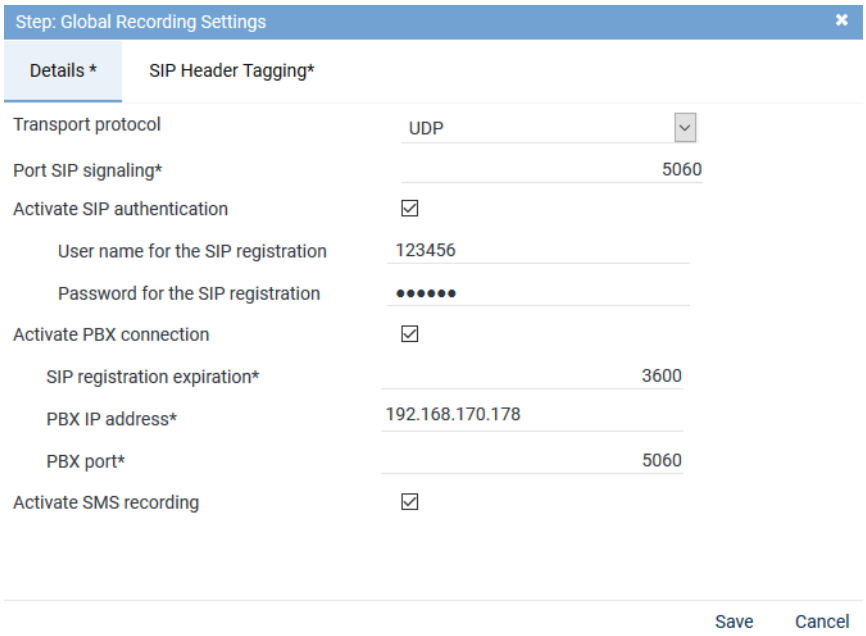

Fig. 52: Configuration step - Global Recording Settings

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

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

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

Tab. 11: Global recording settings

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

Tab SIP Header Tagging

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

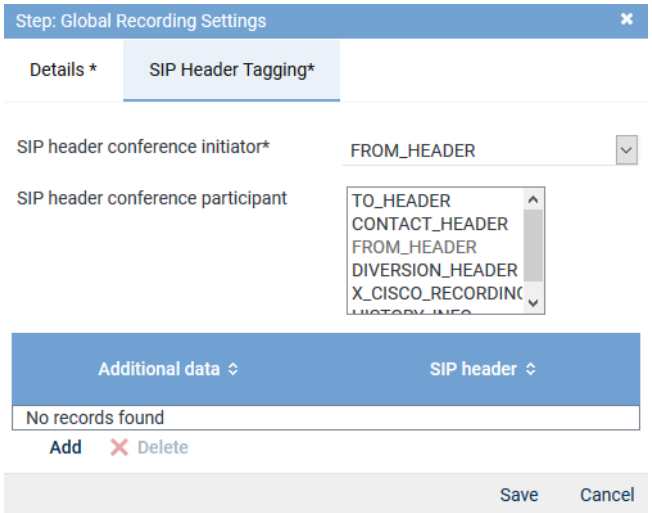

Fig. 53: Tab SIP Header Tagging Configure sources

2. Enter the following parameters:

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

Tab. 12: Configure SIP header tagging

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

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

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

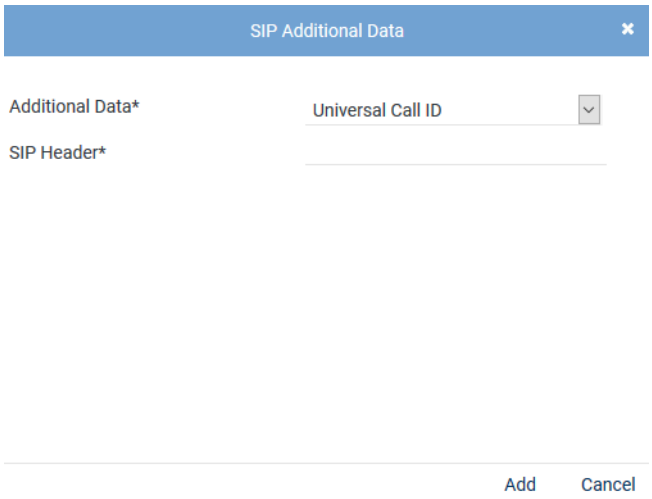

Fig. 54: SIP Additional Data

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

4. Enter the following parameters:

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

