

EVOIPneo active for Mitel MiVoice MX-ONE (CSTA3)



Administration manual for system providers

5/12/2020

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (country-specific)

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

Copyright © 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.

Contents

1	General information	5
2	Introduction	6
3	System requirements.....	9
3.1	Hardware components	9
3.1.1	Recorder	9
3.2	Software components	9
3.2.1	Mitel MiVoice MX-ONE software components	9
3.3	Genesys system components (optional)	9
3.3.1	Genesys Framework	9
4	Installation requirements	10
4.1	Licenses	10
4.2	Information	11
5	Overview install and configure product.....	12
6	Installation	13
7	Configuration.....	14
7.1	Configure Mitel MiVoice MX-ONE CSTA 3	14
7.1.1	Configure CSTA server	14
7.1.2	Configure extension monitor points.....	15
7.1.3	Check functionality	16
7.2	Configure Mitel Border Gateway	19
7.2.1	Install certificate on the MBG	19
7.3	System Configuration	21
7.3.1	Start application	22
7.3.2	Configure recording solution	23
7.3.2.1	Configure recording solution All-in-one Basic	23
7.3.2.2	Configure recording solution All-in-one Failover	84
7.3.2.3	Configure recording solution Multi-Server Recording	149
7.3.2.4	Configure recording solution Multi-Server Failover	214
7.3.2.5	Synchronization options	280
7.3.2.6	Standby management for failover architectures.....	284
7.3.3	Software update	287
7.3.4	Configure XML PHONEapp	288
7.3.4.1	Configure key control	288
7.3.4.2	Configure Servers module	289
7.3.4.3	Configure PHONEapp.....	290
7.3.4.4	Configure PBX module.....	298
7.3.4.5	Configure Phones module.....	299
7.3.4.6	Configure Recording Planner module	300

7.3.5	Import InAttend conversation to neo	301
7.3.5.1	Configure import job	301
7.3.5.2	Replaying conversations in POWERplay Web.....	311
7.4	Configure CTIconnect add-on	311
7.4.1	Configure Genesys T-Server (optional)	311
7.4.1.1	Configure IP address and port of the Genesys T-Server	311
7.4.1.2	Configure IP address and port of the Genesys Configuration Server	312
7.4.1.3	Configure switch instance in the Genesys Configuration Server	313
7.4.1.4	Create users for the Genesys Configuration Server	314
8	Troubleshooting.....	316
	List of figures	317
	List of tables	327
	Glossary	329

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.

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



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

The recording solution EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA 3) provides the functionality which is necessary for an active recording of audio and additional data in connection with a Mitel MiVoice MX-ONE PBX.

For the communication between the recording server and the PBX, the protocol "CSTA Phase III" is used via **TCP/TLS** (ECMA-269, ECMA-323). The signaling provides the information about the conversation participants as well as other additional information and controls the streaming of the conversation data to the recording server.

Based on the criteria configured in the Recording Planner, the Recording Control service makes a recording decision. The EVOIP_{neo} recording service records the corresponding conversation data and saves them on the recording server.

The **CSTA** connection can be established via a secured, encrypted **TLS** connection.

By using the add-on MiContact Center Enterprise, the agent's additional data can be added to the conversation data.

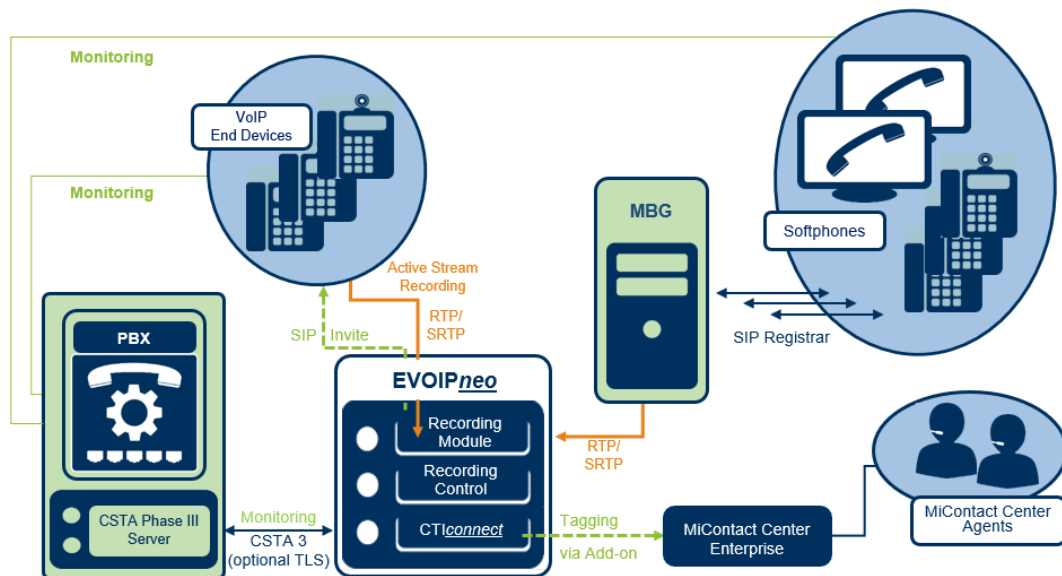


Fig. 1: Recording solution with Mitel MiVoice CSTA 3

Recording solution with active streaming

For the monitored end devices, the recording server receives the audio data directly from the phones. 2 separate RTP data streams are sent for each recorded end device. Depending on the configuration of the PBX, these streams can also be encrypted. The CSTA Phase III protocol provides the respective key.

Recording solution with VoIP end devices of Mitel without MBG

EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA 3) VoIP

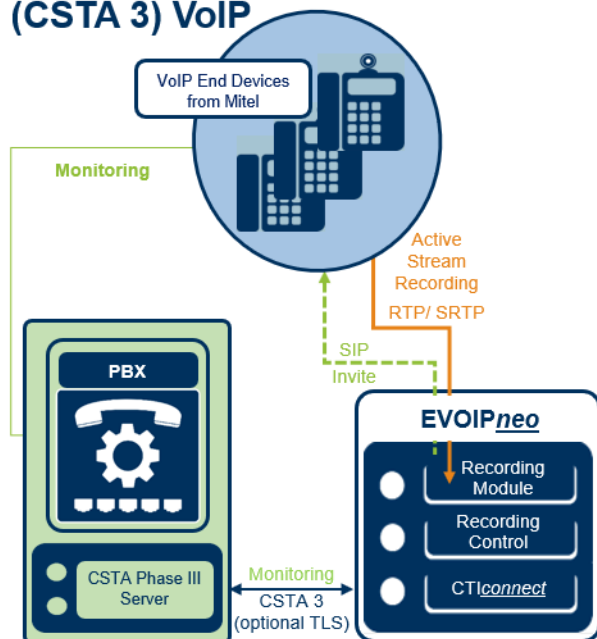


Fig. 2: Recording solution with VoIP end devices without MBG

Recording solution via a Mitel Border Gateway (MBG)

To record softphones and detached end devices (teleworker workplaces), the recording server additionally needs to communicate with the Mitel Border Gateway (MBG). The communication runs via an [SSL](#) tunnel to the Mitel Border Gateway (MBG).

NOTICE! For this recording variant, the phones which are supposed to be recorded, must have been registered on the [MBG](#) or the [SRC](#).

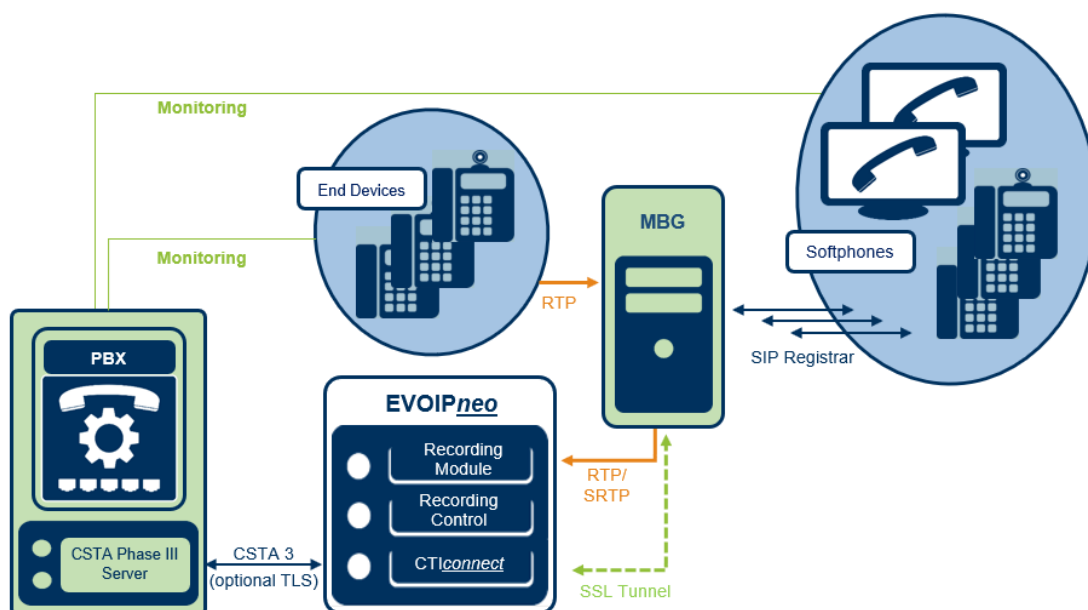


Fig. 3: Recording solution with MBG

Recording solution with intrusion

Recording solutions *neo* version 5.3 or higher offer the feature intrusion which includes the recording server in the conversation by silently adding it to the call. That way VoIP and TDM end devices can be recorded. In case of silent recording or when recording by means of the intrusion feature, the recording server initiates a silent conference with comprises the other call participants. The recording server registers with the PBX by means of the configured recording server extension via the CSTA connection. Therefore, an extension for the recording server must be available for each concurrent recording.

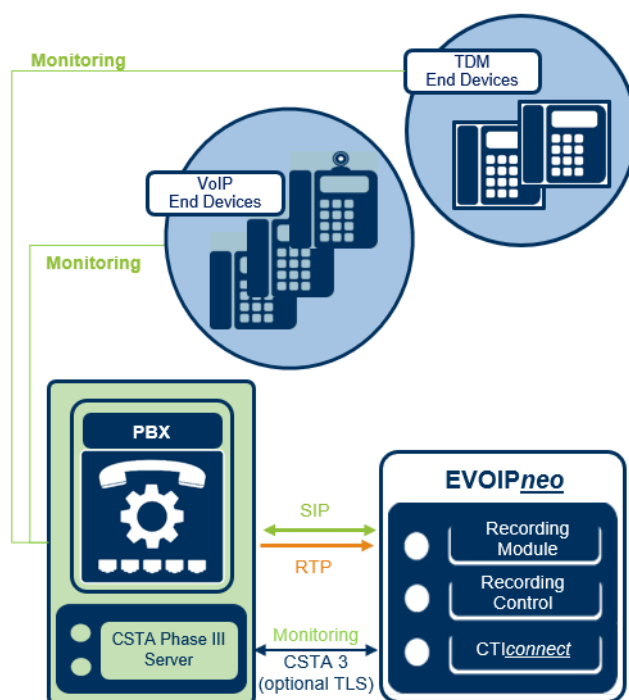


Fig. 4: Recording solution with intrusion



This type of recording does not allow recording conference calls, as intrusion itself is already the recording of a conference. A participant who is recorded by means of intrusion cannot participate in another conference call.

See also

📄 CTIconnect module [▶ 62]

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.

3.2.1 Mitel MiVoice MX-ONE software components

If external SIP trunks are used and calls are recorded in encrypted form, version 6.3 SP2 or higher must have been installed on the PBX.

The firmware of the phone must be version R5.0.0.2024 or higher.

3.3 Genesys system components (optional)

3.3.1 Genesys Framework

When using a CTI_{connect} for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

4 Installation requirements



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



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

4.1 Licenses

ASC

License name	Number
EVOIP _{neo} Base license - active	1 license per recording server
EVOIP _{neo} active for Mitel MiVoice MX-ONE (CSTA 3)	1 license per concurrent recording

Tab. 1: Licenses for recording server

License name	Number
PHONE _{app} universal for recording control per system	1 license per recording system

Tab. 2: Licenses for the phone application (optional)

Mitel MiVoice MX-ONE

License name	Number
CSTA license	1 license per end device
Intrusion	1 SIP extension per recording resource (third-party SIP license)

Tab. 3: Licenses

Mitel Border Gateway

License name	Number
MBG tap license	1 license per concurrent recording

Tab. 4: Licenses



If you are using several MBGs, the licenses must be available on each MBG.

MiContact Center Enterprise (optional)

License name	Number
MiContact Center Enterprise	1 basic package, contains licenses for 500 recording resources

Tab. 5: Licenses for MiContact Center Enterprise optional

Genesys T-Server (optional)

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

License name	Number
Genesys Universal SDK	1 per recording server

Tab. 6: Licenses for Genesys

4.2 Information

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

- IP address of the recording server
- List of extensions to be recorded



When updating versions \leq [neo 5.1](#), the [CTI](#) configuration parameter must be adjusted according to the new [CSTA 3](#) connection. See [chapter "CTIconnect module", p. 62](#).

The *HTTP web service link* is no longer required; however an IP address to the PBX with the default port 8882 must be configured.

5

Overview install and configure product

The following steps have to be taken:

1. Install neo software
2. 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
Assignment of the previously created recording architecture
 - Configure CTI connection data
Configuration of CTI connection parameters and of the grammar
 - Configure monitor points
Set monitor points for the extensions to be recorded
 - Global recording settings
Configuration of the settings for all recording servers in the network
 - Configure recording servers
Configuration of the parameters of the recording server, e. g. IP address, RTP incoming port and extensions
 - Configure add-on
By default, the add-on has been deactivated.
The following add-ons can be configured optionally for this recording solution:
MiContact Center Enterprise
Genesys T-Server
 - Configure miscellaneous settings
Optional configuration of participant information in an additional data field

6 Installation



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



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



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

7 Configuration

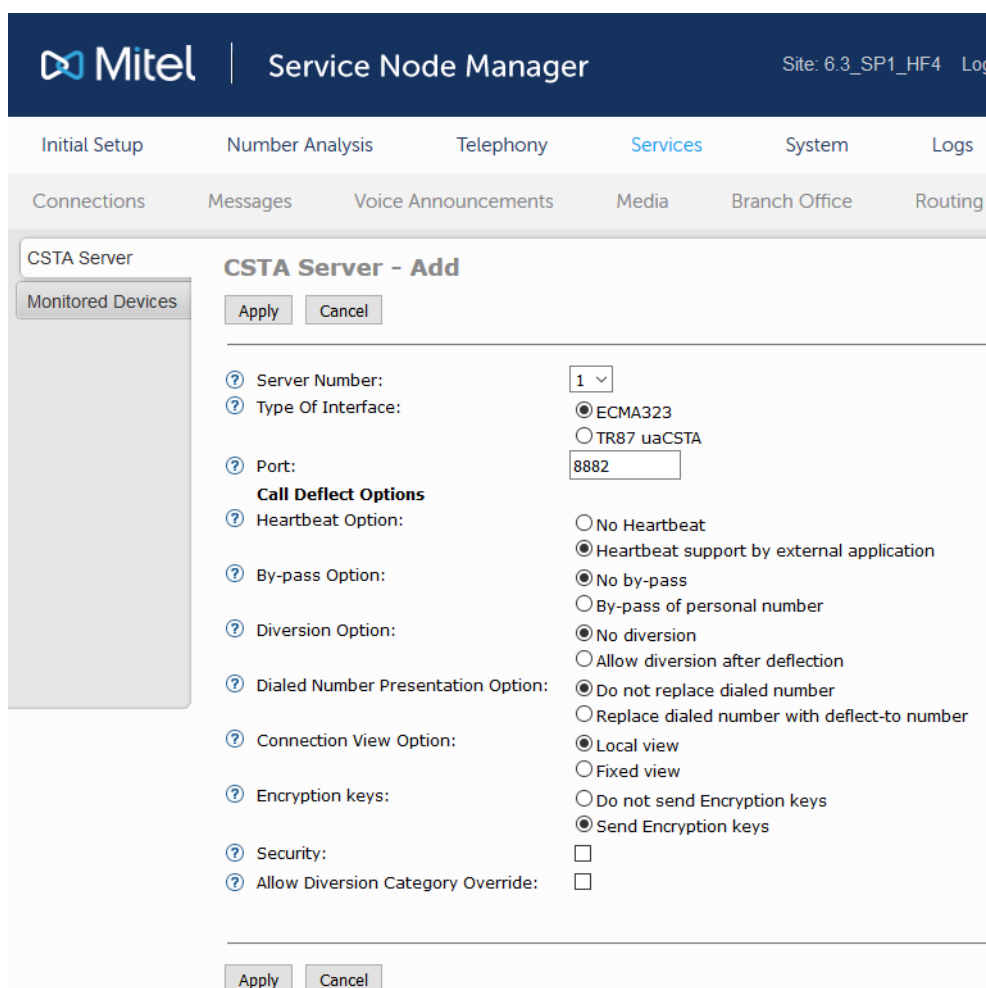
7.1 Configure Mitel MiVoice MX-ONE CSTA 3



The Mitel MiVoice MX-ONE PBX should be configured by a Mitel technician. The configuration file of the PBX has to contain the IP address of the recording server so that the [RTP](#) data can be sent to the recording server.

7.1.1 Configure CSTA server

1. Log in to the *Provisioning Manager*.
2. Select the tab *System*.
3. Below, select the menu item *Subsystem*.
4. Select the respective subsystem.
⇒ The *Service Node Manager* opens.
5. Select the tab *Services*.
6. Below, select the menu item *CSTA Server* in the menu bar.
7. Select the menu item *CSTA Server* in the navigation bar.



The screenshot shows the Mitel Service Node Manager interface. The top navigation bar includes 'Initial Setup', 'Number Analysis', 'Telephony', 'Services' (selected), 'System', and 'Logs'. Below this, a secondary navigation bar shows 'Connections', 'Messages', 'Voice Announcements', 'Media', 'Branch Office', and 'Routing'. The main content area is titled 'CSTA Server - Add' and contains the following configuration options:

- Server Number:** 1 (dropdown)
- Type Of Interface:** ☒ ECMA323, ☐ TR87 uaCSTA
- Port:** 8882 (text input)
- Call Deflect Options:**
 - Heartbeat Option:** ☐ No Heartbeat, ☒ Heartbeat support by external application
 - By-pass Option:** ☒ No by-pass, ☐ By-pass of personal number
 - Diversion Option:** ☒ No diversion, ☐ Allow diversion after deflection
 - Dialed Number Presentation Option:** ☒ Do not replace dialed number, ☐ Replace dialed number with deflect-to number
 - Connection View Option:** ☒ Local view, ☐ Fixed view
 - Encryption keys:** ☐ Do not send Encryption keys, ☒ Send Encryption keys
 - Security:** ☐
 - Allow Diversion Category Override:** ☐

Buttons for 'Apply' and 'Cancel' are located at the bottom of the form.

Fig. 5: Configure CSTA server

8. Click on the button *Add*.
9. Select the following options:

Type of Interface	ECMA323
Port	Enter the port you would like to use for the communication, for TCP 8882, for TLS 8883.
Heartbeat Option	Heartbeat support by external application Not obligatory but recommended.
By-pass Option	No by-pass
Diversion Option	No diversion
Dialed Number Presentation Option	Do not replace dialed number
Connection View Option	Local view
Encryption keys	Send Encryption keys
Security	<p>Activate this option if the connection via TLS is supposed to be used. Unencrypted by default.</p> <p>NOTICE! If the option <i>Encryption keys</i> has been activated and the option <i>Security</i> deactivated at the same time, the <i>encryption keys</i> are transferred without encryption. This is a security gap as potential attackers could intercept these keys and use them to decrypt the encrypted streams of audio data.</p>

10. Click on the button *Apply* to save the settings.



Different codecs of RX-TX in one [SIP](#) conversation are not supported.