Tab. 13: Configure SIP conversation parameters

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

Configure recording server for All-in-one Basic

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

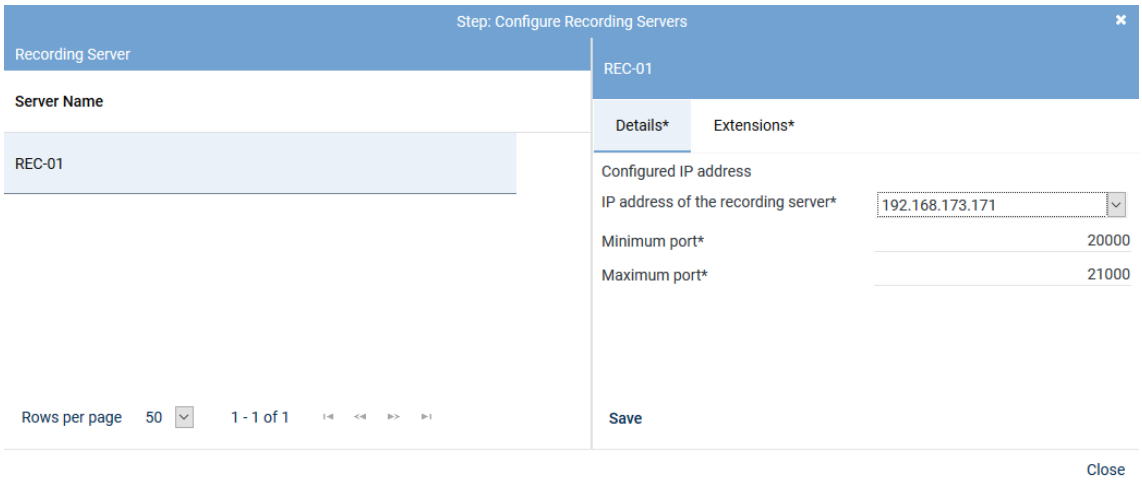

Fig. 55: Configuration step - Configure recording servers

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

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

Tab. 14: Configure recording servers

ⓘ This recording solutions allows recording data streams in stereo. For stereo recording, reckon with 4 ports as only even ports are used to receive RTP.

Stereo recording requires more storage space, too.

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

Tab Extensions

1. Click on the tab *Extensions*.

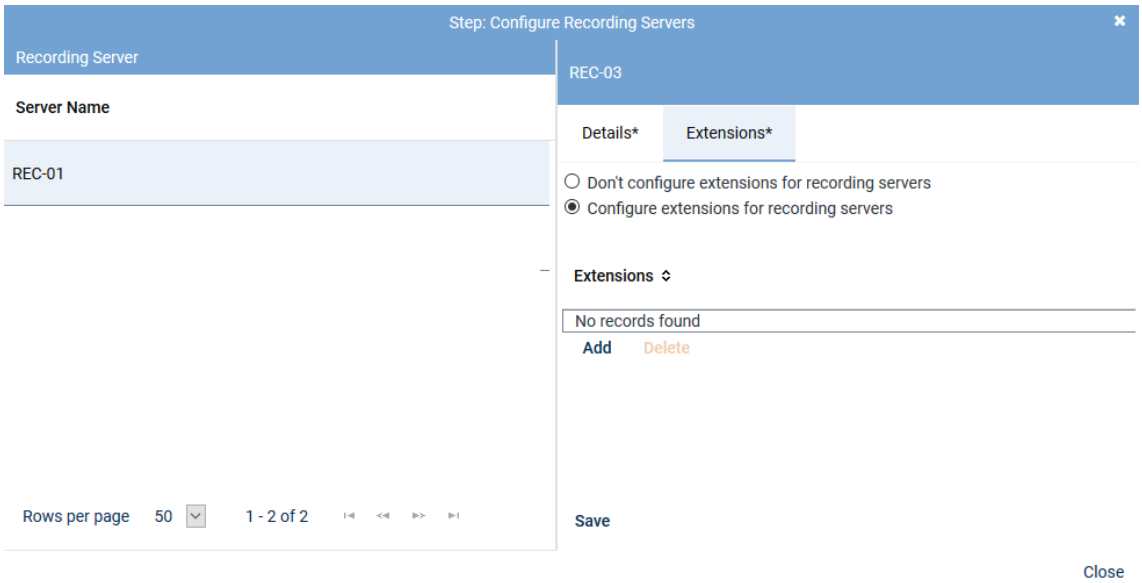

Fig. 56: Tab Extensions

The following options are available:

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

2. To add extensions, click on the button *Add* in the table *Extensions*.

   ⇨ The window *Add Extensions* appears.

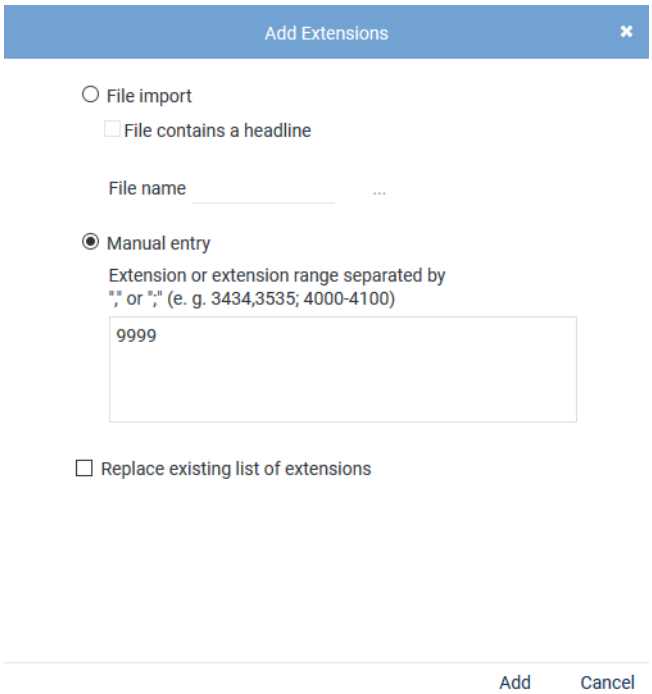

Fig. 57: Add extensions

3. In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.
4. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
5. If errors have been detect, the window *Result* appears.
   Click on the button *Display Error Report* to open the window *Error Report*.
   To close the window *Error Report*, click on the button *Close*.
   To close the window *Result*, click on the button *Close*.
6. The configured extensions now appear in the detail view.

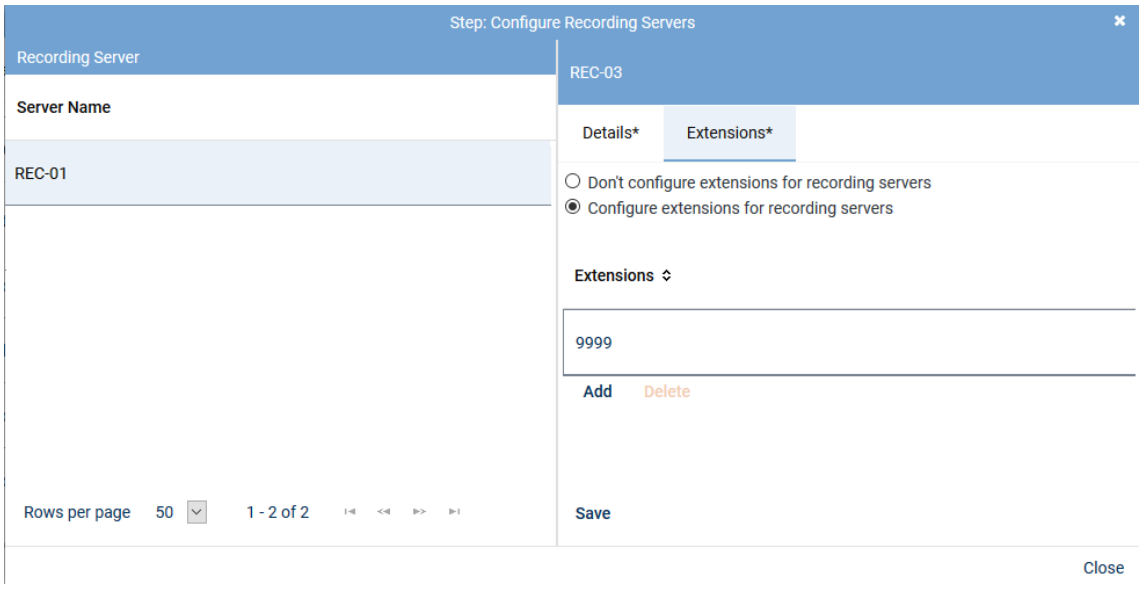

Fig. 58: Added extensions

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

Configure add-on

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

Add-ons are not supported in this recording solution.