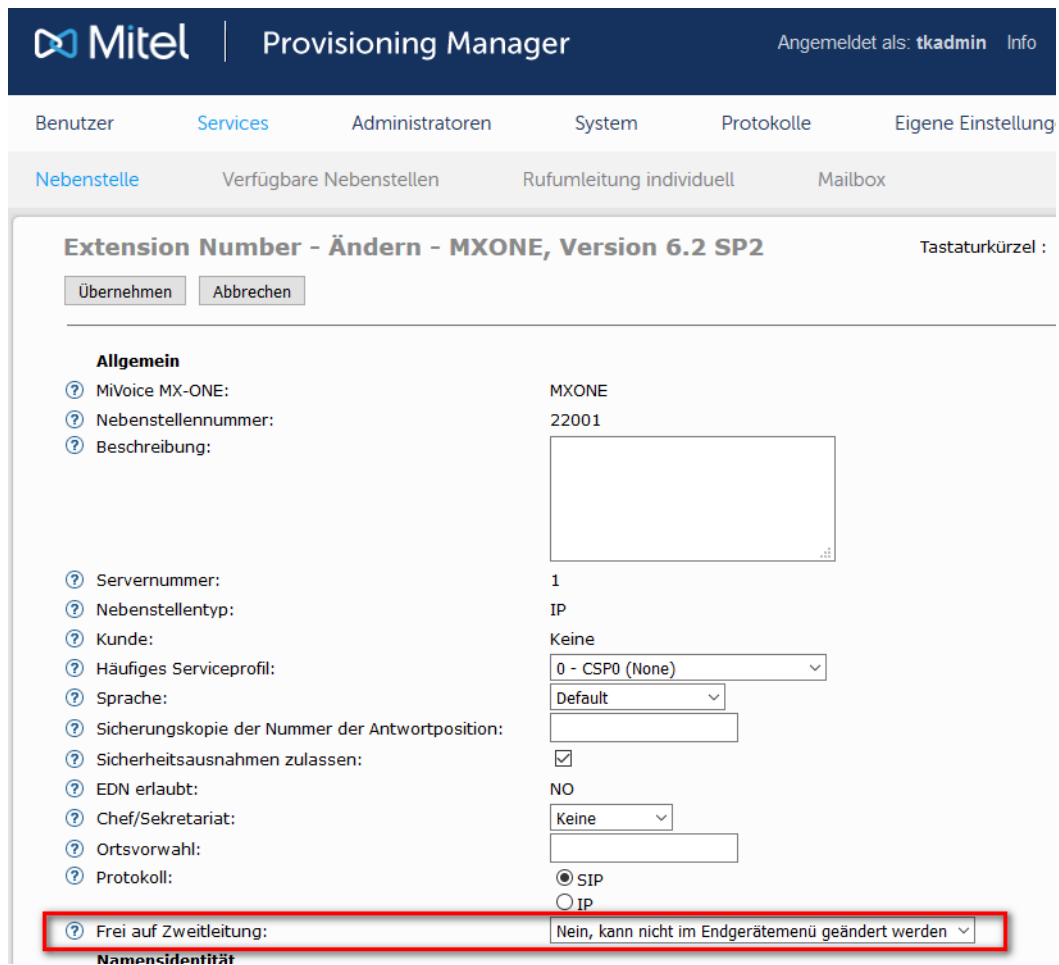
7.1.2

Configure extension monitor points

The extension monitor points are configured in the Provisioning Manager, usually by a Mitel engineer.

To be able to use the intrusion feature, the parameter for the free-line signal on the second line in the configuration of the extension to be monitored must be set to *No* (> Frei auf Zweitleitung > Nein, ...) . Only then, can the CTIconnect service initiate an intrude call and a silent conference.

1. Log in to the *Provisioning Manager*.
2. Change to the menu item *Services*.
3. Select the menu item *Nebenstelle* (extension).
4. Enter the respective extension.
5. Click on the button *Ändern* (Change).



Extension Number - Ändern - MXONE, Version 6.2 SP2 Tastaturkürzel :

Allgemein

☐ MiVoice MX-ONE: MXONE
☐ Nebenstellenummer: 22001
☐ Beschreibung:
☐ Servernummer: 1
☐ Nebenstellentyp: IP
☐ Kunde: Keine
☐ Häufiges Serviceprofil: 0 - CSP0 (None)
☐ Sprache: Default
☐ Sicherungskopie der Nummer der Antwortposition:
☐ Sicherheitsausnahmen zulassen: ☒
☐ EDN erlaubt: NO
☐ Chef/Sekretariat: Keine
☐ Ortsvorwahl:
☐ Protokoll:
☒ SIP
☐ IP

Namensidentität

☐ Frei auf Zweitleitung: Nein, kann nicht im Endgerätemenü geändert werden

Fig. 6: Configure free-line signal for extension

6. For the parameter *Frei auf Zweitleitung* (free-line signal on second line), select the entry *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device) from the drop-down list.
7. Click on the button *Übernehmen* (Apply) to save the setting.

7.1.3 Check functionality

Check monitor points

1. Log in to the *Mitel Service Node Manager* to check the monitor points that have been set.
2. Select the tab *Services > CSTA Server*.
3. Select the menu item *Monitored Devices* in the navigation bar.
 - ⇒ A list of the set monitor points appears.

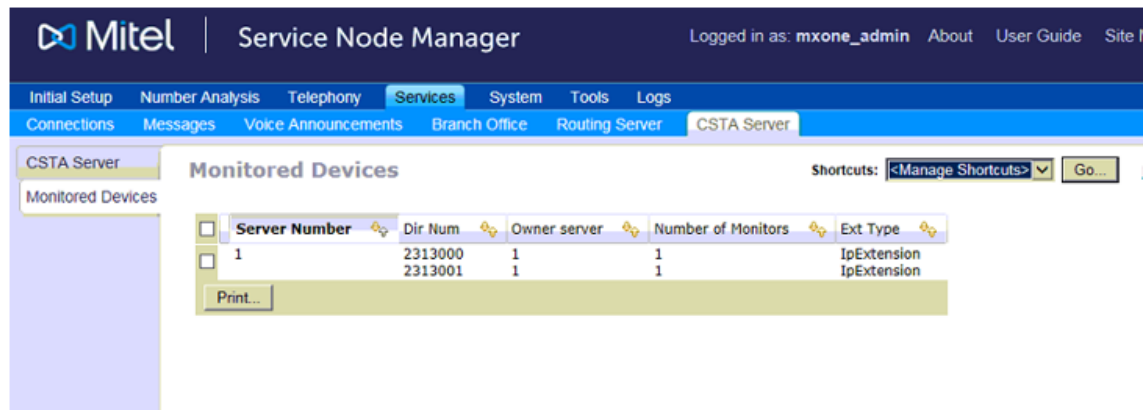


Fig. 7: Check set monitor points

Check license status

1. Log in to the respective phone as administrator via the web interface to check the license status.

The following login data is valid by default:

Username	admin
Password	22222

2. Select the menu item *License Status* in the navigation bar to check whether the license is valid.

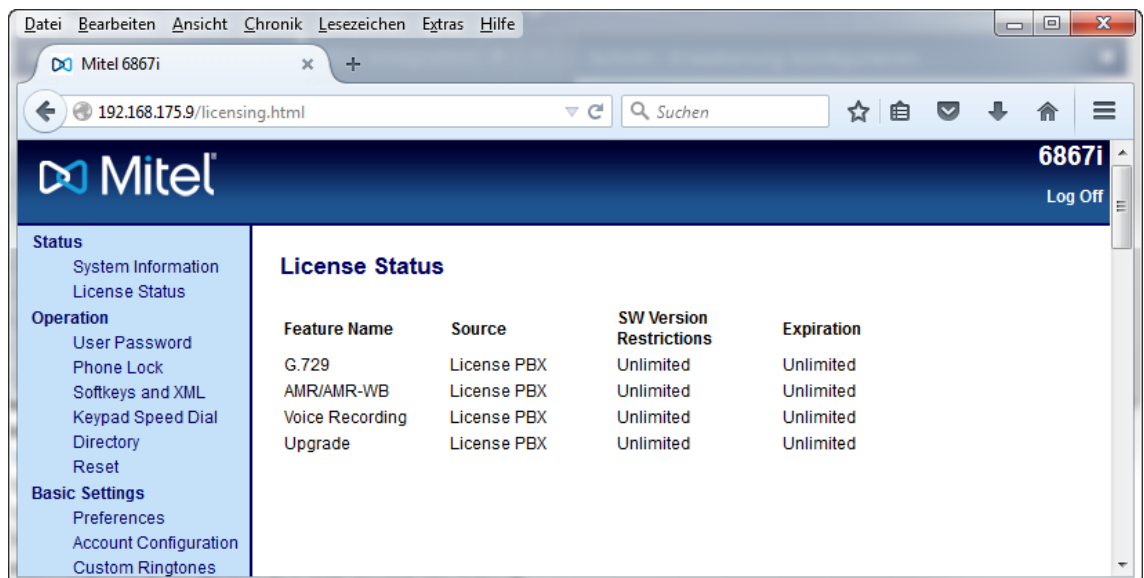


Fig. 8: Check license status

Check server, path and port

1. Select the menu item *Advanced Settings > Configuration Server* in the navigation bar to check the settings of the server, the path and the port.

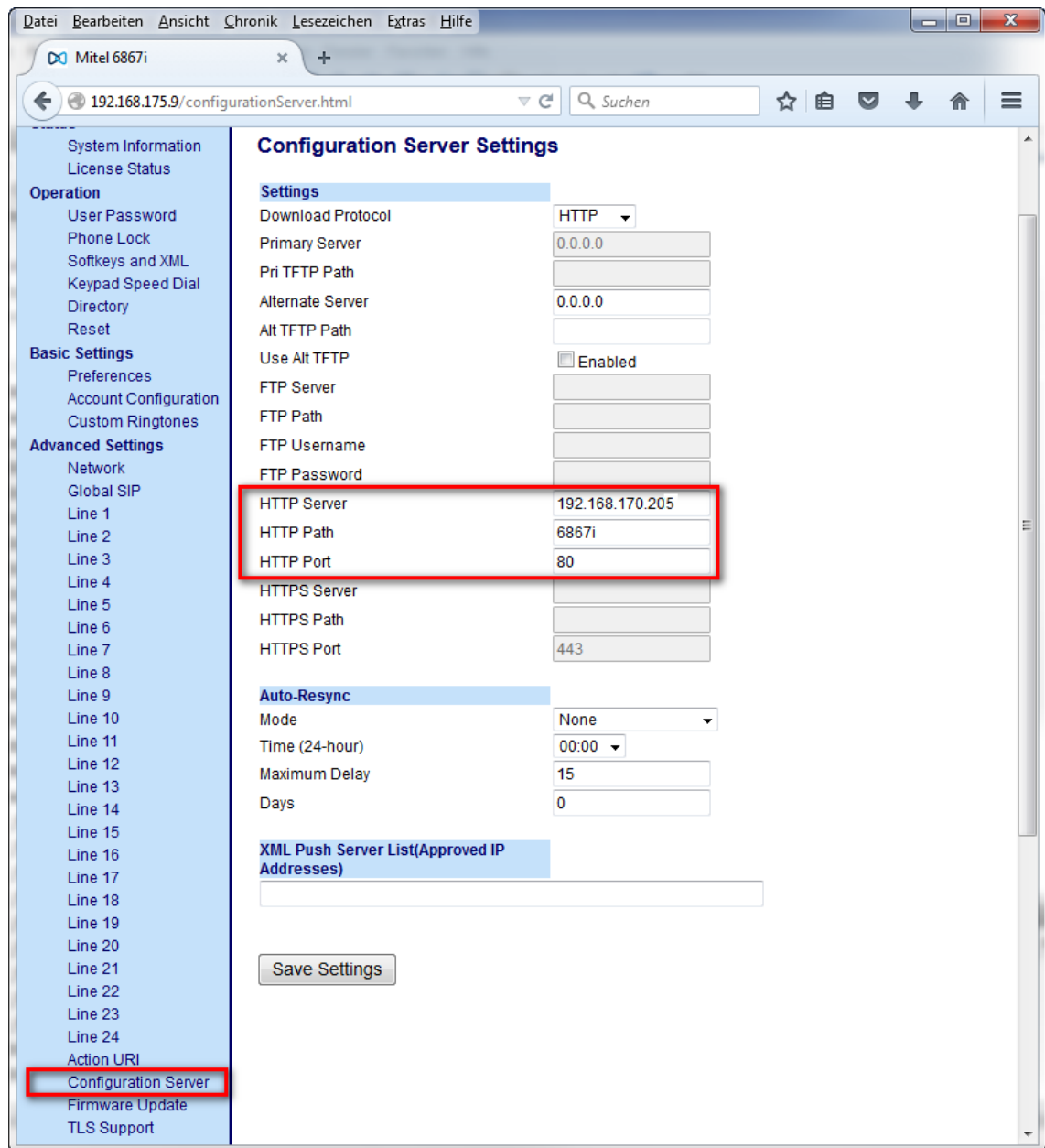


Fig. 9: Check server, path and port

2. Click on the button *Save Settings* to save the entries.

Check IP address and transport protocol

The configuration of the recording by means of a [SIP](#) INVITE without MBG is saved in the configuration file *startup.cfg*. The phones get the settings from this configuration file upon starting.

1. Open the configuration file of the phone via the browser using the IP address of the PBX, e. g. <http://192.168.170.205/6867i>.
⇒ The file *startup.cfg* opens.

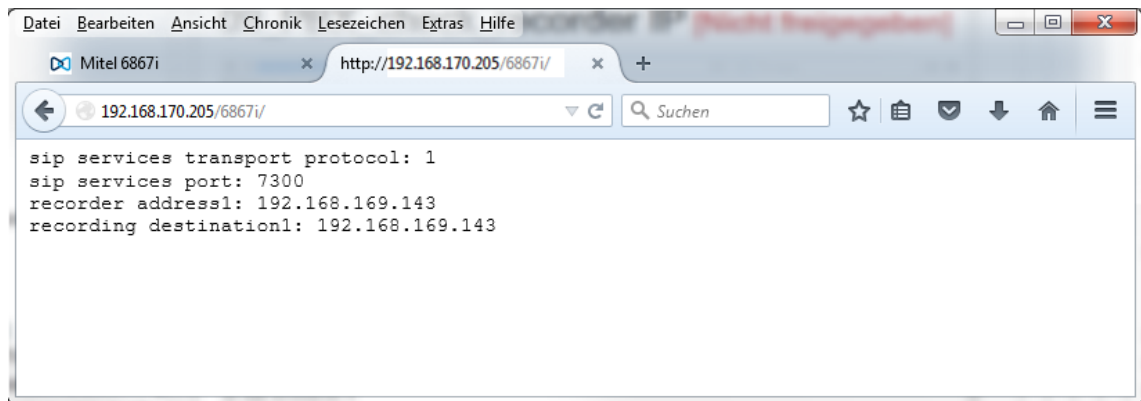


Fig. 10: Check IP address and transport protocol

2. Here, you can check the ACTIVE VOIP RECORDING SETTINGS.

<i>recorder address1</i>	Enter the IP address of the recording server, e. g. 192.168.169.143 .
<i>sip services transport protocol:</i>	Enter the respective value for the deployed transport protocol: UDP = 1 TCP = 2 The configuration must coincide with the SIP configuration of the end devices in the PBX.
<i>recorder periodic beep</i>	If this parameter has been configured, a beep signal is sent in defined intervals during the recording. This entry only appears if it has been configured in the PBX.

If recording has been configured in the *startup.cfg* and calls are recorded according to the [SIP](#) INVITE mechanism, the display of the phone indicates that recording is taking place. This information is not displayed if calls are recorded by means of the [MBG](#).

7.2 Configure Mitel Border Gateway

7.2.1 Install certificate on the MBG

To be able to establish an [SSL](#) connection from the recording server to the Mitel Border Gateway ([MBG](#)), you have to confirm the security certificate on the [MBG](#).



If you use a pre-shared key, you don't need to confirm the security certificate.

1. Connect to the [MBG](#).

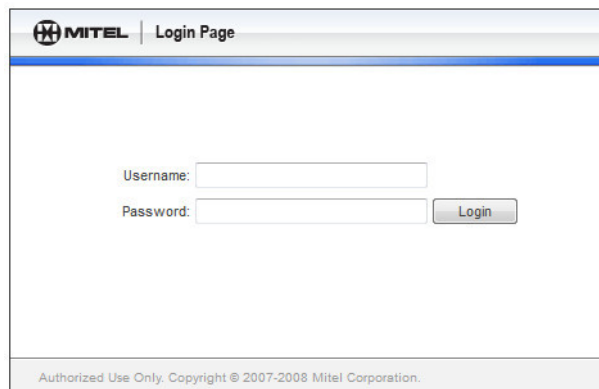
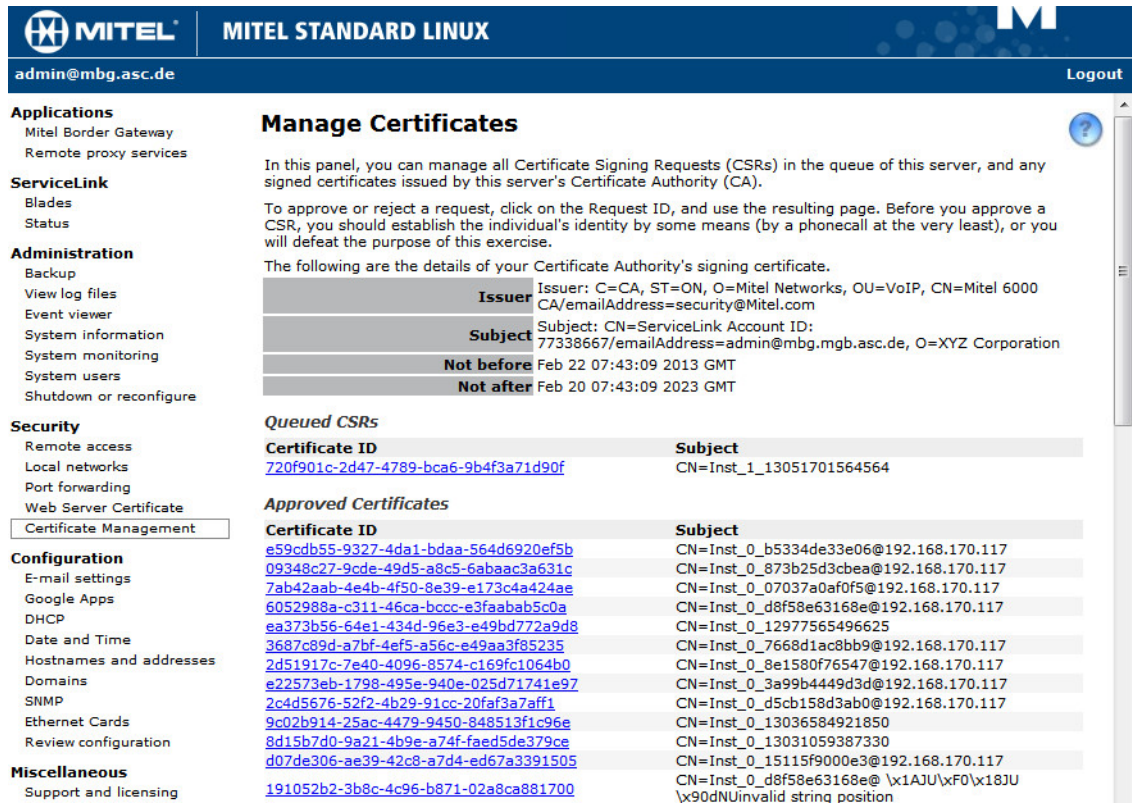


Fig. 11: Login screen MBG

- Log in to the web interface. The access data for the Mitel Border Gateway is provided by the Mitel engineer.

⇒ The following window appears:



The screenshot shows the Mitel Standard Linux web interface. The top header includes the Mitel logo, the text "MITEL STANDARD LINUX", the user "admin@mbg.asc.de", and a "Logout" button. The left sidebar contains a navigation menu with categories: Applications (Mitel Border Gateway, Remote proxy services), ServiceLink (Blades, Status), Administration (Backup, View log files, Event viewer, System information, System monitoring, System users, Shutdown or reconfigure), Security (Remote access, Local networks, Port forwarding, Web Server Certificate, Certificate Management), Configuration (E-mail settings, Google Apps, DHCP, Date and Time, Hostnames and addresses, Domains, SNMP, Ethernet Cards, Review configuration), and Miscellaneous (Support and licensing). The "Certificate Management" option is highlighted.

Manage Certificates

In this panel, you can manage all Certificate Signing Requests (CSRs) in the queue of this server, and any signed certificates issued by this server's Certificate Authority (CA).

To approve or reject a request, click on the Request ID, and use the resulting page. Before you approve a CSR, you should establish the individual's identity by some means (by a phonecall at the very least), or you will defeat the purpose of this exercise.

The following are the details of your Certificate Authority's signing certificate.

Issuer	Issuer: C=CA, ST=ON, O=Mitel Networks, OU=VoIP, CN=Mitel 6000 CA/emailAddress=security@Mitel.com
Subject	Subject: CN=ServiceLink Account ID: 77338667/emailAddress=admin@mbg.mgb.asc.de, O=XYZ Corporation
Not before	Feb 22 07:43:09 2013 GMT
Not after	Feb 20 07:43:09 2023 GMT

Queued CSRs

Certificate ID	Subject
720f901c-2d47-4789-bca6-9b4f3a71d90f	CN=Inst_1_13051701564564

Approved Certificates

Certificate ID	Subject
e59c0b55-9327-4da1-bdaa-564d6920ef5b	CN=Inst_0_b5334de33e06@192.168.170.117
09348c27-9cde-49d5-a8c5-6abaac3a631c	CN=Inst_0_873b25d3cbea@192.168.170.117
7ab42aab-4e4b-4f50-8e39-e173c4a424ae	CN=Inst_0_07037a0af0f5@192.168.170.117
6052988a-c311-46ca-bccc-e3faabab5c0a	CN=Inst_0_d8f58e63168e@192.168.170.117
ea373b56-64e1-434d-96e3-e49bd772a9d8	CN=Inst_0_12977565496625
3687c89d-a7bf-4ef5-a56c-e49aa3f85235	CN=Inst_0_7668d1ac8bb9@192.168.170.117
2d51917c-7e40-4096-8574-c169fc1064b0	CN=Inst_0_8e1580f76547@192.168.170.117
e22573eb-1798-495e-940e-025d71741e97	CN=Inst_0_3a99b4449d3d@192.168.170.117
2c4d5676-52f2-4b29-91cc-20faf3a7aff1	CN=Inst_0_d5cb158d3ab0@192.168.170.117
9c02b914-25ac-4479-9450-848513f1c96e	CN=Inst_0_13036584921850
8d15b7d0-9a21-4b9e-a74f-faed5de379ce	CN=Inst_0_13031059387330
d07de306-ae39-42c8-a7d4-ed67a3391505	CN=Inst_0_15115f9000e3@192.168.170.117
191052b2-3b8c-4c96-b871-02a8ca881700	CN=Inst_0_d8f58e63168e@ \x1AJU\xF0\x18JU \x90dNUinvalid string position

Fig. 12: Certificate Management

- Select the menu item *Security > Certificate Management* in the structure view.