Configure miscellaneous settings

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

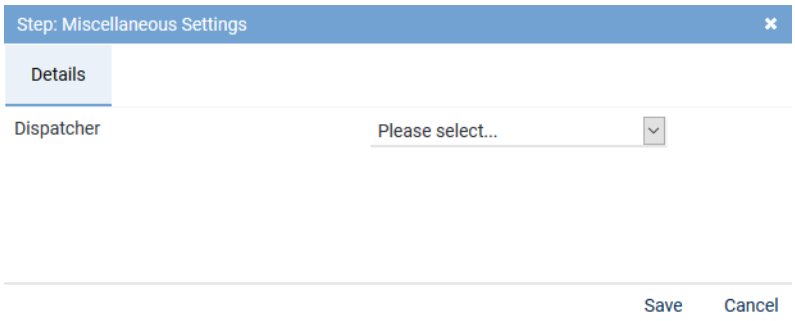

Fig. 59: Configure miscellaneous settings

2. Enter the following parameter:

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

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

Activate integration

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

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

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

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

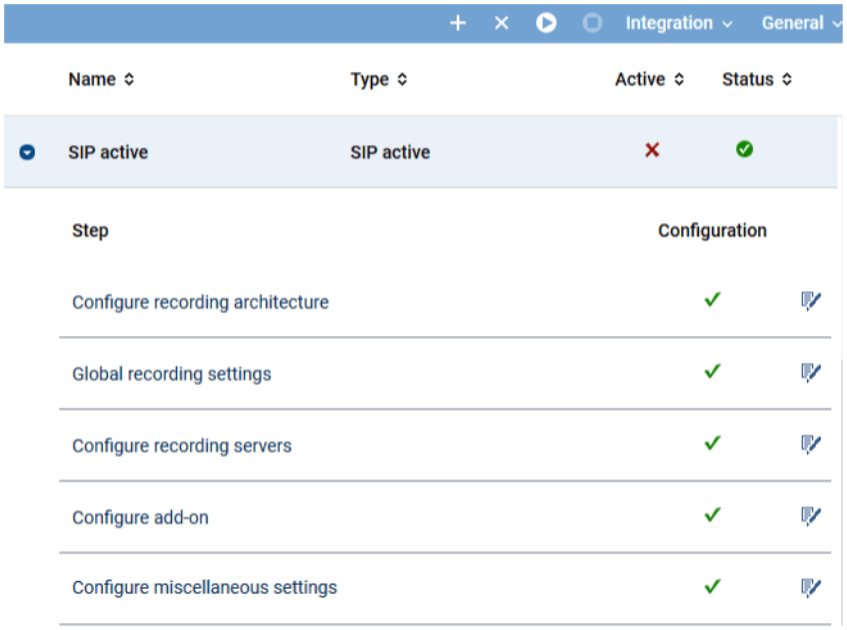

Fig. 60: Activate integration

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

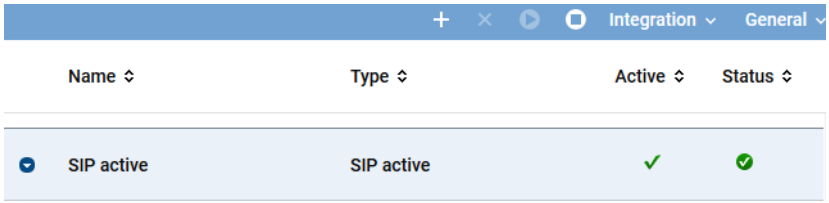

Fig. 61: Activated integration

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

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

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

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

Deactivate/Delete integration

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

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

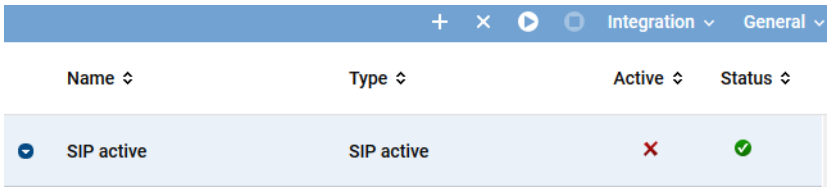

Fig. 62: Deactivate integration

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

7.1.2.1.6 Additional configuration steps for video recording

Configure employees

To be able to record the video conversations of agents, you have to configure the respective employees as agents in the Employees module and configure their *extension* or their *PBX Agent ID* in the agent data in the group field *Telephony* as well as activate the option *Video recording* in the group field *Miscellaneous Settings*.

1. Log in to the application System Configuration as *1st-tenant-admin*.

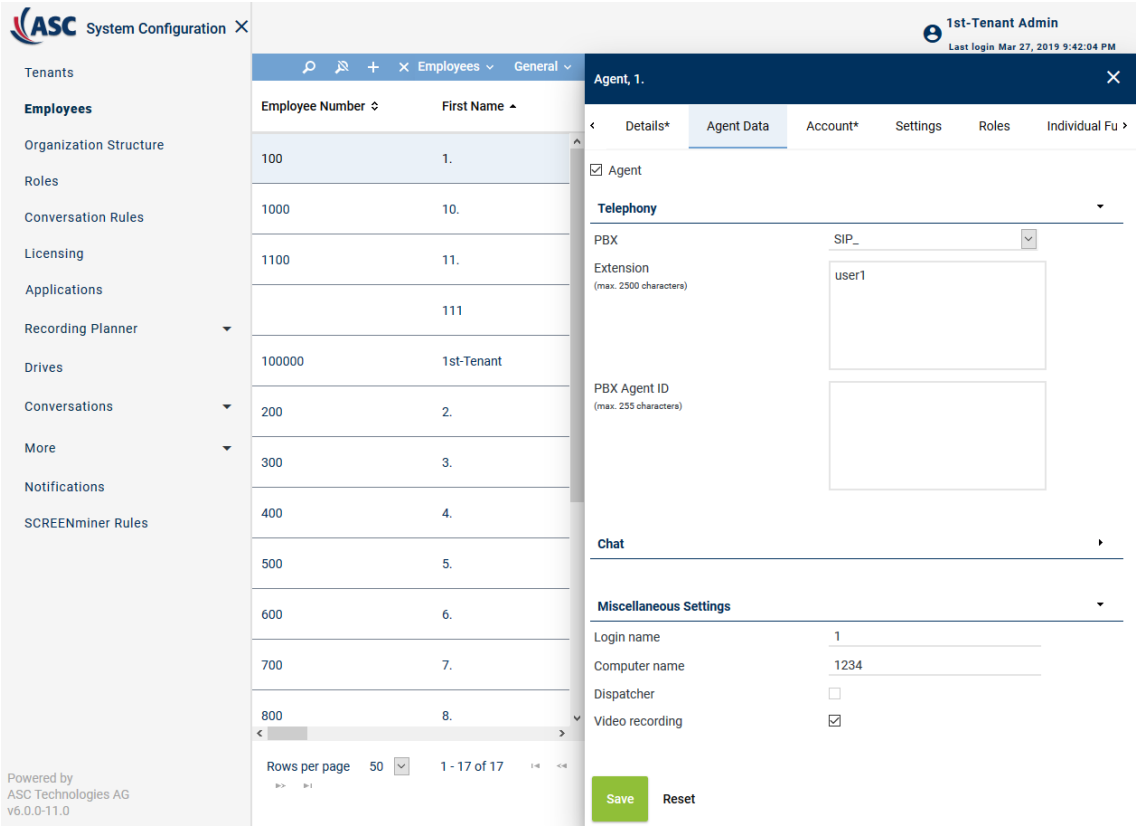

Fig. 63: Main view Employees

2. Click on the tab *Agent Data*.

Group field Telephony

1. Enter the following parameters:

PBX	Enter the name of the PBX in which the extensions has been configured.
Extension	Enter the extension if an extension has been configured in the PBX.
PBX Agent ID	Enter the PBX Agent ID if it has been configured in the PBX for this purpose.

Group field Miscellaneous Settings

1. Enter the agent's data.

User name	Enter the user name that has been configured for this agent.
Computer name	Enter the computer name that has been configured for this agent.
Video recording	Activate the check box so that the video conversations can be recorded.

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

Configure Recording Planner

To be able to record the video conversations, you have to configure the Recording Planner module.