⇒ In the section *Queued CSRs*, certificates which have not yet been confirmed are listed.
- Click on the certificate of the recording server.

⇒ The certificate is displayed.

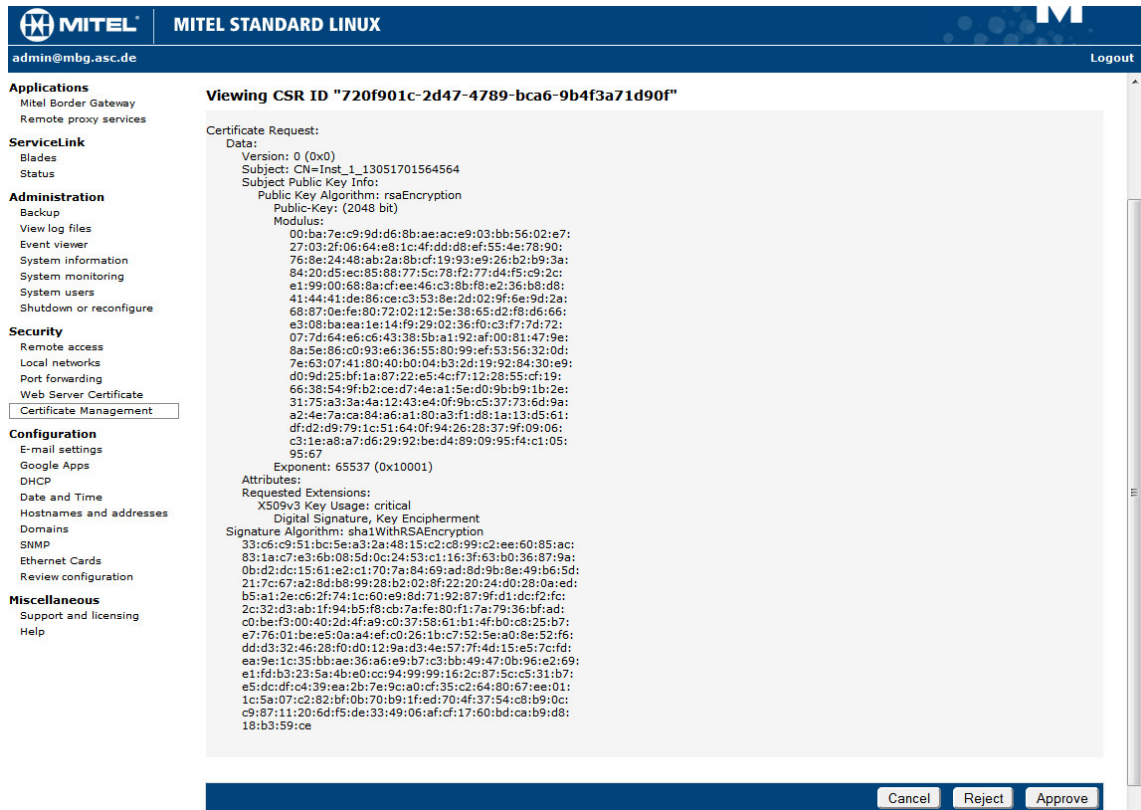


Fig. 13: Confirm selected certificate

5. Click on the button **Approve**.

⇒ The following success message appears once the certificate have been released:

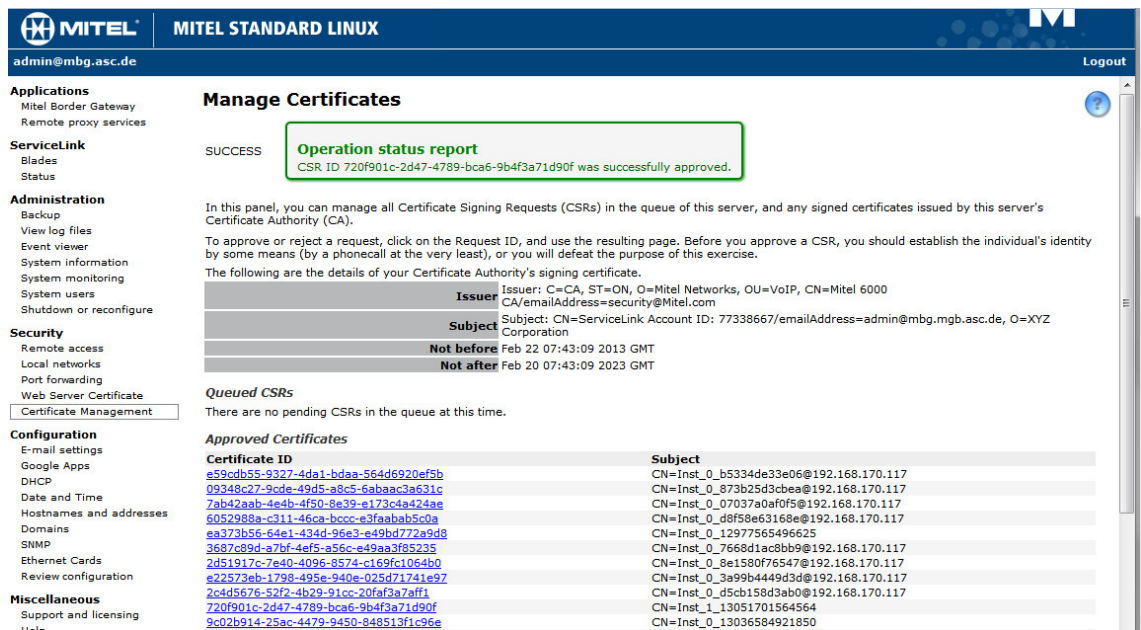


Fig. 14: Success message for a released certificate

The recording server can now establish a connection with the **MBG** via the **SSL** tunnel.

7.3

System Configuration



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

7.3.1 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.

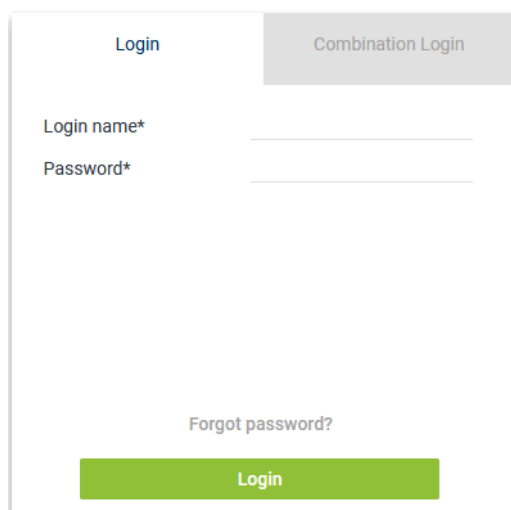


Fig. 15: System Configuration - web interface

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

Login data for the administrator of the system provider:

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

Tab. 7: Login data - system provider

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

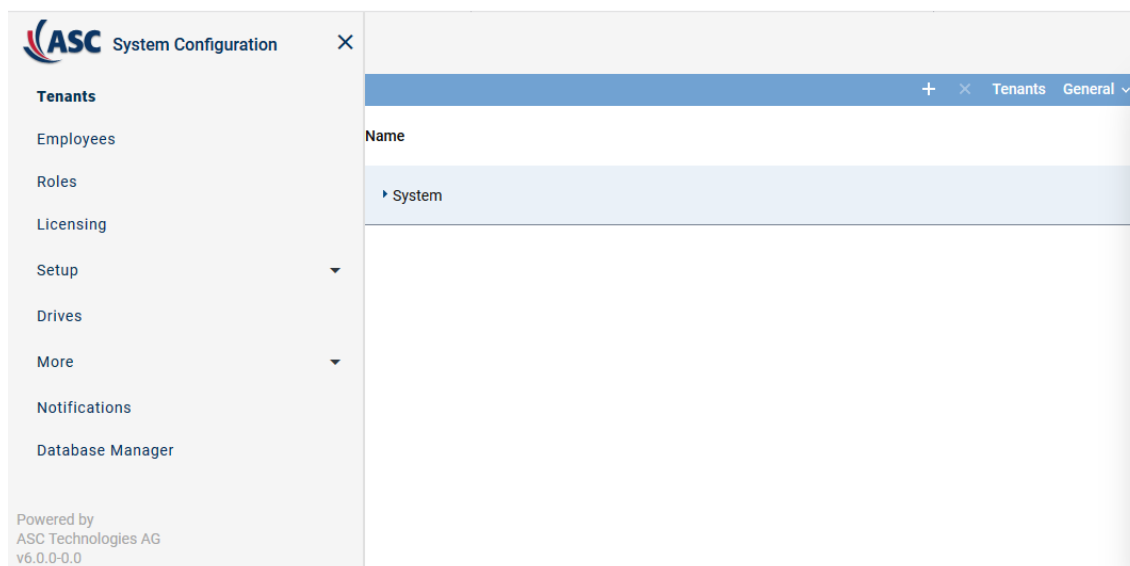


Fig. 16: System Configuration - main view:

7.3.2 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
- Multi-Server Recording
- Multi-Server Failover

7.3.2.1 Configure recording solution All-in-one Basic

7.3.2.1.1 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:

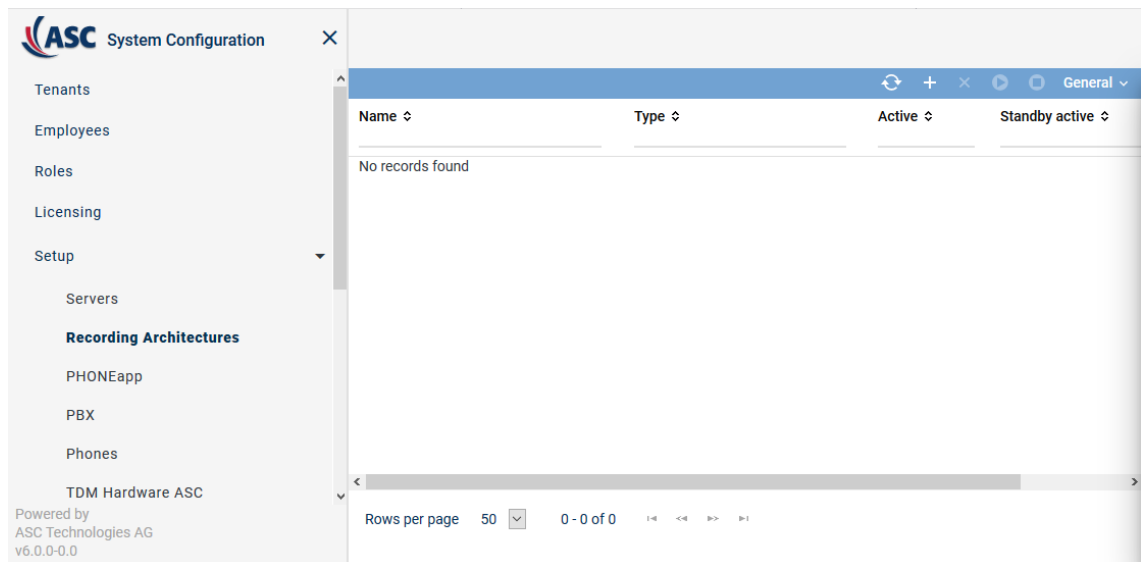




Fig. 17: Recording architectures - main view

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


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

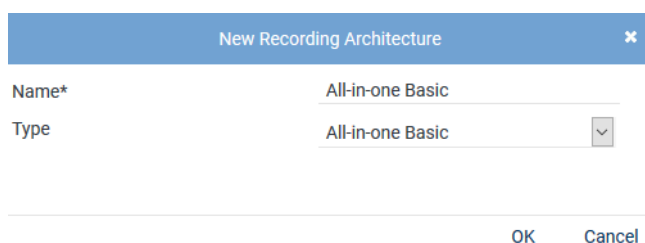
Create recording architecture All-in-one Basic

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



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

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



New Recording Architecture

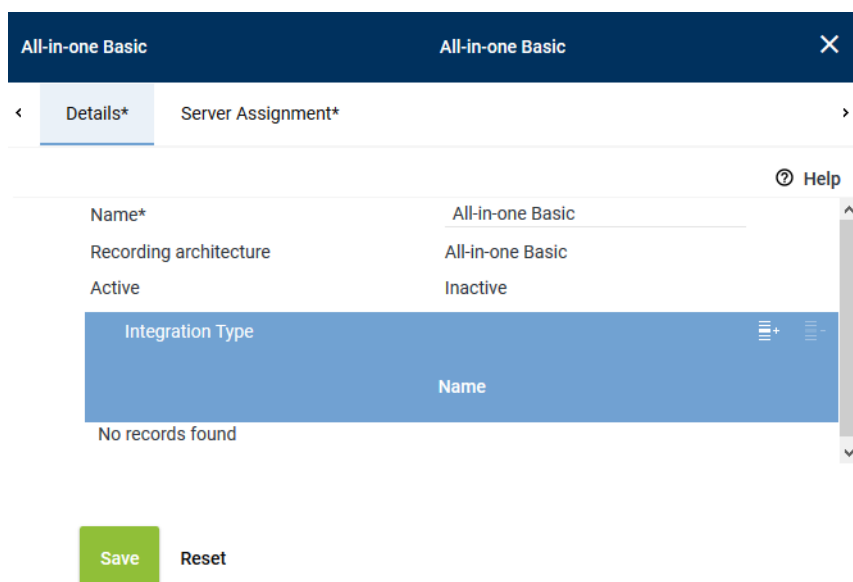
Name* All-in-one Basic

Type All-in-one Basic

OK Cancel

Fig. 18: Create recording architecture - All-in-one Basic Recording

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



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

< Details* Server Assignment* >

Help

Name*	All-in-one Basic
Recording architecture	All-in-one Basic
Active	Inactive


Integration Type

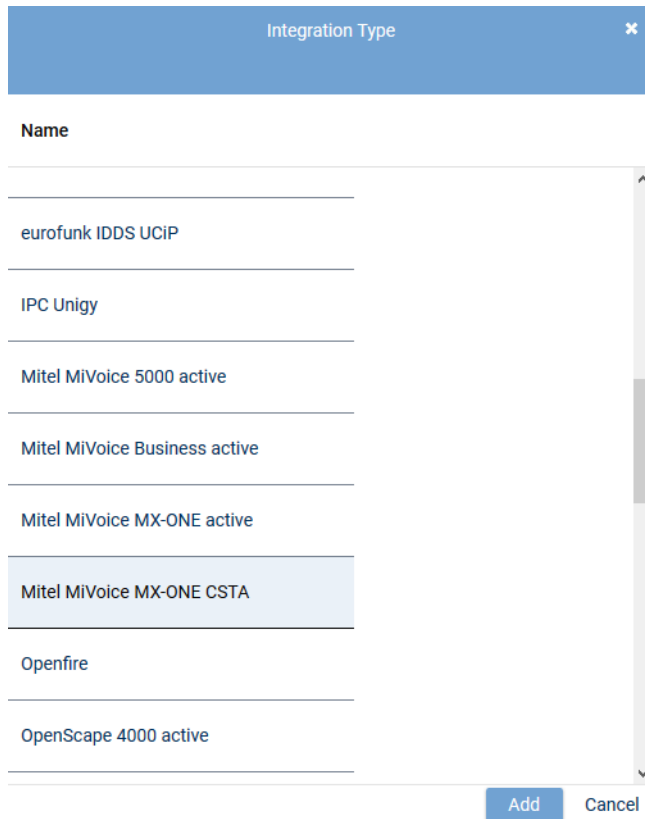
No records found

Save Reset

Fig. 19: Recording architecture - tab Details

Add integration type

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



The dialog box titled "Integration Type" contains a list of integration types. The list is as follows:

Name
eurofunk IDDS UCIP
IPC Unigy
Mitel MiVoice 5000 active
Mitel MiVoice Business active
Mitel MiVoice MX-ONE active
Mitel MiVoice MX-ONE CSTA
Openfire
OpenScape 4000 active

The "Mitel MiVoice MX-ONE CSTA" option is currently selected. At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Fig. 20: 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 *Mitel MiVoice MX-ONE CSTA* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign server for All-in-one Basic

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

All-in-one Basic

All-in-one Basic

×

Details*

Server Assignment*

Server*

REC-01

+

-

Used in activated architecture

No

Recording type

☐ VoIP/Video
☐ TDM
☐ Screen
☐ Chat

Save

Reset

Fig. 21: Recording Architecture - tab Server Assignment

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

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

Rows per page 20 ▾

1 - 8 of 8

⏪

<⏪

⏩>

⏩

Add

Cancel

Fig. 22: Recording Architecture - assign server

- Select the entry of the corresponding server.



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

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

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen




☐ Chat

Fig. 23: Recording Architecture - activate recording type



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

Activate recording architecture

1. Click on the button **Save**.
2. Select the recording architecture in the main view so that the icon  (*Activate*) in the tool-bar becomes active.
3. To activate the recording architecture, click on the icon  (*Activate*).
⇒ In the column *Active*, the icon  (*Active*) appears.





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

Fig. 24: 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 extension for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.3.2.1.2 Configure servers

Every server in your network that the *neo* software has been installed on is automatically identified as a server of the recording system and displayed in the main view of the Servers module. In the Servers module, you can configure the usage of the servers in your recording system.

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

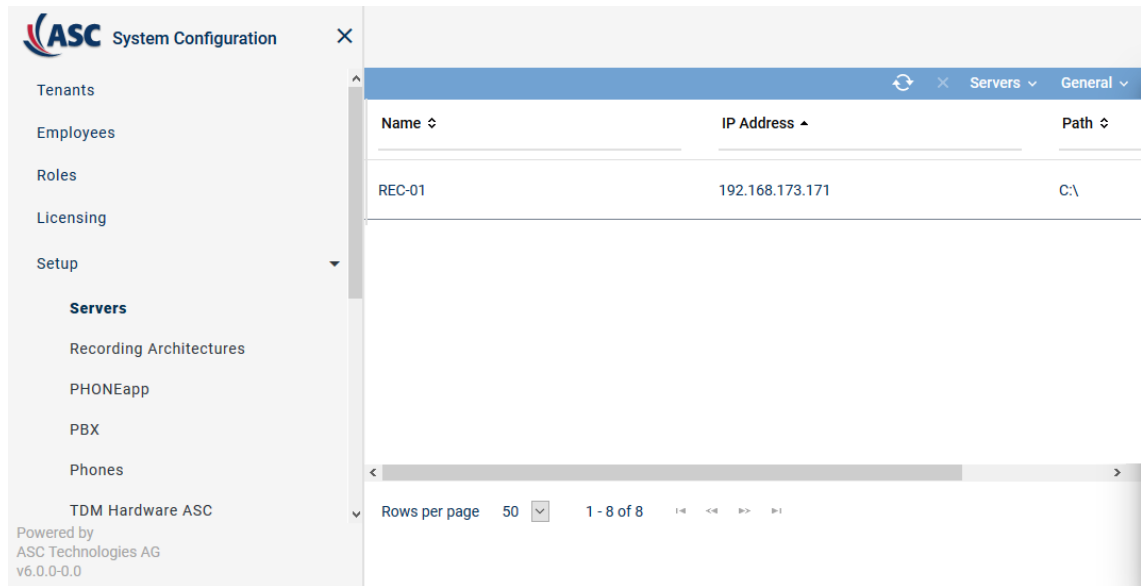


Fig. 25: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	Date on which the settings of the server were updated for the last time.

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

Toolbar of the Servers module

The toolbar offers the following functions.

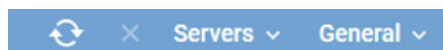




Fig. 26: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Delete</i>	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations" , p. 30.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see chapter "Administrate NTP server" , p. 46.
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view:

	<ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
<i>Save Table Configuration</i>	Saves the current table configuration of the main view as default view of the user.
<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
<i>Reset Search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
<i>General Help</i>	Opens the online help.
<i>Module Help</i>	Opens the module-specific online help.