1. Log in to the application System Configuration as *1st-tenant-admin*.

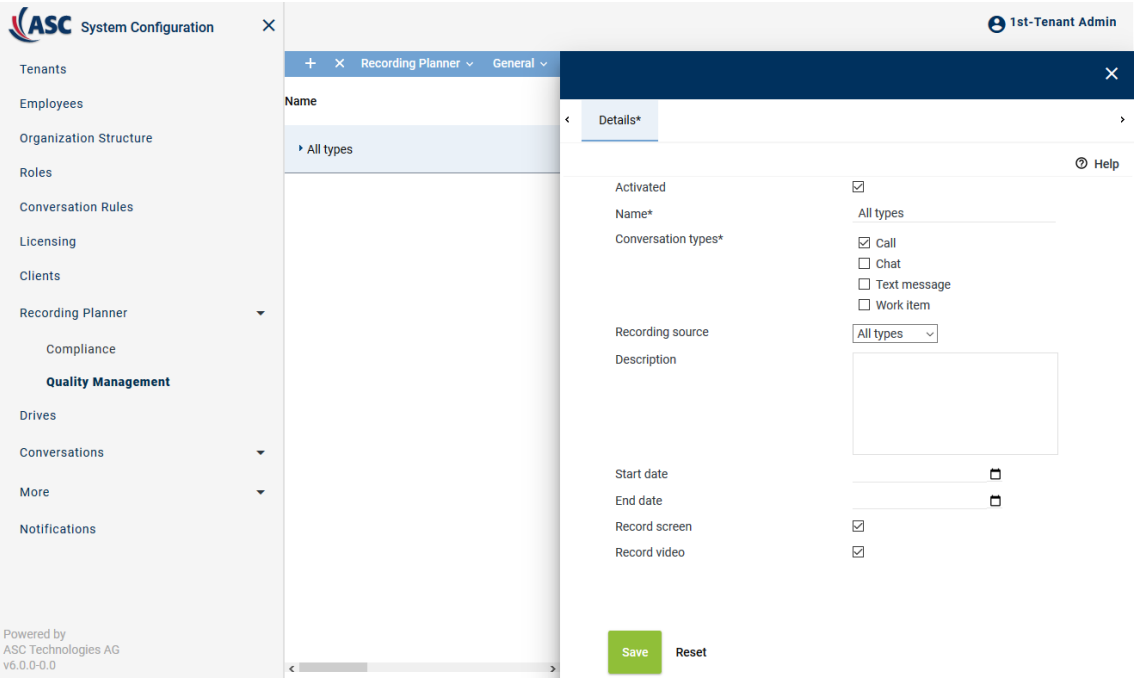

Fig. 64: Main view Recording Planner

2. Activate the following options for video recording:

Conversation types	Activate the following option so that video conversations can be recorded.
	☑ *Call*

Record screen	Activate the option so that video conversations can be recorded. This option is activated automatically upon activating the conversation type *Call*.
Record video	Activate the option so that video conversations can be recorded. This option is activated automatically upon activating the conversation type *Call*.

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

List of figures

Fig. 1 Overview of the recording solution ... 5
Fig. 2 System Configuration - web interface ... 11
Fig. 3 System Configuration - main view: ... 12
Fig. 4 Recording architectures - main view ... 13
Fig. 5 Toolbar Recording Architectures module ... 13
Fig. 6 Create recording architecture - All-in-one Basic Recording ... 15
Fig. 7 Recording architecture - tab Details ... 15
Fig. 8 Select integration type ... 16
Fig. 9 Recording architecture - tab Server Assignment ... 16
Fig. 10 Recording architecture - assign server ... 17
Fig. 11 Recording architecture - activate recording variant ... 17
Fig. 12 Recording architecture - activate recording architecture ... 18
Fig. 13 Servers - main view ... 18
Fig. 14 Toolbar Servers module ... 19
Fig. 15 Add server locations ... 20
Fig. 16 Delete server location ... 21
Fig. 17 Servers - tab Details ... 21
Fig. 18 Servers - tab usage ... 22
Fig. 19 Group field API Server ... 22
Fig. 20 Select storage expansion ... 24
Fig. 21 Group field Audio analysis ... 24
Fig. 22 Group field Recording Control/Key Management ... 25
Fig. 23 Group field Data Processing ... 26
Fig. 24 Select server ... 28
Fig. 25 Group field Replay ... 28
Fig. 26 Select server ... 30
Fig. 27 Group field Virtualization ... 30
Fig. 28 Servers module - tab Media Streamer ... 31
Fig. 29 Servers Module - tab Replay Server Address Mapping ... 33
Fig. 30 Servers module - tab Key Management ... 34
Fig. 31 Servers module - tab Keystore/Virtualization ... 35
Fig. 32 Create new PBX ... 36
Fig. 33 Toolbar PBX module ... 36
Fig. 34 Create new PBX - tab Details ... 37
Fig. 35 Tenants - main view - tab Extensions ... 39
Fig. 36 Assign extensions to tenants ... 39
Fig. 37 Remove extensions ... 41
Fig. 38 Select extensions ... 41
Fig. 39 Tenants - main view - tab PBX Agent ID ... 42
Fig. 40 Assign PBX Agent IDs to tenants ... 43
Fig. 41 Select PBX Agent IDs ... 44

Fig. 42 Tenants - main view - tab Chat Identifier 45
Fig. 43 Assign chat IDs to tenants 45
Fig. 44 Select chat IDs 47
Fig. 45 Integrations - main view 47
Fig. 46 Toolbar Integrations module 48
Fig. 47 Create integration type 48
Fig. 48 Select PBX 49
Fig. 49 Assign recording architecture - All-in-one Basic 49
Fig. 50 Configuration steps of the integration 50
Fig. 51 Configuration step - Configure Recording Architecture 50
Fig. 52 Configuration step - Global Recording Settings 51
Fig. 53 Tab SIP Header Tagging Configure sources 52
Fig. 54 SIP Additional Data 53
Fig. 55 Configuration step - Configure recording servers 53
Fig. 56 Tab Extensions 54
Fig. 57 Add extensions 55
Fig. 58 Added extensions 55
Fig. 59 Configure miscellaneous settings 56
Fig. 60 Activate integration 57
Fig. 61 Activated integration 57
Fig. 62 Deactivate integration 58
Fig. 63 Main view Employees 58
Fig. 64 Main view Recording Planner 59

List of tables

Tab. 1 Licenses of ASC 8
Tab. 2 Login data - system provider 11
Tab. 3 Configure audio analysis 24
Tab. 4 Configure recording control/key management 25
Tab. 5 Configure data storage 26
Tab. 6 Configure replay 28
Tab. 7 Configure virtualization 30
Tab. 8 Create PBX 37
Tab. 9 PBX parameters with complete phone number 38
Tab. 10 Create integration type 49
Tab. 11 Global recording settings 51
Tab. 12 Configure SIP header tagging 52
Tab. 13 Configure SIP conversation parameters 53
Tab. 14 Configure recording servers 54

Glossary

API

Application Programming Interface

API server

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

CSV

Comma-separated values is a file format which stores tabular data in plain text form.

Digest Authentication

In Digest Access Authentication (also RFC 2617) the server sends a random string of characters (nonce) created specifically for this purpose along with the WWW-Authenticate-Header. The browser calculates the hashcode (usually MD5) of a combination of user name, password, contained string of characters, HTTP method, and requested URI. It sends it back to the server in the authentication header along with the user name and the random string of characters. The server then calculates the hash total for comparison purposes. This method resembles Message Authentication Code. Provided that the used hash function is safe in terms of the cryptographic construction, attackers do not profit from sniffing the communication since the hash function prevents a reconstruction of the access data and because the access data are different for the next request due to using a nonce. (Especially the widespread hash function MD5 is not considered safe anymore.) The remaining data transmission is not protected, though. To achieve this Hypertext Transfer Protocol Secure (HTTPS) can be used. Translation of the German-language source: Wikipedia (20/02/2017)

DTMF

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

IP

Internet Protocol, basic protocol for Internet communication

LCR

Last Conversation Repeat

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.

SDES

Session Description Protocol Security Descriptions

SDP

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

SIP

Session Initiation Protocol

SMS

Short Message Service, text message (GSM, landline)

SRTP

Secure real-time protocol

TCP

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

TDM

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

TLS

Transport Layer Security; previously known as Secure Sockets Layer (SSL), is a hybrid encryption protocol for safe data transmission in the Internet. Since version 3.0, the SSL protocol is developed under the new name TLS.

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)

VAD

Voice Activity Detection or silence suppression

VM

Virtual machine

VoIP

Voice over IP