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

Administrate server locations

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

Add server locations

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

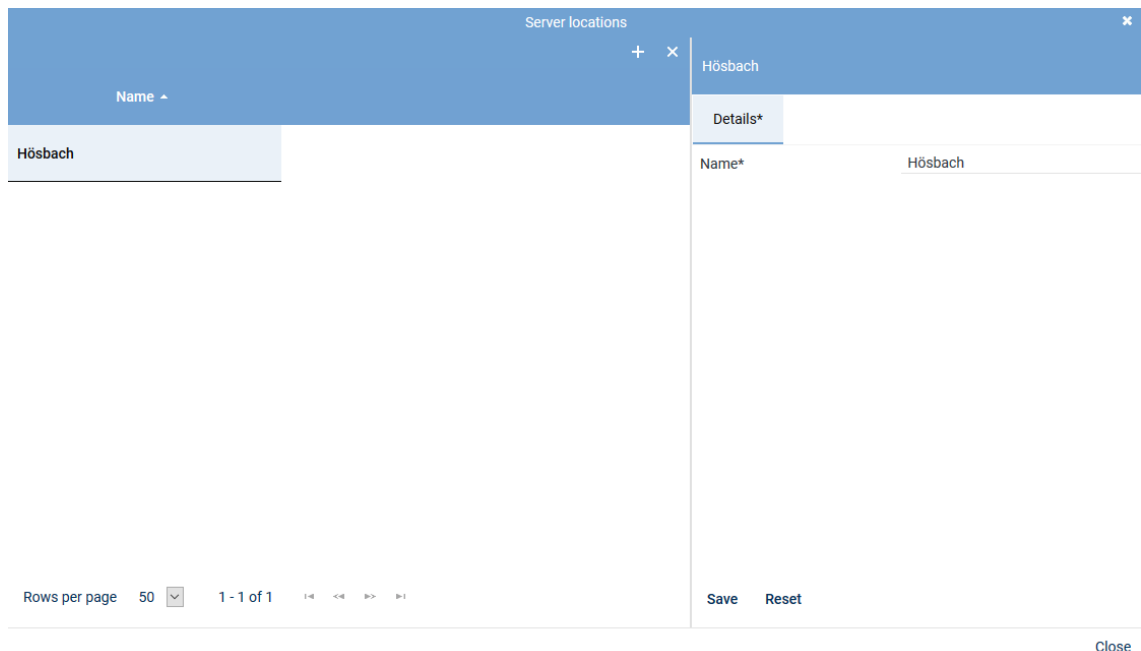



Fig. 27: Add server locations

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

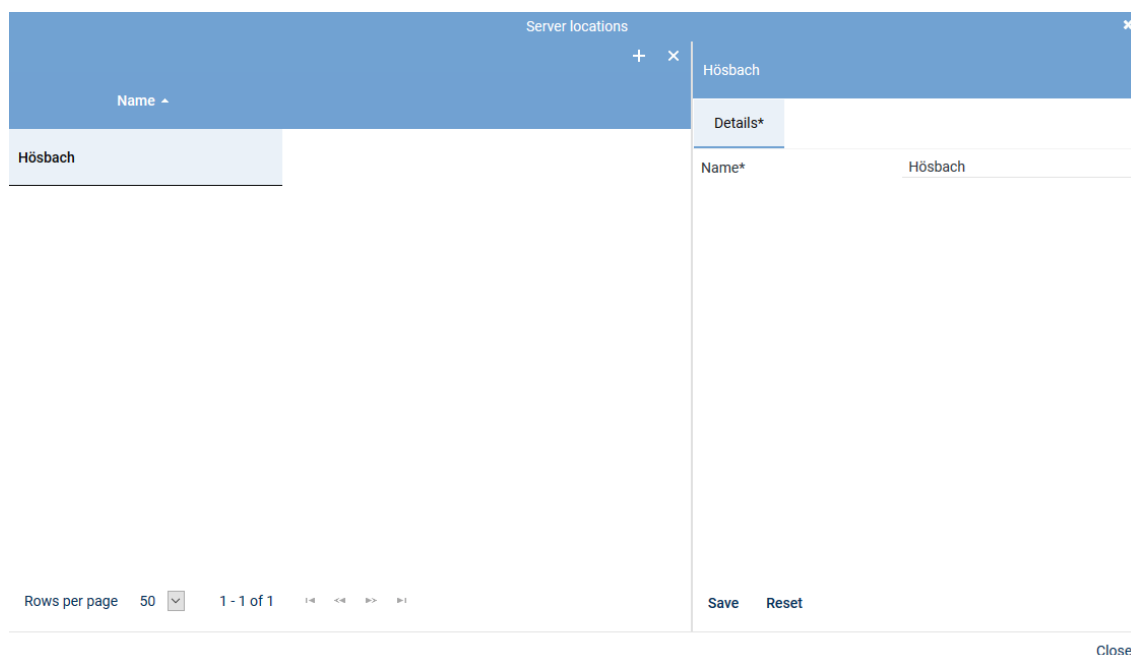
6. To close the window, click on the button *Close*.

Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (X) in the top right corner. Below the title bar is a toolbar with a "+" icon and a "x" icon. The main area is divided into two panes. The left pane contains a table with a single row: "Hösbach". The right pane is titled "Details*" and contains a form with a label "Name*" and a text input field containing "Hösbach". At the bottom of the window, there is a footer area with "Rows per page 50" and "1 - 1 of 1" on the left, and "Save" and "Reset" buttons on the right. A "Close" button is located at the bottom right of the window.

Fig. 28: Delete server location

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

Tab Details

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

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

? Help

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

Fig. 29: Servers - tab Details

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

Tab Usage

- Click on the tab *Usage* to configure the purpose of usage.



Since a server can be used for several recording solutions, all purposes of use are listed. Note that some purposes of use do not apply for some recording solutions. As an example: You cannot use audio analysis or replay via phone in a chat recording.

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

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

Fig. 30: Servers - tab Usage

Group field API Server

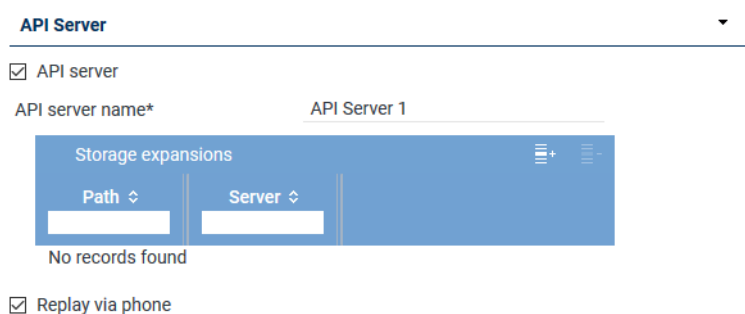


Fig. 31: Group field API Server


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




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


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

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

Parameter	Value/Description
<i>API server</i>	<p>Tick the check box to start the API server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>In order to be able to reach the API server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 42.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the storage expansions, see chapter "Add storage expansion for replay", p. 34.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (<i>Remove</i>), you can remove the storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> Application POWERplay Pro Application POWERplay Instant Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 41. To be able to do so, at least 1 PBX must have been configured in the system.</p>

Add storage expansion for replay

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

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

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 32: Select storage expansion

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

Group field Audio Analysis

Audio Analysis ▼

☒ Audio analysis (SAES mode)

Stream audio data from* + -

☐ Emotion detection

Stream audio data from* + -

Fig. 33: Group field Audio Analysis

Parameters	Value/Description
<i>Audio analysis</i>	<p>Activate this check box to use the server for audio analysis. The audio data is then streamed for audio analysis from the configured server to this server.</p> <ul style="list-style-type: none"> Stream audio data from From the list of available servers, select the server from which the audio data is supposed to be streamed for audio analysis via the button +.
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for the audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>

Tab. 8: Configure audio analysis

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☒ Recording control/Monitoring

Recording architecture ▼

☒ neo key management

Fig. 34: Group field Recording Control/Key Management

Parameters	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <u>CLIENT</u><i>command</i> or an API recording control or if you would like to use <i>Monitoring</i>. This feature is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the respective recording architecture you would like to use for the control.
<i>- neo key management</i>	<p>The function allows customer-specific encryption of the recordings. To be able to configure the key management, you have to activate the check box <i>Key management</i>.</p> <p>This function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p>

Parameters	Value/Description
	For further information about the configuration of the key management refer to the administration manual <i>Configuration of servers and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i> .

Tab. 9: Configure Recording Control/Key Management

Group field Data Processing

Data Processing ▼

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address
No records found	

Activate period of time ☒

from 11:59:36

to 11:59:36

Receives data from

Name	Only Replay
No records found	



☒ Archiving





☒ Export

☒ Import

Recording architecture Please choose... ▼


Fig. 35: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	Activate the check box to allow the modification of the additional functions of data processing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 38. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which an API server and a replay server have been configured.</p>

Parameter	Value/Description
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 38. By clicking on the icon  (<i>Remove</i>), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which the function <i>Data Storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 10: 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.



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

Rows per page: 20 | 1 - 6 of 6 | < << >> >

Add Cancel

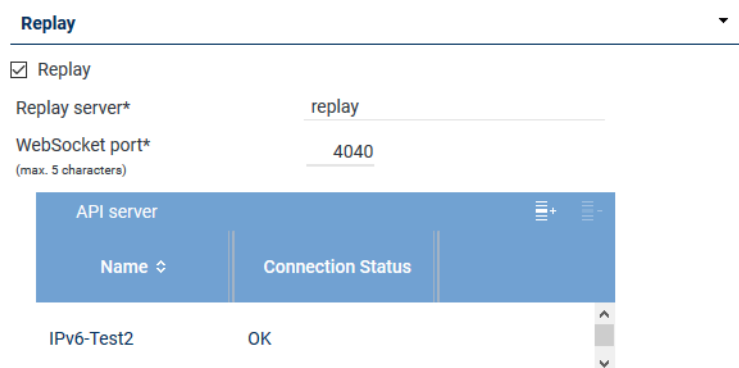
Fig. 36: Select server



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

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

Group field Replay



Replay

☒ Replay



Replay server* replay

WebSocket port* 4040
(max. 5 characters)

Name	Connection Status
IPv6-Test2	OK

Fig. 37: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated <i>Replay Feature</i> . Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.

Parameter	Value/Description
	<p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 39. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 11: 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. 38: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 33](#).

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

Virtualization ▼

☐ VM support

Fig. 39: Group field Virtualization

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

Tab. 12: 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.

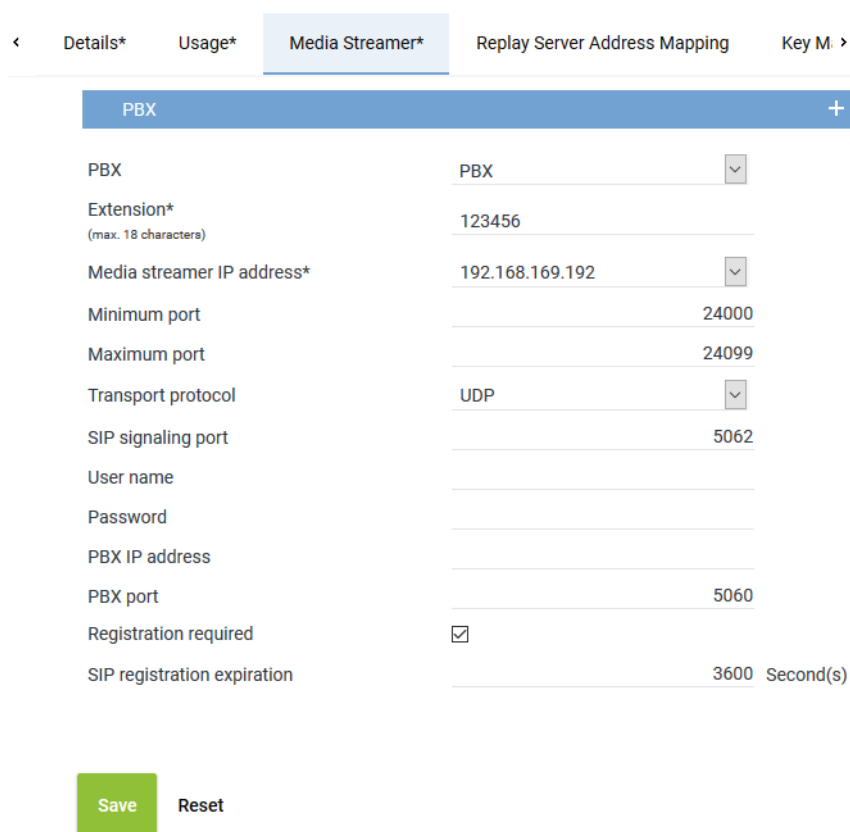
Tab Media Streamer

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*.



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

PBX +

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

Save Reset

Fig. 40: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX, see chapter "Create PBX", p. 47.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>

<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. In the drop-down list, all IP addresses of the server are displayed.</p> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</p>
<i>Minimum port</i>	Enter the minimum port which is supposed to be used for the audio data exchange.
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p>
<i>Transport protocol</i>	<p>Select the transport protocol type you would like to use for the SIP communication from the drop-down list.</p> <p>TCP = unencrypted UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address 169.254.254.101.</p>
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box Registration required.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

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

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



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

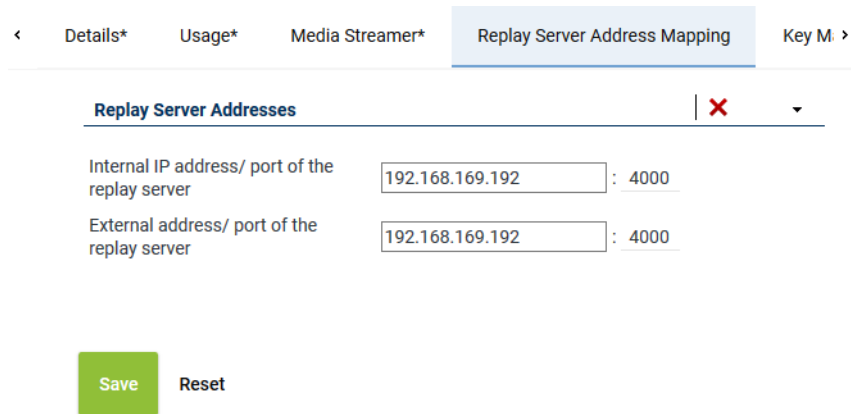


Fig. 41: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



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

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



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



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

Tab Key Management

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

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

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

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage
until

0 Day(s)

0 Hour(s)

☐ Key expiration date
after

0 Day(s)

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

Save Reset

Fig. 42: Servers module - tab Key Management

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

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

In case of an error ... automatically

Select whether simple key management is supposed to be used if the neo key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the neo key management has been activated but does not work.

☒ = In case of an error, simple key management is used as replacement.

☐ = In case of an error, no recording takes place as long as the neo key management has been activated. In this case, disable key management in the tab *Usage*.



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



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

Tab Keystore/Virtualization

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

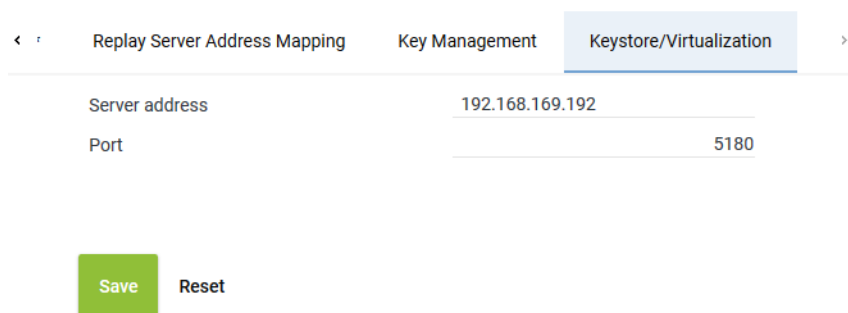
In this tab, you can configure the connection data for the service *DongleMan* for the neo key management and for the authentication of the VM.



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*.



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

Fig. 43: 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

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

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

Administrate NTP server

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

Add NTP server

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

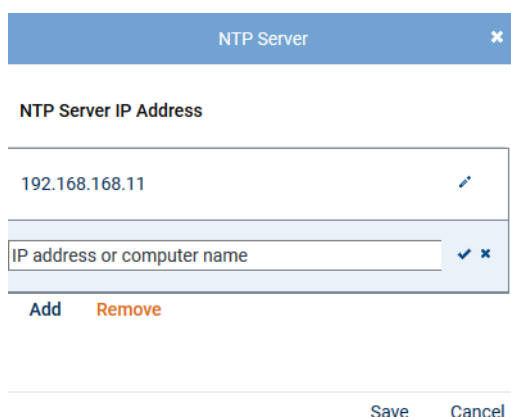





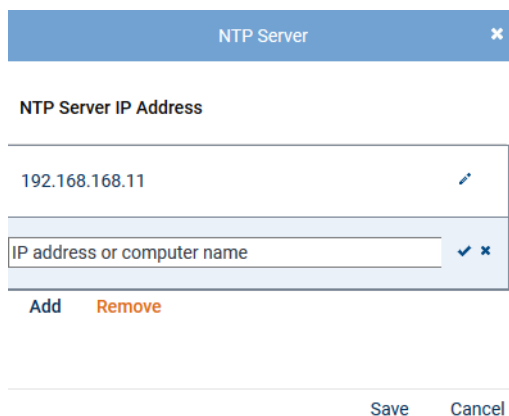
Fig. 44: Add NTP server

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

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




Edit IP address

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



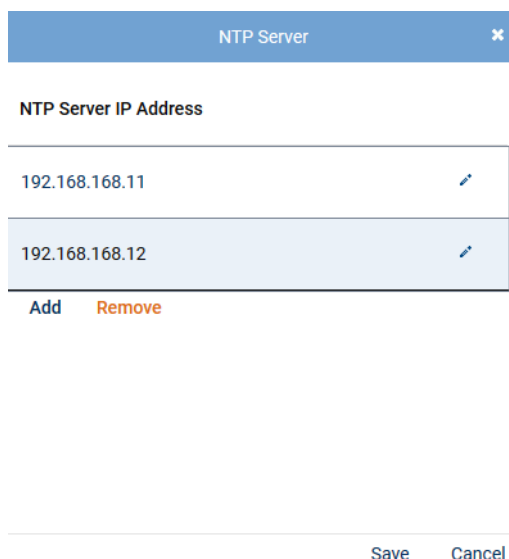
The screenshot shows a window titled "NTP Server" with a close button (X). Below the title is the section "NTP Server IP Address". It contains a table with one row showing the IP address "192.168.168.11" and an edit icon (pencil). Below the table is a text input field with the placeholder "IP address or computer name" and check/cancel icons. At the bottom are "Add" and "Remove" buttons. At the very bottom are "Save" and "Cancel" buttons.

Fig. 45: Edit IP address

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

Remove NTP server

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



The screenshot shows the "NTP Server" window with two rows in the "NTP Server IP Address" table. The first row has the IP "192.168.168.11" and an edit icon. The second row has the IP "192.168.168.12" and an edit icon. The "Add" and "Remove" buttons are at the bottom, along with "Save" and "Cancel" buttons at the very bottom.

Fig. 46: Remove NTP server

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

7.3.2.1.3 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:

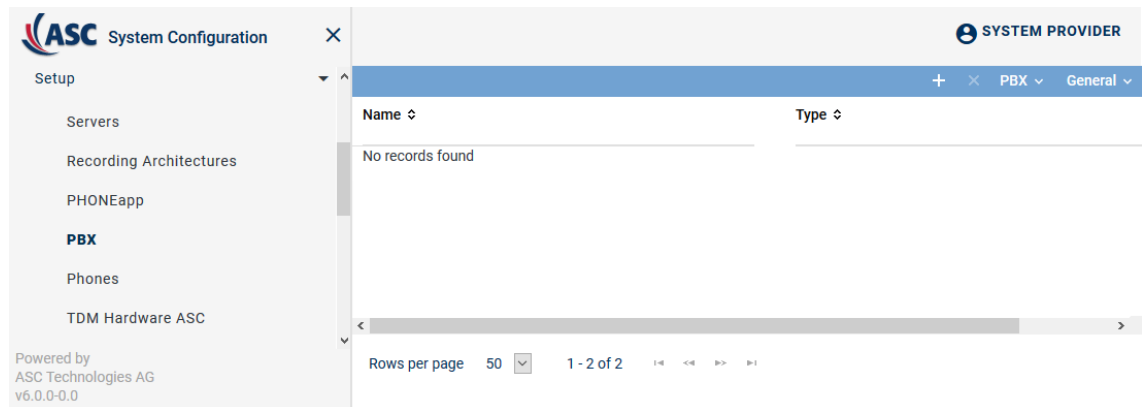




Fig. 47: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.



Fig. 48: Toolbar PBX module

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



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

Create new PBX

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

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

×

< Details* PHONEapp Configuration Web Service >

Name* Mitel MiVoice MX-ONE

PBX type* Mitel MiVoice MX-ONE ▼

Maximum length of extensions 4 ▼

Country code
☒ Select from list
United States (1) ▼

☐ Enter manually

Area code* 6021

Net code* 5963

Non Phone IPs

No records found

[Add](#) [Delete](#)

IPs to be Ignored

No records found

[Add](#) [Delete](#)

MACs to be Ignored

No records found

[Add](#) [Delete](#)

Save

Reset

Fig. 49: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 13: Create PBX

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

7.3.2.1.4 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.

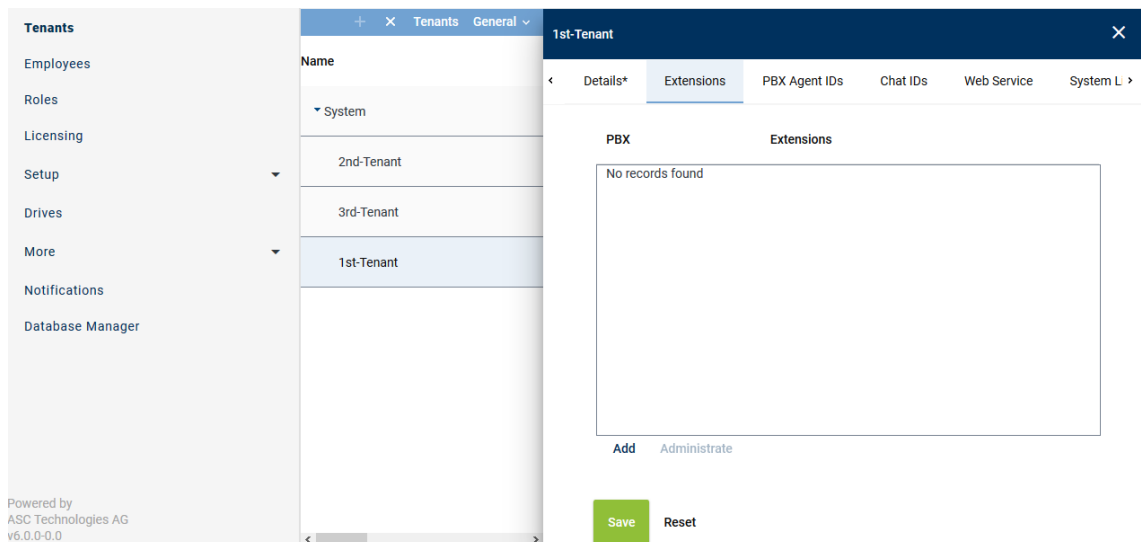


Fig. 50: Tenants - main view - tab Extensions

Add extensions

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

Add Extensions ✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 51: Assign extensions to tenants

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

<i>File import</i>	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The 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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p>

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

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

Remove extensions

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

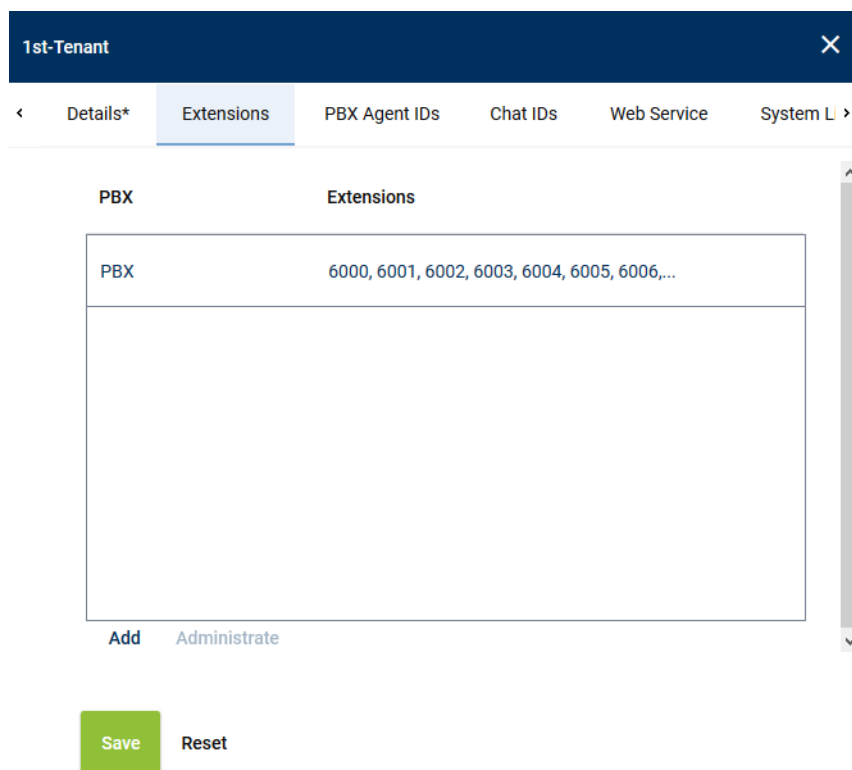


Fig. 52: Remove extensions

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. 53: 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.

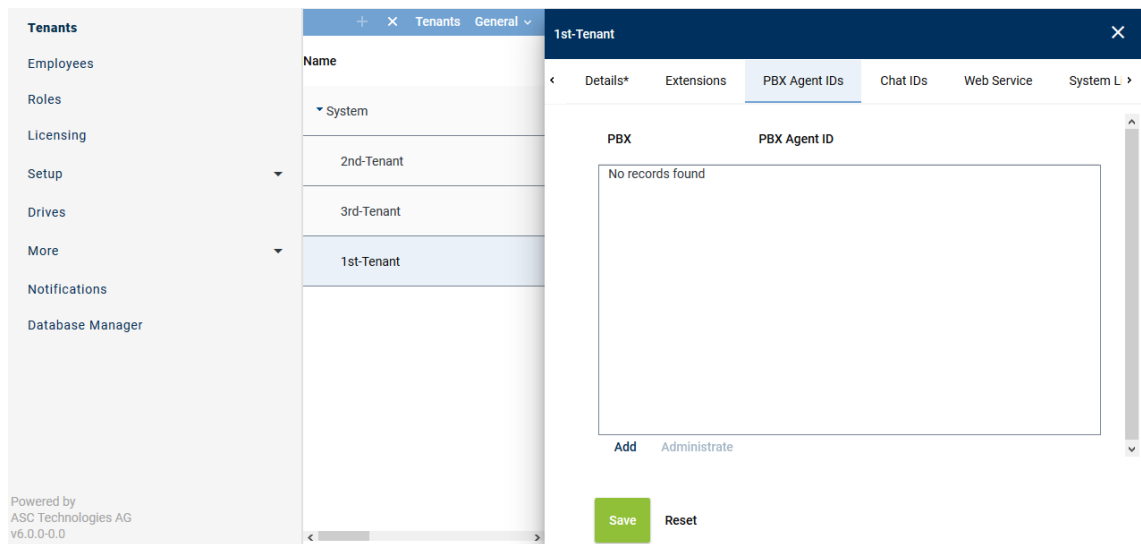


Fig. 54: Tenants - main view - tab PBX Agent ID

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:

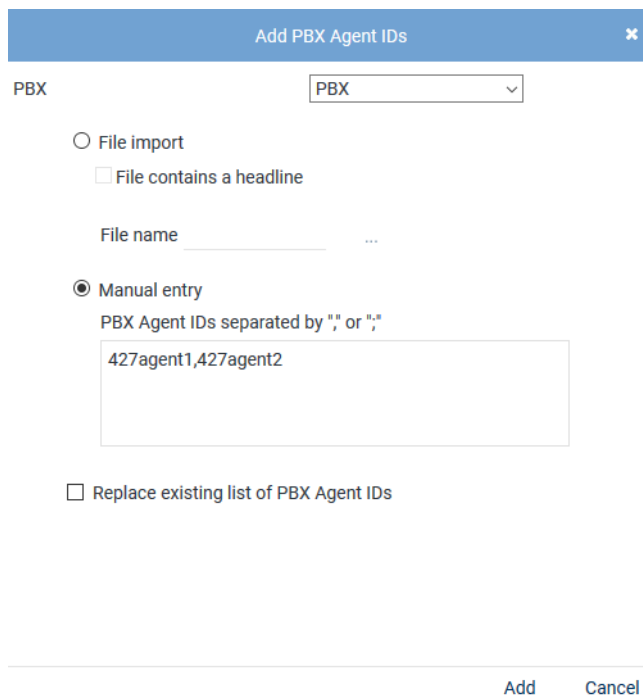




Fig. 55: Assign PBX Agent IDs to tenants

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

<i>File import</i>	Select this option to import the PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = 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.</p>

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

Remove PBX Agent ID

- In the list, select the **PBX** for which you would like to remove the assigned PBX Agent IDs.
- Click the button *Administrate*.
- 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.

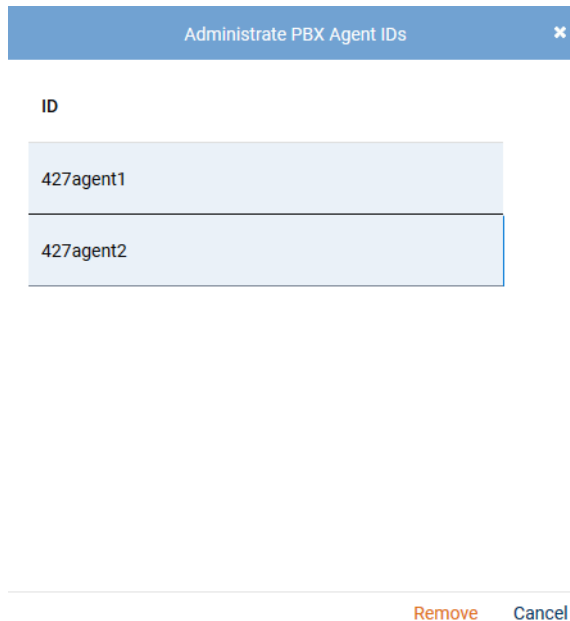


Fig. 56: Select PBX Agent IDs

- 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*.

7.3.2.1.5 Configure additional data

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

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

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

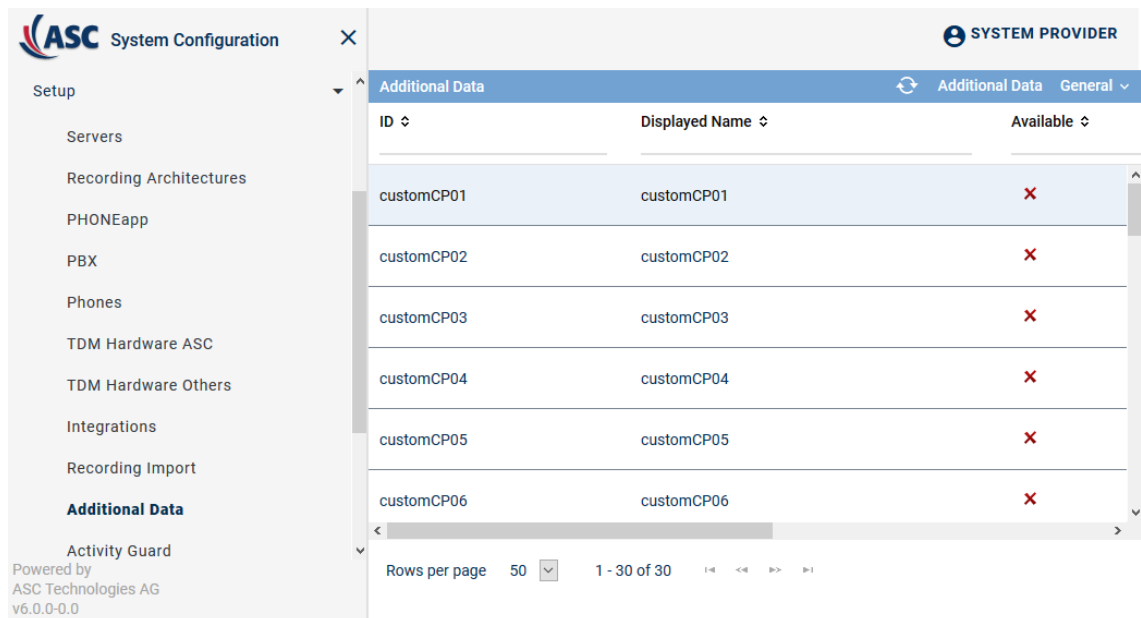


Fig. 57: Additional Data module main view

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

Change display name

Change Display Name
▼







Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 58: Configure additional data

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

Availability

Availability
▼

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

Save

Reset

Fig. 59: Additional data - configure availability

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



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



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

7.3.2.1.6 Create integration for All-in-one Failover

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

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

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

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

⇒ The following window appears:

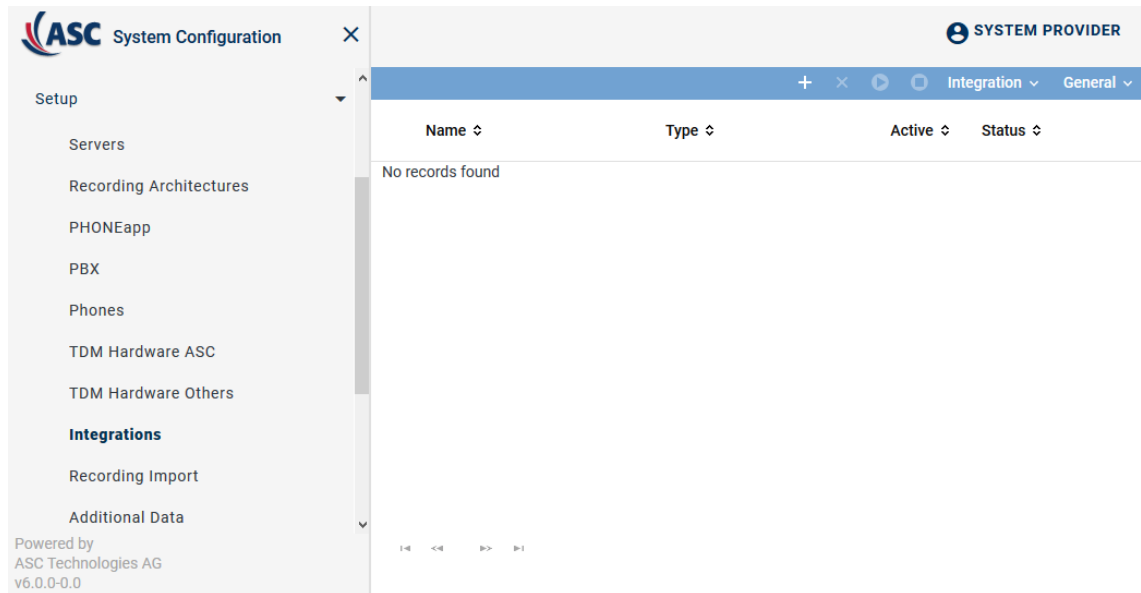




Fig. 60: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 61: Toolbar Integrations module

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

<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Import grammar

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

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

- To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.
⇒ The window *Upload File* appears.

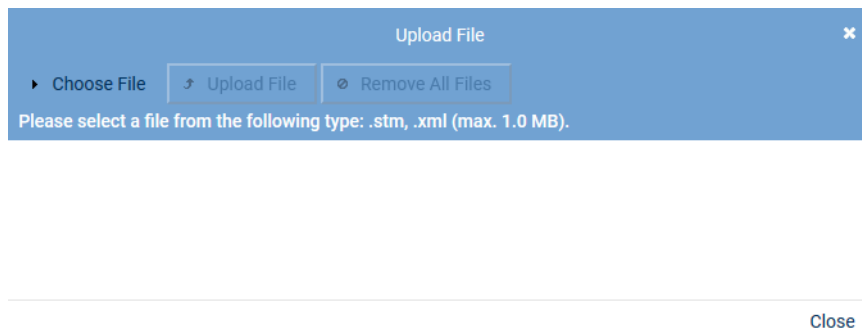


Fig. 62: Choose file

- Click on the button *Choose File*.
- Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
- Click on the button *Open*.
⇒ The selected file appears in the window *Upload File*.

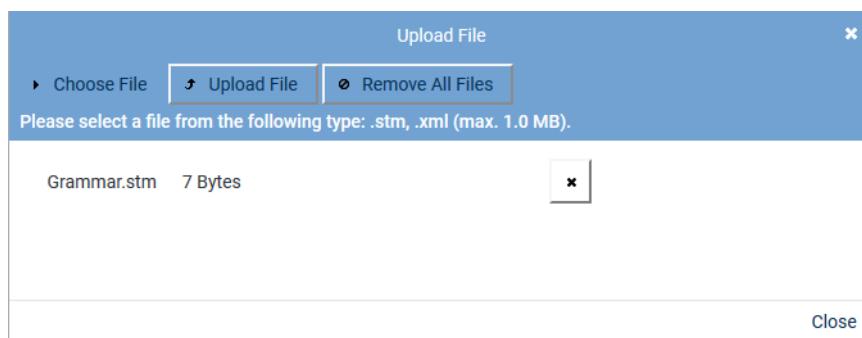



Fig. 63: Upload grammar

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

Assign integration type


- 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. 64: Create integration type

2. Enter the following parameters:

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

Tab. 14: Create integration type

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

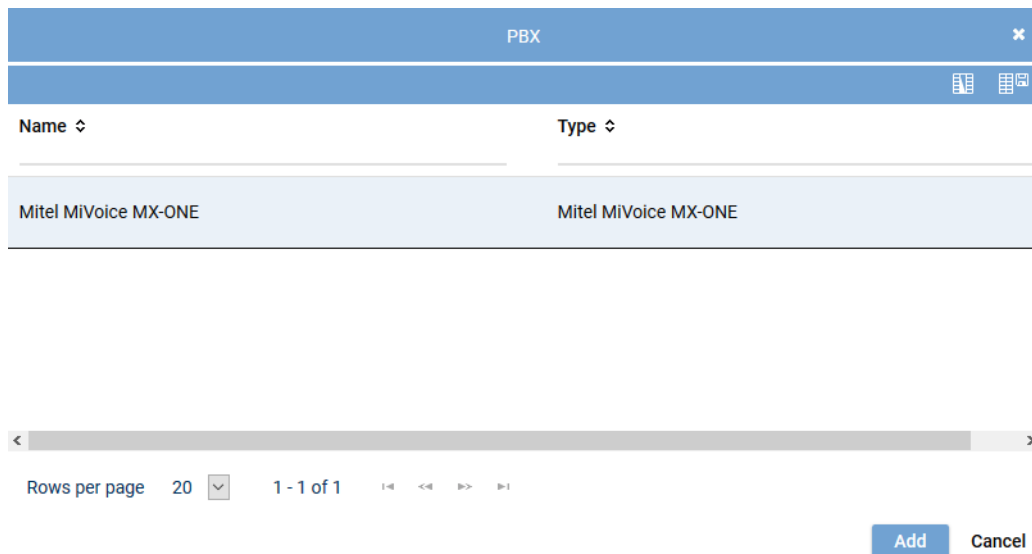



Fig. 65: Integrations - select PBX

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

Assign recording architecture for All-in-one Basic

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Basic

Save Cancel Back Next

Fig. 66: 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:









Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA		X	⚙️
Step	Configuration				
Configure recording architecture	✓				
Configure CTI connection data	X				
Configure monitor points	X				
Global recording settings	X				
Configure recording servers	X				
Configure add-on	✓				
Configure miscellaneous settings	✓				

Fig. 67: 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. 68: Configuration step - Configure Recording Architecture


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

Configure CTI connection data

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.

In this configuration step, you configure grammars, connection data, and - if required - additional data.

CTIconnect module

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.

⇒ In the detail view, the tabs *Module 1* and *Module 2* appear.



After an update, this section must be configured again.

Tab module 1

- Select the tab *Module 1* to configure the **CSTA** connection to the PBX.

By configuring module 1, you configure the recording type *Active Stream Recording* and/or *Intrusion*.

The **CSTA** connection is used to monitor the configured monitor points and to start the recording via the intrusion feature.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

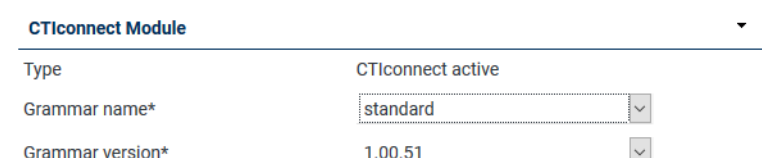


Fig. 69: Configure CTIconnect module

- Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 15: Configure CTIconnect module



After an update of the *neo* software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 1

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.

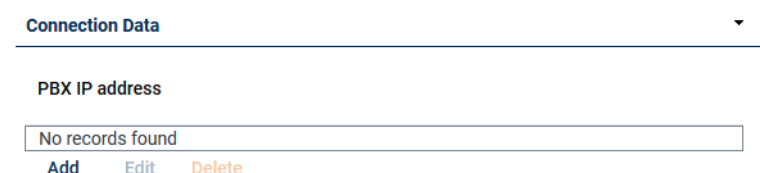


Fig. 70: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.



Fig. 71: Configure connection data

- Enter the following parameters:

Parameters	Value/Description
PBX IP address	Enter the IP address of the PBX.

Parameters	Value/Description
<i>PBX CSTA port</i>	Enter the port via which the CSTA connection is supposed to be run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate the check box to use the connection with TLS .

Tab. 16: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

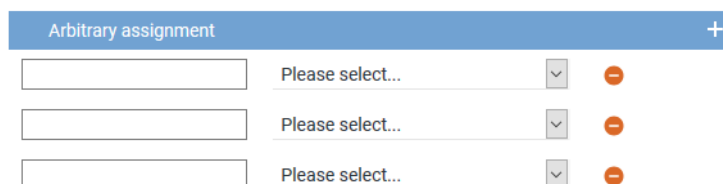



Fig. 72: Arbitrary assignment of the additional data

The following additional data are always available:

- *Start time*
- *End time*
- *Duration*
- *Calling Party Phone Number*

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

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



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



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

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

1. Here, you can configure how long to wait for the CTI~~connect~~ module to successfully connect with the PBX and how many connection attempts are to be made. If you have configured further connections, the system will switch to the next configured connection.



Only one CTI connection can be active at the same time. Connections cannot be established simultaneously.

Failover waiting time*	10
Failover repetitions*	3

Fig. 73: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI connect module attempts to establish another connection. Once this waiting time is over, new connection attempts are made depending on the configured number of failover repetitions.
<i>Failover repetitions</i>	Enter how many times the CTI connect module is supposed to try to establish a connection before switching to the next configured connection. The CTI connect module makes as many connection attempts as have been configured for the failover repetitions. For each connection attempt, the configured failover waiting time is observed. If all connection attempts for the first configured connection have failed, the system switches to the next configured connection.



When configuring a failover architecture, the configuration of the switching conditions for the **CTI** connections must be considered. If only the last of several configured connections is established, the waiting times and repeated connection attempts of the previous connections must be taken into account. If the overall failover time configured for the recording architecture is too short, then a system failover may be triggered even though there would be a **CTI** connection which could be established successfully.



After an update, this section must be configured again.

Automatic identification of the recording type

The recording type of an end device is identified by means of analyzing the "Switching Function Representation" determined by **CSTA** as well as by means of the intrusion flag set in the configuration of the monitor points. The regular expression which can be configured here serves to determine whether the end device with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (invitation) can be recorded. The "Switching Function Representation" is extracted from the **CSTA** information and interpreted on basis of the "Switching Function Representation Format" (N<DN!SA/EXT>NM). The NM section is checked by means of the regular expression. It is checked whether the end device type is contained in the expression. If the expression matches the NM section, then the above mentioned recording mode is used for this end device.

Regular expression for phone type identification*

```
^[A-Za-z]*\\s[0-9]{4}[a-zA-Z]?$|^([0-9]{4})[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 74: Configure regular expression for phone type identification

A sensible expression has been saved for the parameter; however, it may be necessary to adjust the parameter to support other phones.



When entering regular expressions, several characters must be added to form escape sequences so that the meaning remains intact when the software extracts them, see <https://docs.oracle.com/javase/tutorial/java/data/characters.html>. When they are not added to form escape sequences, a simple "\", for instance, will be filtered out internally. When reading them in again, "\s" will then be interpreted as "s" only. Thus, the regular expression will not work anymore after reading them in. To retain the required "\s" upon reading the expression in, an additional "\\" must be added in the file to read "\\s".



For further information about regular expressions see https://en.wikipedia.org/wiki/Regular_expression..



A short introduction on regular expressions and a test tool to check the functionality of regular expression can be found at <https://www.freeformatter.com/java-regex-tester.html>.

The recording type is determined in the following order:

- *Intrusion*
If the feature Intrusion has been activated by means of the GUI, it is used for recording.
- *Invitation Pattern*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type.
- *SRC*
If the regular expression does not match for the respective phone, recording is done via **SRC**.

Tab Module 2

1. Select the tab *Module 2* to configure the connection data of the [MBG](#).

By configuring module 2, you configure recording via the Mitel Border Gateway.

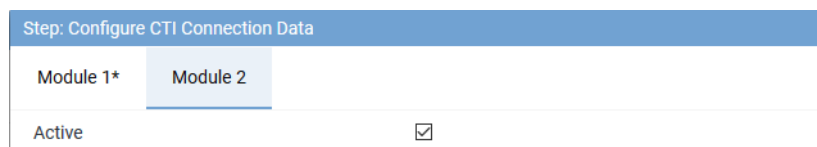


Fig. 75: Activate CTIconnect module 2

Active Tick the check box to display the configuration parameters and to activate the module.

☒ Module 2 has been activated.

☐ Module 2 has not been activated.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the [CTIconnect](#) module.

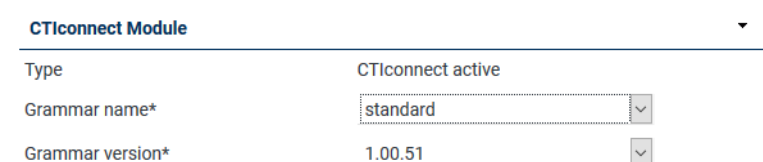


Fig. 76: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 17: Configure CTIconnect module



After an update of the [neo](#) software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 2

In this group field, you can configure the connection data to the [CTIconnect](#) module.

In case, the connection to the [CTIconnect](#) module fails, the recording with the recording variant via the [MBG](#) continues with restricted additional data. Phone numbers and direction continue to be available.

Connection Data ▼

Connection data

No records found

[Add](#)
[Edit](#)
[Delete](#)

Fig. 77: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

Configure Connection
✕

Connection data*	192.168.170.136
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>

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

Fig. 78: Configure connection

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the connection data to the MBG or the SRC .
<i>PBX port</i>	Enter the port via which the MBG connection is supposed to run default <i>6810</i> .
<i>Activate indirect recording</i>	This option must not be activated for this type of recording.

Tab. 18: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

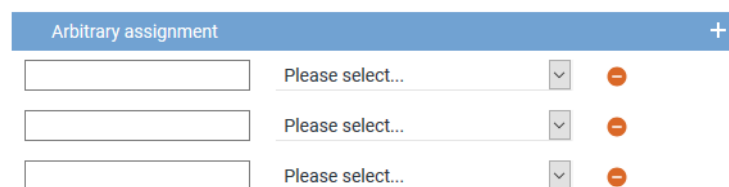



Fig. 79: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure monitor points

In this configuration step, the monitor points for the monitored end devices are configured.

1. In the main view in the line *Configure monitor points*, click on the button  (*Edit configuration step*).
⇒ The window *Step: Configure Monitor Points* appears in the detail view.

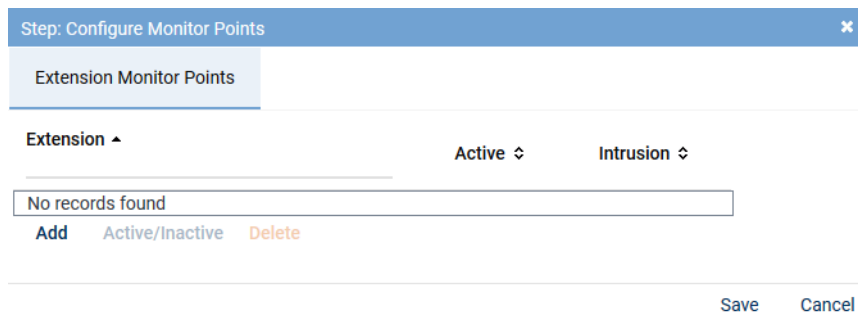


Fig. 80: Configuration step - configure monitor points

Extension monitor points



For the recording variant with **MBG** or **SRC**, the phones to be recorded must have been registered in the **SRC**. This does not apply to the recording variant with SIP Invite or Intrusion.

1. In the tab *Extension Monitor Points*, click on the button *Add* to add the extensions for the monitored end devices.
2. Select the menu item *Enter Extensions*.
⇒ The window *Add Extension Monitor Points* appears.

Add Extension Monitor Points
✕

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry





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

6000-6006

☐ Replace existing list of extensions

Add
Cancel

Fig. 81: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
	<p>File contains a headline</p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p>

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

☒ = Function has been activated; all assignments of the PBXs which are listed in the detail view are overwritten and only the new assignment is applied.

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

3. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
4. If errors have been detected, the window *Result* appears.
Click on the button *Display Error Report* to open the window *Error Report*.
To close the window *Error Report*, click on the button *Close*.
To close the window *Result*, click on the button *Close*.
5. The configured extensions now appear in the detail view.

Step: Configure Monitor Points ✕

Extension Monitor Points

Extension ▲	Active ⇅	Intrusion ⇅
6000	✓	<input checked="" type="checkbox"/>
6001	✓	<input checked="" type="checkbox"/>
6002	✓	<input type="checkbox"/>
6003	✓	<input type="checkbox"/>
6004	✓	<input type="checkbox"/>
6005	✓	<input type="checkbox"/>
6006	✓	<input type="checkbox"/>

Add
Active/Inactive
Delete

Save
Cancel

Fig. 82: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Delete To delete extension monitor points, select the respective extension in the list and click on the button *Delete*. To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Intrusion To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column *Intrusion*.

☒ = Intrusion feature has been activated.

☐ = Intrusion feature has not been activated.

6. Click on the button *Save* to apply the settings and to finish this configuration step.



An extension which is supposed to be monitored and recorded by means of intrusion must be configured in the PBX to send an engaged signal if it is in a conversation. Only then, can the CTI~~connect~~ service initiate an intrude call and a silent conference.

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 15](#).

Global recording settings

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.

Step: Global Recording Settings

Details

Transport protocol	TCP	
Port SIP signaling*		5060
Remote SIP port*		7300
Activate SIP authentication	<input checked="" type="checkbox"/>	
User name for the SIP registration	#Extension	
Password for the SIP registration	••••••••	
Activate PBX connection	<input checked="" type="checkbox"/>	
SIP registration expiration*		3600
PBX IP address*	192.168.170.219	
PBX port*		5060

Save
Cancel

Fig. 83: Configuration step - Global Recording Settings

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

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

Parameter	Value/Description
	UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling. On this port, the recording server can reach the Mitel end devices for the Active Streaming Recording by means of SIP to start the recording. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices, default 7300.
<i>Activate SIP authentication</i>	Activate the check box if the SIP registration is supposed to be authenticated. The option <i>Activate SIP authentication</i> is only used together with or as an expansion of the option <i>Activate PBX connection</i> .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration for the recording of the extensions used with the intrusion feature. The user name is configured in the PBX and applies for all extensions to be registered.
<i>Password of the SIP registration</i>	Enter the password for the SIP registration for the recording of the extensions used with the intrusion feature. The password is configured in the PBX and applies for all extensions to be registered.
<i>Activate PBX connection</i>	Activate the check box if you would like to use the intrusion feature. When this option has been activated, the configured extensions of the recording server are registered on the PBX. Once the check box has been activated, the following parameters become active to be configured.
<i>SIP registration expiration</i>	Enter the period in seconds until the registration runs out.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port for the communication with the PBX, default 5060.

Tab. 19: Global recording settings

- Click on the button **Save** to apply the settings and to finish this configuration step.



After an update, this section must be configured again.

Configure add-on



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

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



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

Configure add-on for MiContact Center Enterprise

The add-on refers to the usage of MiContact Center Enterprise and must only be configured if MiContact Center Enterprise is used.

The integration runs in combination with the PBX and the recording server which is responsible for the actual conversation recording. The conversation events and the additional data are captured via MiContact Center Enterprise and sent to the recording server.

1. Select the add-on *MiContact Center Enterprise* in the detail view.

Step: Configure Add-on

Details *

Select add-on
☐ None
☒ MiContact Center Enterprise

CTIconnect Module

Type CTIconnect passive
Grammar name* standard
Grammar version* 2.00.01

Connection Data

Server name* 192.168.170.205
Port* 2601

Additional Data

CALLID Universal Call ID
PRIVATEDATA Please select...
SERVICEGROUPID Please select...
SERVICEGROUPLIST Please select...
IVRDATA1 Please select...
IVRLABEL1 Please select...
IVRDATA2 Please select...
IVRLABEL2 Please select...
IVRDATA3 Please select...
IVRLABEL3 Please select...
OASID Please select...

Arbitrary assignment +

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

Save Cancel

Fig. 84: Configure add-on for MiContact Center Enterprise

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 20: Configure CTIconnect module

Group field Connection Data

1. Set the following parameters in the group field *Connection Data*:

Parameter	Value/Description
<i>Server Name</i>	Enter the IP address or the name of the server that the MiContact Center Enterprise runs on.
<i>Port</i>	Enter the port for the connection to MiContact Center Enterprise.

Tab. 21: Configure connection data

Group field Additional Data

The following additional data is delivered in the protocol when using MiContact Center Enterprise:

- *CALLID*
- *PRIVATEDATA*
- *SERVICEGROUPLIST*
- *IVRDATA1*
- *IVRLABEL1*
- *IVRDATA2*
- *IVRLABEL2*
- *IVRDATA3*
- *IVRLABEL3*
- *OASID*

Arbitrary assignment

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



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

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



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

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

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

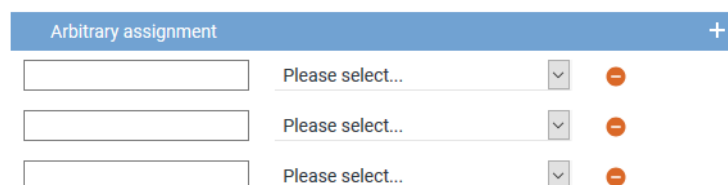



Fig. 85: Arbitrary assignment of the additional data

The following additional data are always available:

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

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



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



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

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI~~connect~~ service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

CTIconnect for Genesys T-Server

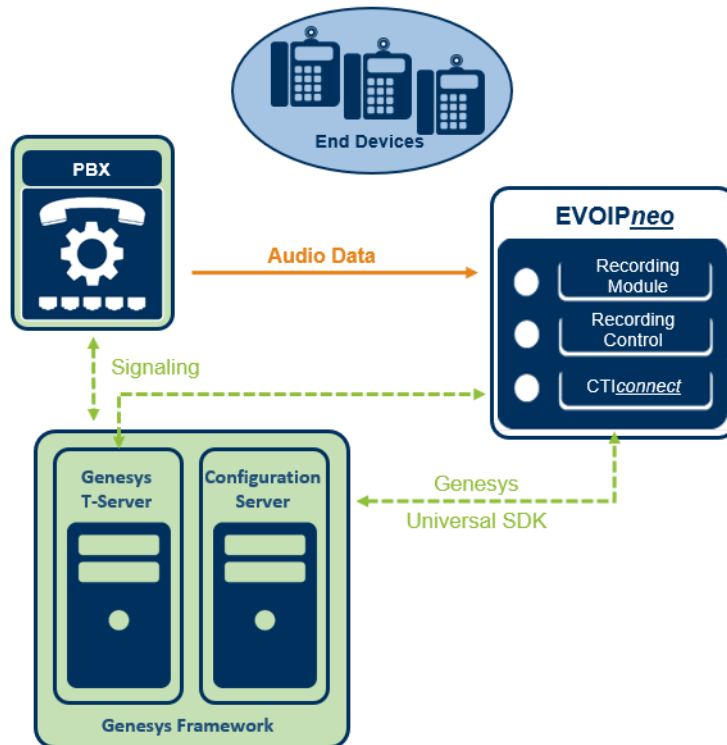


Fig. 86: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 311](#).

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.



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

When using a CTIconnect for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.


By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

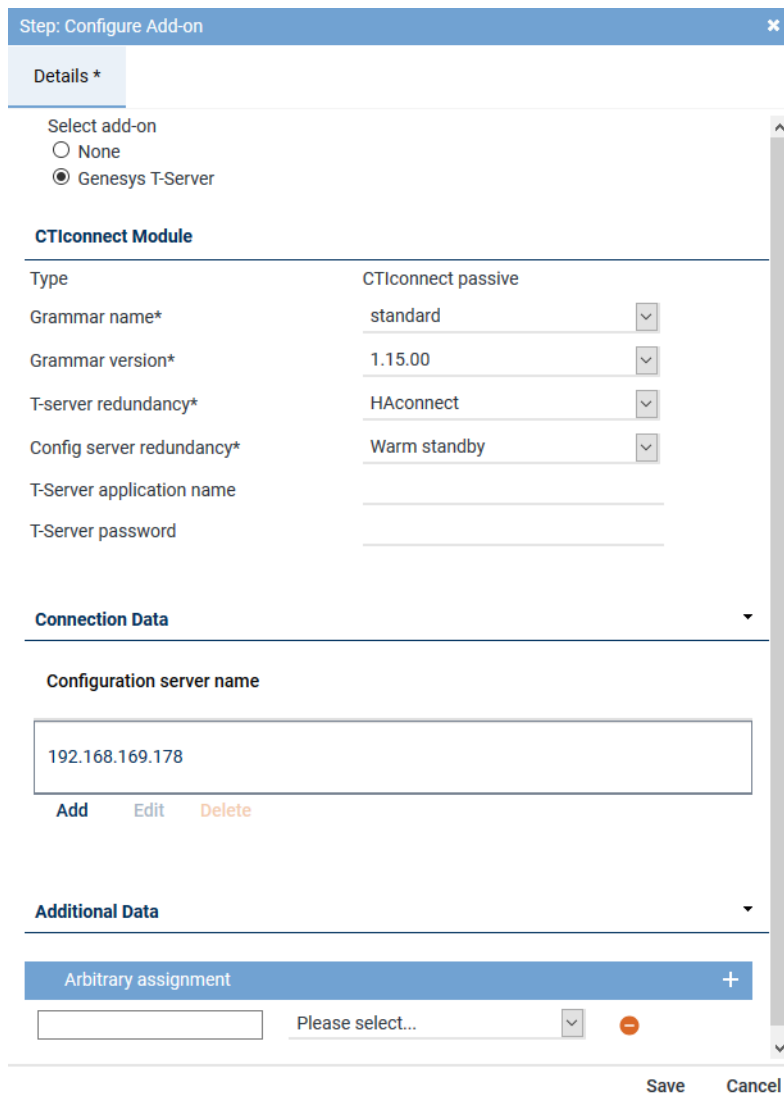
Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path
C:\ASC Product Suite\data\CTIConnectForGenesysT\.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button  (*Edit configuration step*) in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type CTIconnect passive

Grammar name* standard

Grammar version* 1.15.00

T-server redundancy* HAconnect

Config server redundancy* Warm standby

T-Server application name

T-Server password

Connection Data

Configuration server name

192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment

Please select...

Save Cancel

Fig. 87: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 22: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

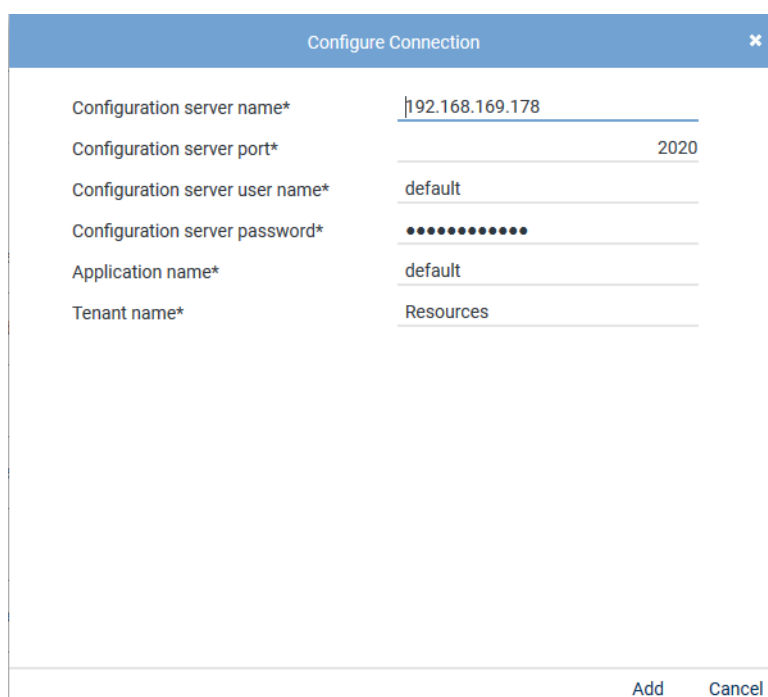


Fig. 88: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.

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

Tab. 23: Configure connection data

Group field Additional Data

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

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



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

Arbitrary assignment

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



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

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



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

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

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

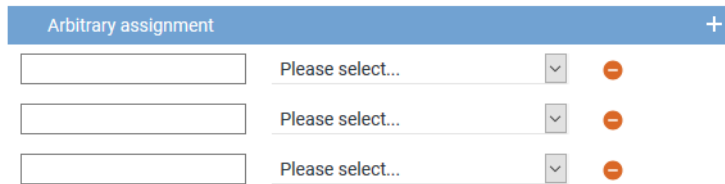



Fig. 89: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure miscellaneous settings

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

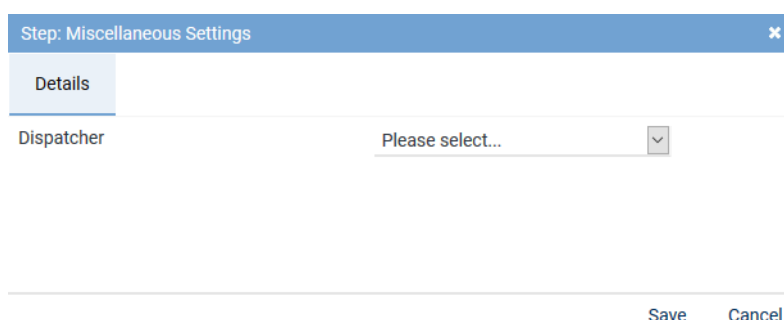


Fig. 90: Configure miscellaneous settings

2. Enter the following parameter:


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





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

Activate integration

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

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

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

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





















	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		
Step		Configuration		
Configure recording architecture				
Configure CTI connection data				
Configure monitor points				
Global recording settings				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 91: Activate integration

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








    Integration ▾ General			
Name ▾	Type ▾	Active ▾	Status ▾
	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	 

Fig. 92: 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.



For updates, the integration is stopped and deactivated. Once the update has been completed successfully, you must configure the integration again. Once the configuration has been completed, start the recording architecture again and activate the integration so that the new configuration is applied.

Deactivate/Delete integration

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

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







+ ×   Integration ▾ General			
Name ↕	Type ↕	Active ↕	Status ↕
 Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		

Fig. 93: Deactivate integration

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

7.3.2.2 Configure recording solution All-in-one Failover

7.3.2.2.1 Create recording architecture

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

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

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

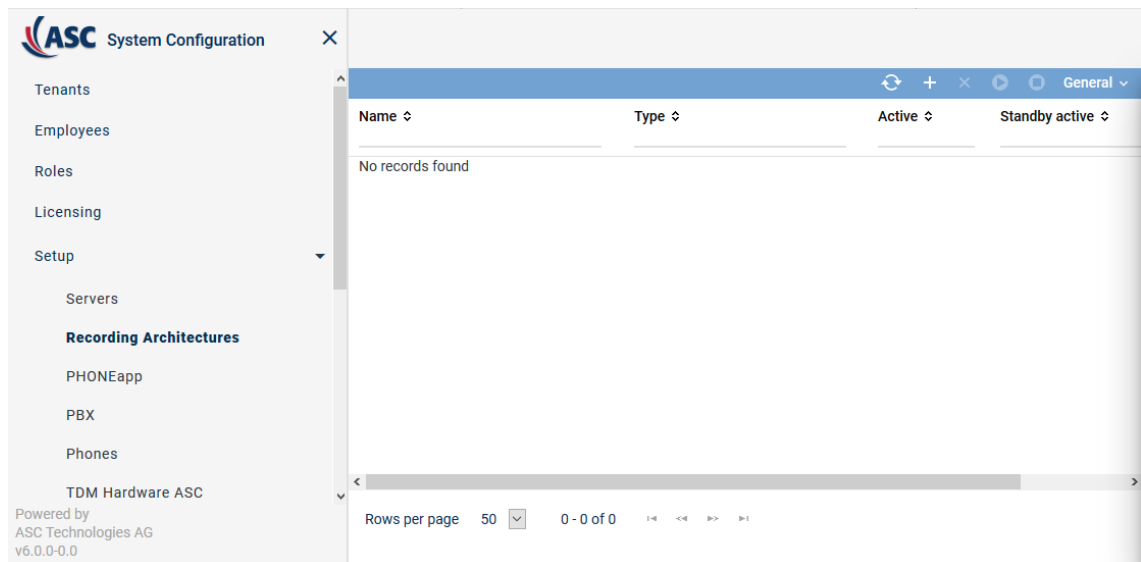





Fig. 94: Recording architectures - main view

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

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

Create recording architecture All-in-one Failover

If a standby recording server is supposed to take over recording in case of an error, you have to create a recording architecture of the type *All-in-one Failover*.

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

⇒ The window *New Recording Architecture* appears.

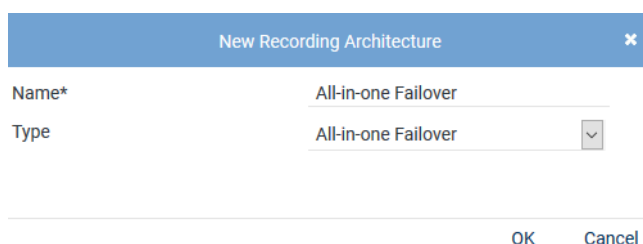


Fig. 95: Create recording architecture - All-in-one Failover

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 Failover*.
NOTICE! The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.
⇒ Your entries now appear in the detail view.

All-in-one Failover
All-in-one Failover ✕

Details*

Server Assignment*

[? Help](#)

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

Integration Type
☰ + ☰ -

Name
No records found

Save


Reset

Fig. 96: Recording architecture - tab Details - All-in-one Failover

As standby components may have been configured for the active recording server, a failover timeout may be configured in this recording architecture. For further information about failover architectures, see [chapter "Standby management for failover architectures"](#), p. 284.

<i>Failover timeout</i>	<p>Enter a timeout of a minimum of 15 seconds after which the failover process is supposed to start. Depending on the system architecture it may make sense to configure a longer timeout period. The timeout defines the elapse time until the failover process starts. If the status returns to <i>OK</i> within this time, then the failover process is not triggered.</p> <p>NOTICE! Check these parameters after an update and set the timeout to 15 seconds, if required.</p>
<i>Activate standby failover</i>	<p>Activate this option if you would like to ensure that the system switches back to the primary server in case of an error of the standby server.</p> <p>NOTICE! There is no check whether the primary database is working properly before switching back. As a result it is possible that both databases are in an undefined state.</p> <p>NOTICE! After switching back to the original primary server from the standby server, this option is deactivated. If the switching process is supposed to be carried out automatically in the event of a new error, you must activate this option again.</p>
<i>Active</i>	Shows the status of the recording architecture.

Add integration type

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

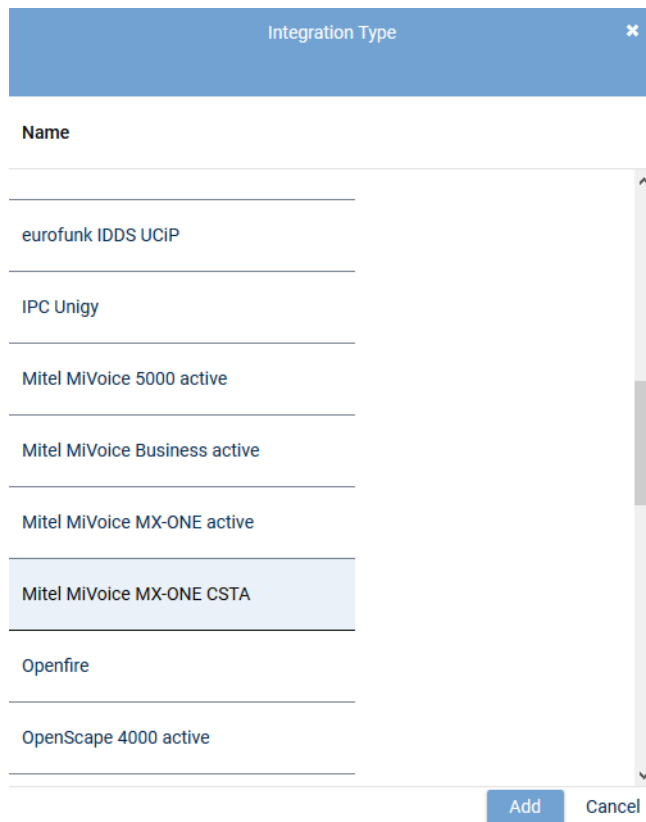


Fig. 97: Select integration type



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



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

- Select *Mitel MiVoice MX-ONE CSTA* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign servers for All-in-one Failover Recording

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

All-in-one Failover

All-in-one Failover

✕

Details*

Server Assignment*

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

Save

Reset

Fig. 98: Recording Architecture - tab Server Assignment

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

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

Fig. 99: Recording Architecture - assign server - example


3. Select the *primary* server.



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

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

- Click on the button *Add*.
⇒ The name of the server now appears in the detail view.

5. To delete an assignment, click on the button .
6. Repeat the steps and select the server which is supposed to be use in case of an error failover operation in the entry field *Standby server*.
7. Select the recording type you would like to use for these servers by activating the check box.

Recording type

☒ VoIP/Video

☒ TDM

☒ Screen

☒ Chat




Fig. 100: Recording Architecture - activate recording type



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

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

Activate recording architecture

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










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

Fig. 101: 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.



For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See [chapter "Standby management for failover architectures", p. 284](#).



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

7.3.2.2.2 Configure servers

Every server in your network that the *neo* software has been installed on is automatically identified as a server of the recording system and displayed in the main view of the Servers module. In the Servers module, you can configure the usage of the servers in your recording system.

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

⇒ The following window appears:

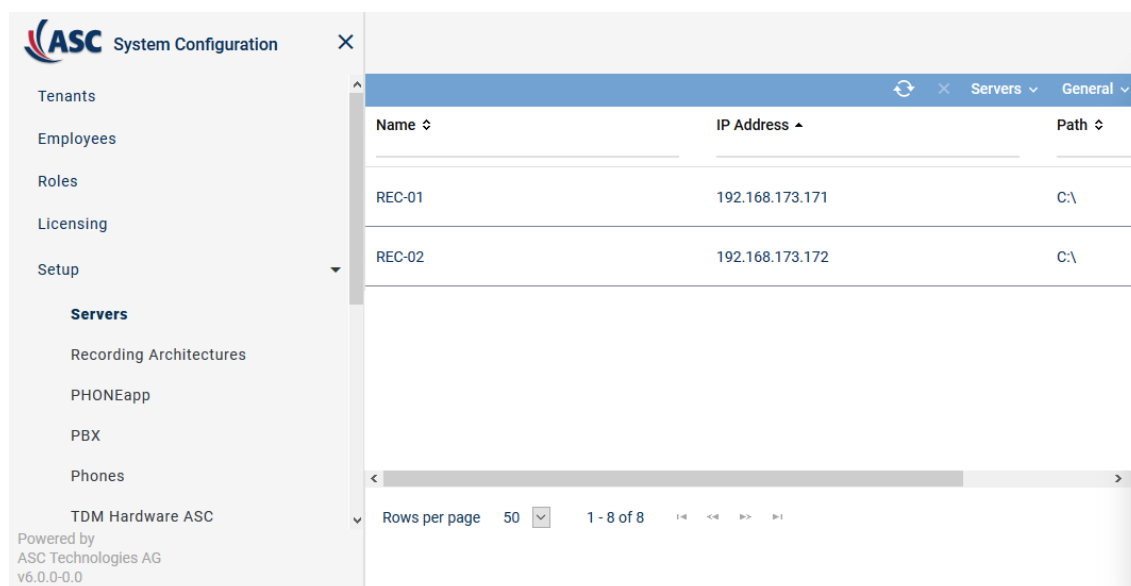


Fig. 102: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	Date on which the settings of the server were updated for the last time.

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

Toolbar of the Servers module

The toolbar offers the following functions.

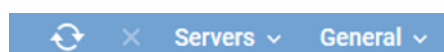




Fig. 103: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Delete</i>	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations" , p. 91.

	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see chapter "Administrate NTP server", p. 108 .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>Save Table Configuration</i>	Saves the current table configuration of the main view as default view of the user.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
	<i>Reset Search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



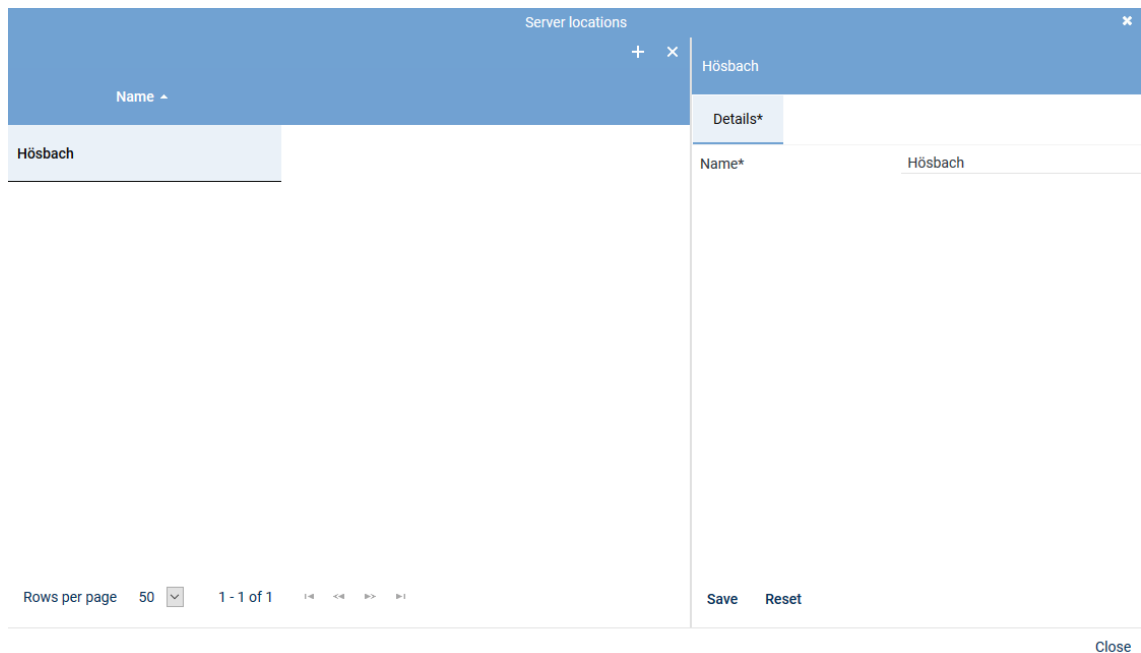
For detailed information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

Administrate server locations

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


Add server locations

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



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

Fig. 104: Add server locations

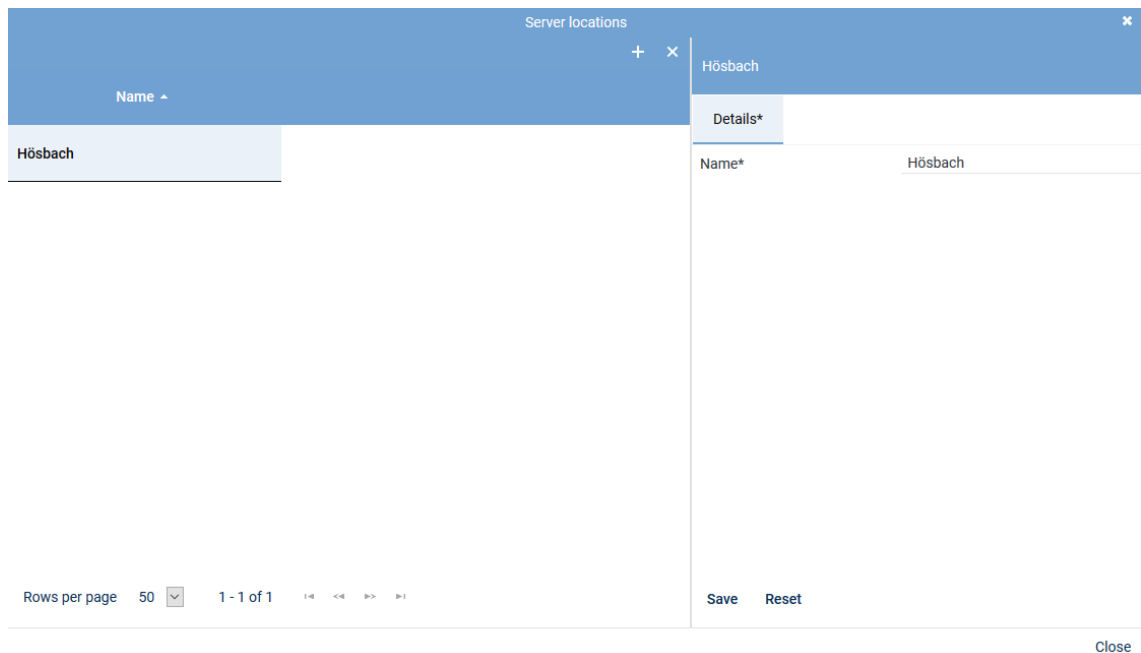
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

Delete server location



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

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



Server locations

Name
Hösbach

Details*


Name* Hösbach

Rows per page 50 1 - 1 of 1

Save Reset

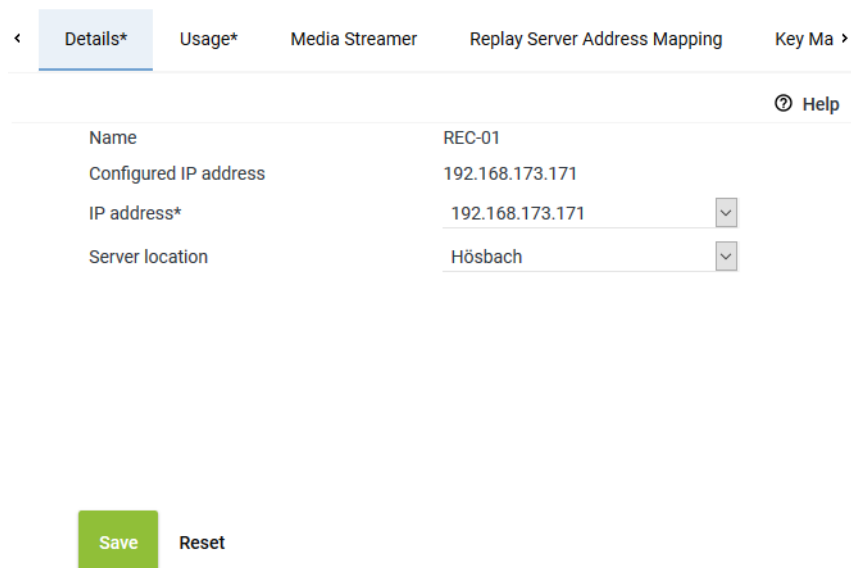
Close

Fig. 105: Delete server location

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

Tab Details

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



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

Help

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

Save Reset

Fig. 106: Servers - tab Details

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

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

Tab Usage

1. Click on the tab *Usage* to configure the purpose of usage.



Since a server can be used for several recording solutions, all purposes of use are listed. Note that some purposes of use do not apply for some recording solutions. As an example: You cannot use audio analysis or replay via phone in a chat recording.

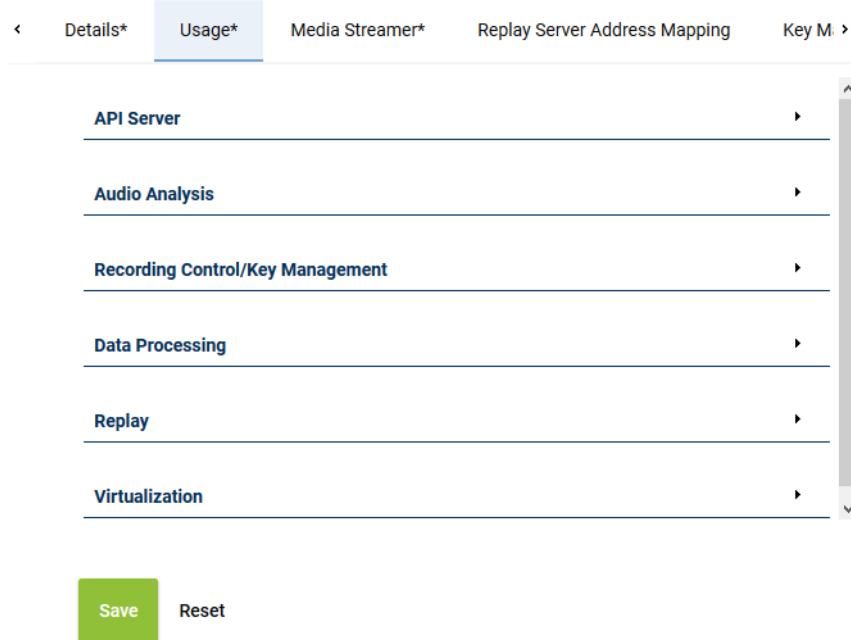


Fig. 107: Servers - tab Usage

Group field API Server

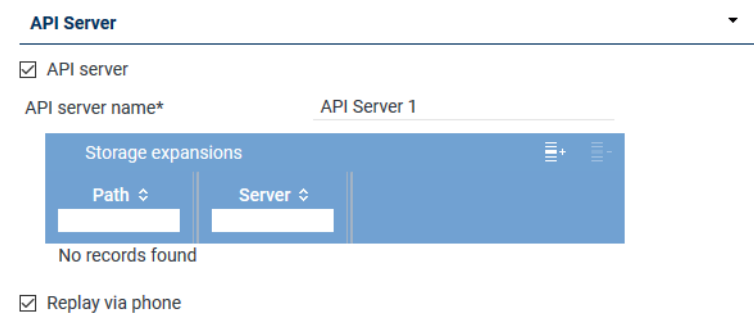


Fig. 108: Group field API Server



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



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


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

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

Parameter	Value/Description
<i>API server</i>	<p>Tick the check box to start the API server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>In order to be able to reach the API server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 104.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List</i> <i>Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the storage expansions, see chapter "Add storage expansion for replay", p. 96. By clicking on the icon  (<i>Remove</i>), you can remove the storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> Application POWERplay<i>play</i> Pro Application POWERplay<i>play</i> Instant Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p>

Parameter	Value/Description
	NOTICE! In the tab <i>Media Streamer</i> , you have to assign this function to a PBX , see chapter "Tab Media Streamer", p. 103 . 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.

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

Rows per page 20 1 - 1 of 1

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

Fig. 109: Select storage expansion

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

Group field Audio Analysis

Audio Analysis


☒ Audio analysis (SAES mode)

Stream audio data from* + -

☐ Emotion detection

Stream audio data from* + -

Fig. 110: Group field Audio Analysis

Parameters	Value/Description
<i>Audio analysis</i>	Activate this check box to use the server for audio analysis. The audio data is then streamed for audio analysis from the configured server to this server. <ul style="list-style-type: none"> Stream audio data from From the list of available servers, select the server from which the audio data is supposed to be streamed for audio analysis via the button .

Parameters	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for the audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>

Tab. 24: Configure audio analysis

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☒ Recording control/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 111: Group field Recording Control/Key Management

Parameters	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <u>CLIENT</u><i>command</i> or an API recording control or if you would like to use <i>Monitoring</i>. This feature is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the respective recording architecture you would like to use for the control.
- <u>neo</u> key management	<p>The function allows customer-specific encryption of the recordings. To be able to configure the key management, you have to activate the check box <i>Key management</i>.</p> <p>This function can only be activated if the license <code>ASC_KEY_MANAGEMENT</code> is available.</p> <p>For further information about the configuration of the key management refer to the administration manual <i>Configuration of servers and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 25: Configure Recording Control/Key Management

Group field Data Processing

Data Processing ▼

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

from 11:59:36

to 11:59:36

Receives data from

Name	Only Replay
No records found	



☒ Archiving





☒ Export

☒ Import

Recording architecture Please choose... ▼


Fig. 112: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	Activate the check box to allow the modification of the additional functions of data processing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 99. By clicking on the icon  (<i>Remove</i>), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 99. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which the function <i>Data Storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<i>Export</i>	Activate the check box <i>Export</i> to allow the export from this server.
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 26: Configure data storage

Add target server to a list

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



Target Server

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

Rows per page 20 1 - 6 of 6

Add Cancel

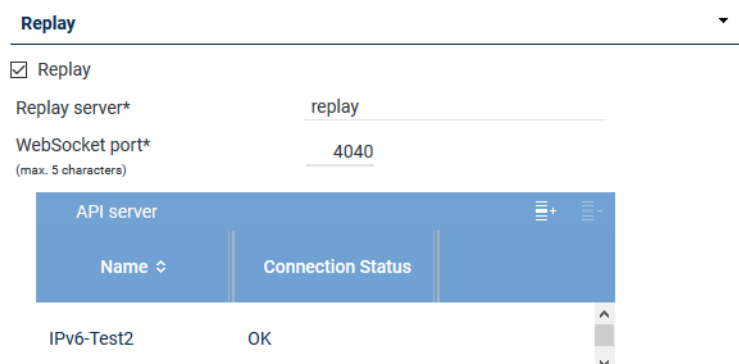
Fig. 113: Select server



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

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

Group field Replay



Replay

☒ Replay



Replay server* replay

WebSocket port* 4040
(max. 5 characters)

API server	
Name ↕	Connection Status
IPv6-Test2	OK

Fig. 114: Group field Replay

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

Parameter	Value/Description
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port (maximum of 5 characters)</i>	Enter the port via which the data to be replayed in <i>POWERplay</i> Web are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 101. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 27: Configure replay


Search and replay functions



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

Add API server to a list

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

- If the replay server runs on a server with a local [API](#) server, it must not necessarily be assigned as the replay server always addresses the local [API](#) server first.
 - If the replay server runs on a separate server, you must assign at least one [API](#) server that the replay server can address.
 - If several [API](#) servers are available in the network, you can assign further [API](#) servers in addition to the local [API](#) server. The assigned [API](#) servers are addressed in order. For this reason, the local [API](#) server should always be first in the list.
- To assign an [API](#) server, click on the icon  (*Add*) in the toolbar of the list *API Server*.
 - Select the server from the list on which the [API](#) service is running.




Fig. 115: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 94](#).

- 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. 116: Group field Virtualization

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

Tab. 28: 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.

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

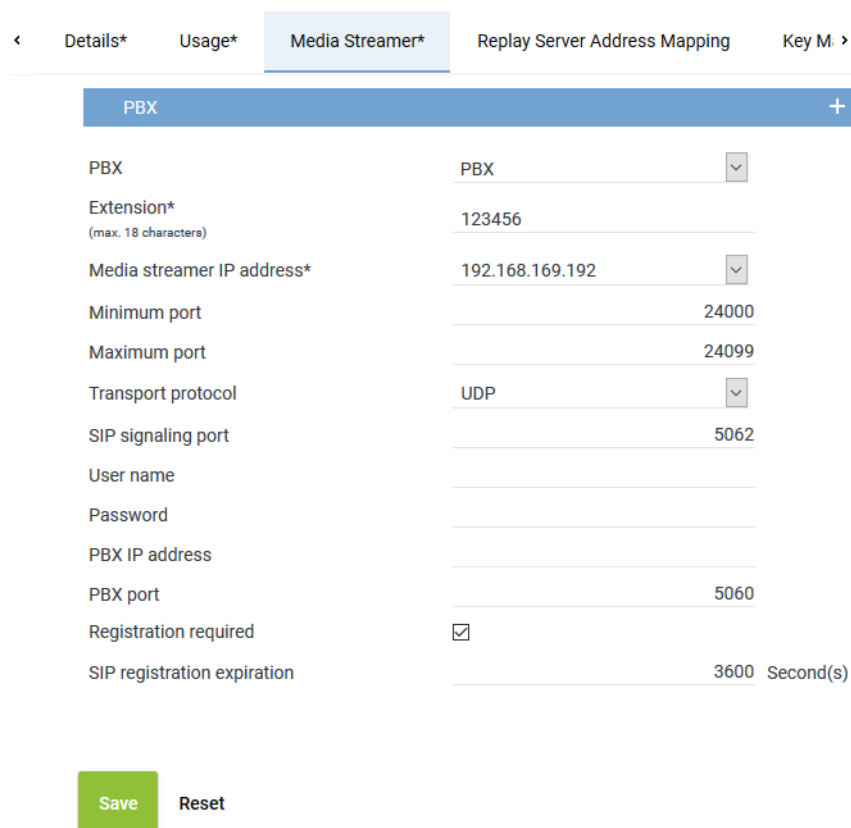
Tab Media Streamer

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

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



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



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

PBX +

PBX PBX
 Extension* 123456
(max. 18 characters)

Media streamer IP address* 192.168.169.192
 Minimum port 24000
 Maximum port 24099
 Transport protocol UDP
 SIP signaling port 5062
 User name
 Password
 PBX IP address
 PBX port 5060
 Registration required ☒
 SIP registration expiration 3600 Second(s)

Save Reset

Fig. 117: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX, see chapter "Create PBX", p. 109.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. In the drop-down list, all IP addresses of the server are displayed.</p> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</p>

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

Tab Replay Server Address Mapping

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

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



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

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

Replay Server Addresses
✖

Internal IP address/ port of the replay server
 : 4000

External address/ port of the replay server
 : 4000

Save
 Reset

Fig. 118: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



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

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



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



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

Tab Key Management

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

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

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

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage

until

0 Day(s)

0 Hour(s)

☐ Key expiration date

after

0 Day(s)

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

Save

Reset

Fig. 119: Servers module - tab Key Management

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

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

In case of an error ... automatically

Select whether simple key management is supposed to be used if the neo key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the neo key management has been activated but does not work.

☒ = In case of an error, simple key management is used as replacement.

☐ = In case of an error, no recording takes place as long as the neo key management has been activated. In this case, disable key management in the tab *Usage*.



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



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

Tab Keystore/Virtualization

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

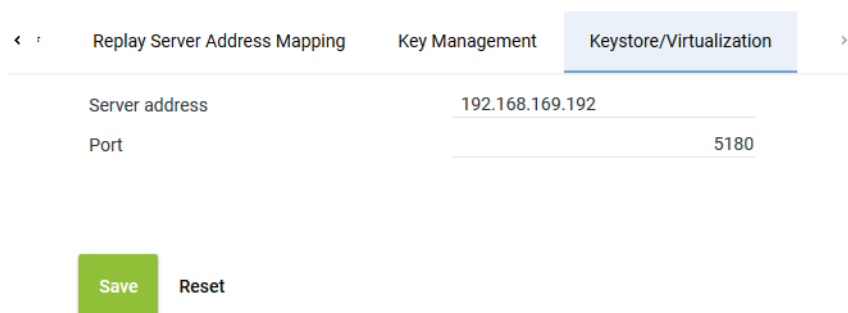
In this tab, you can configure the connection data for the service *DongleMan* for the neo key management and for the authentication of the VM.



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*.



Navigation: < Replay Server Address Mapping | Key Management | **Keystore/Virtualization** >

Server address	192.168.169.192
Port	5180

Buttons: Save (green), Reset

Fig. 120: 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

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

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

Administrate NTP server

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

Add NTP server

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

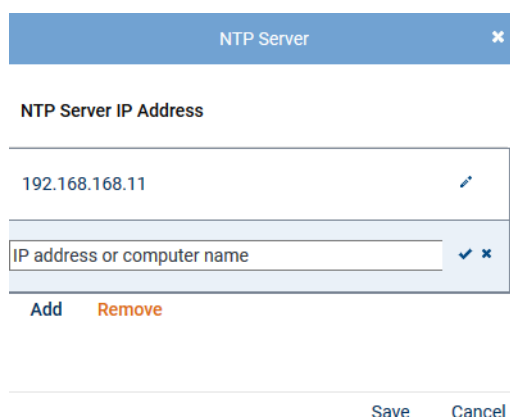





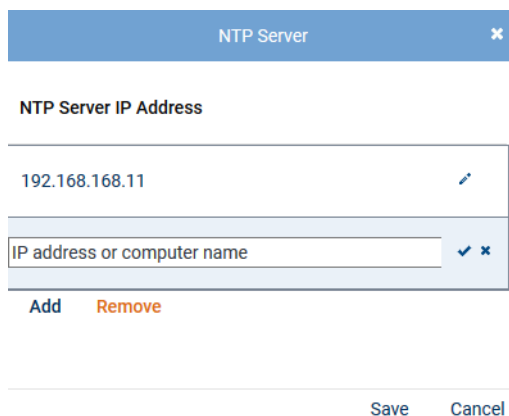
Fig. 121: Add NTP server

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

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




Edit IP address

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



NTP Server




NTP Server IP Address

192.168.168.11	
IP address or computer name	 

Add Remove

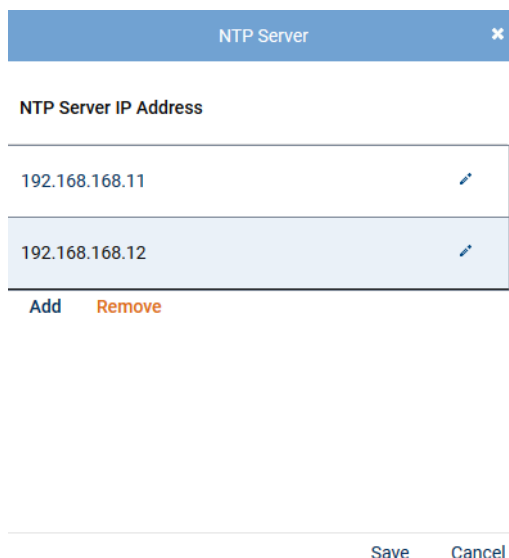
Save Cancel

Fig. 122: Edit IP address

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



Remove NTP server

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



NTP Server

NTP Server IP Address

192.168.168.11	
192.168.168.12	

Add Remove

Save Cancel

Fig. 123: Remove NTP server

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

7.3.2.2.3 Create PBX

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

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

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

⇒ The following window appears:

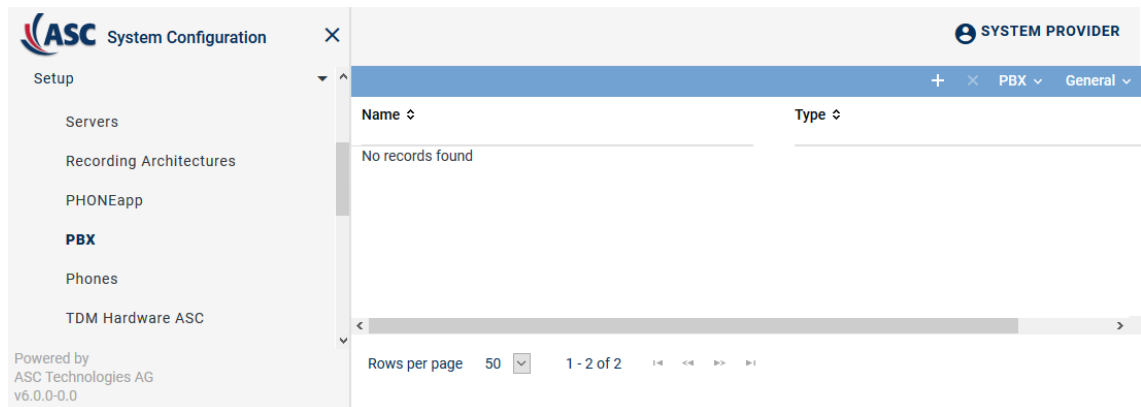


Fig. 124: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.

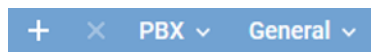




Fig. 125: Toolbar PBX module

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



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

Create new PBX

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

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

×

< Details* PHONEapp Configuration Web Service >

Name*

PBX type*

Maximum length of extensions

Country code

Area code*

Net code*

Mitel MiVoice MX-ONE

Mitel MiVoice MX-ONE ▼

4 ▼

☒ Select from list
 United States (1) ▼
☐ Enter manually

6021

5963

Non Phone IPs

No records found
Add Delete

IPs to be Ignored

No records found
Add Delete

MACs to be Ignored

No records found
Add Delete

Save

Reset

Fig. 126: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 29: Create PBX

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

7.3.2.2.4 Assign recording resources

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

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

Assign extensions to tenants

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



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

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



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

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

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

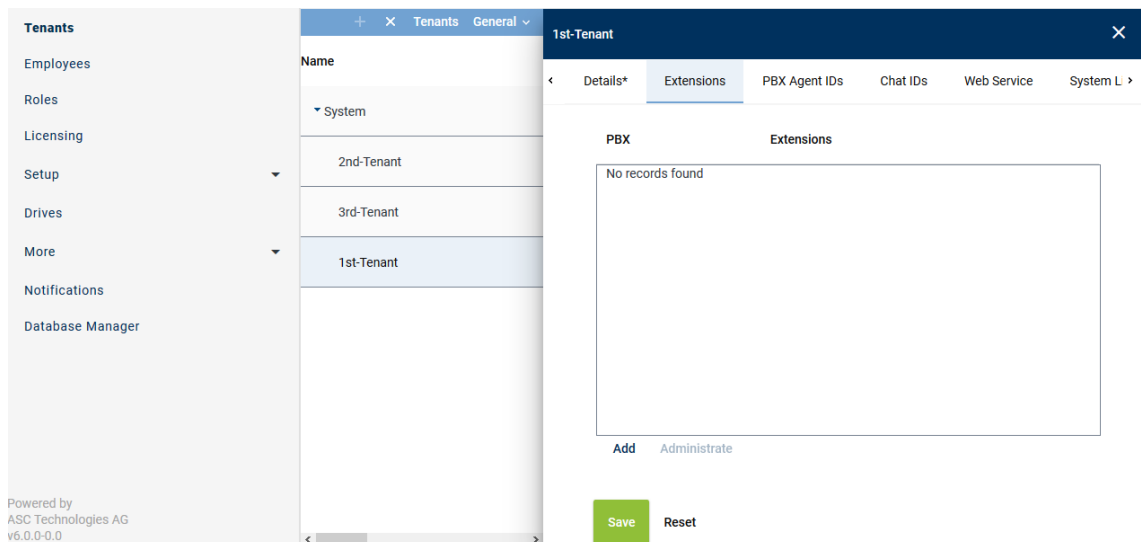


Fig. 127: Tenants - main view - tab Extensions

Add extensions

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

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 128: Assign extensions to tenants

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

<i>File import</i>	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The 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.</p> <p>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.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p>

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

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

Remove extensions

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

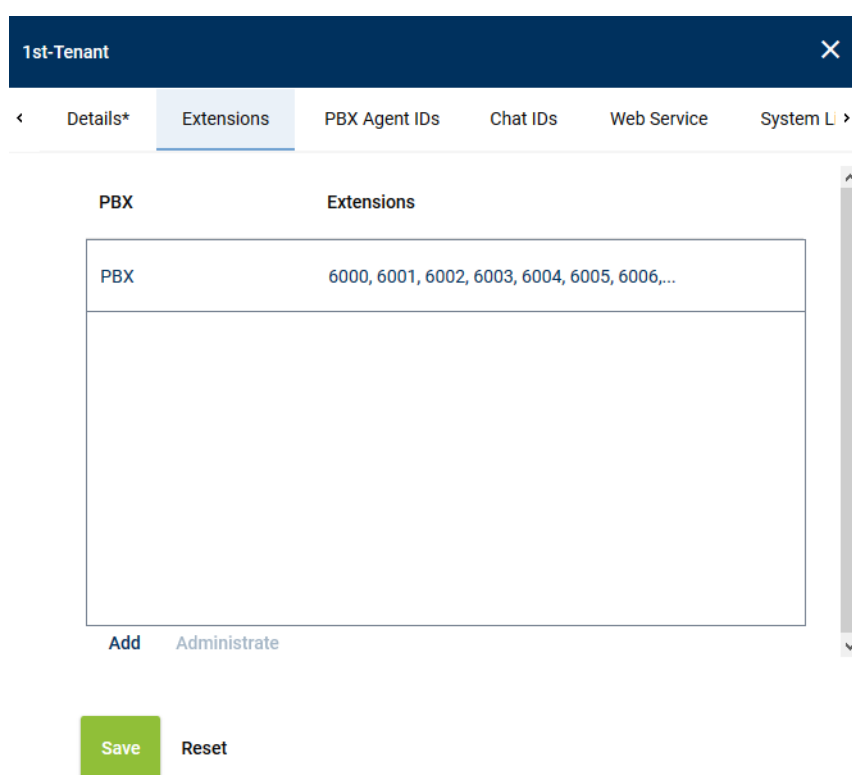


Fig. 129: Remove extensions

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. 130: 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.

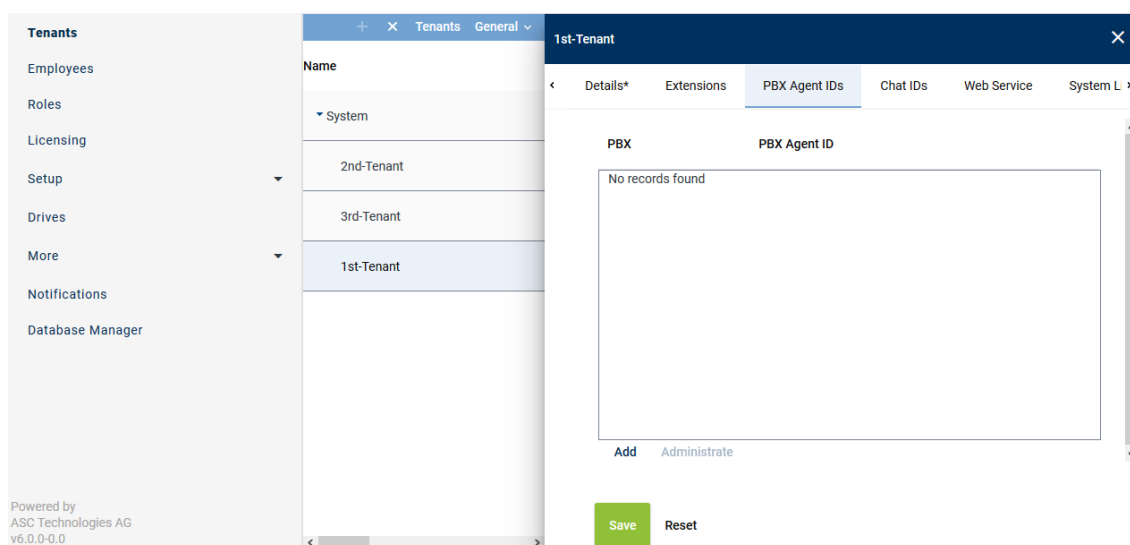


Fig. 131: Tenants - main view - tab PBX Agent ID

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:

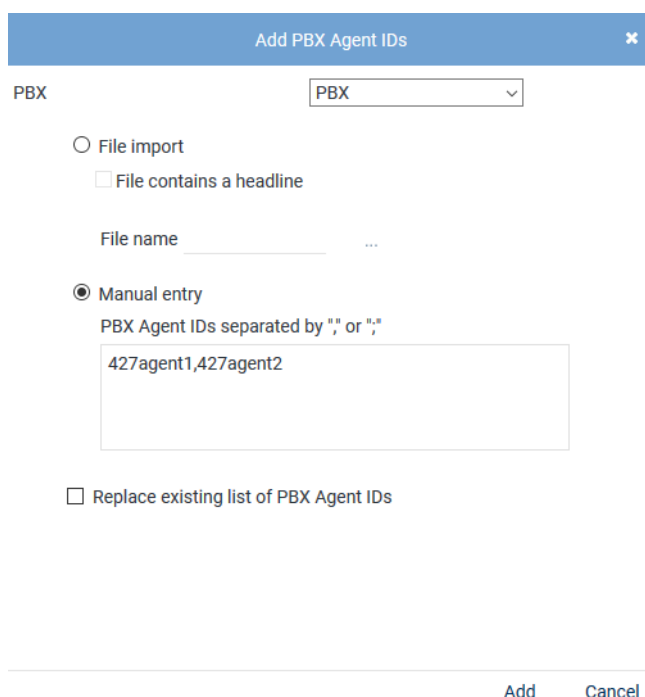


Fig. 132: Assign PBX Agent IDs to tenants

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

<i>File import</i>	Select this option to import the PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = 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.</p>

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

Remove PBX Agent ID

- In the list, select the **PBX** for which you would like to remove the assigned PBX Agent IDs.
- Click the button *Administrate*.
- 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.

Administrate PBX Agent IDs
✕

ID

427agent1

427agent2

Remove Cancel

Fig. 133: 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*.

7.3.2.2.5 Configure additional data

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

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

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

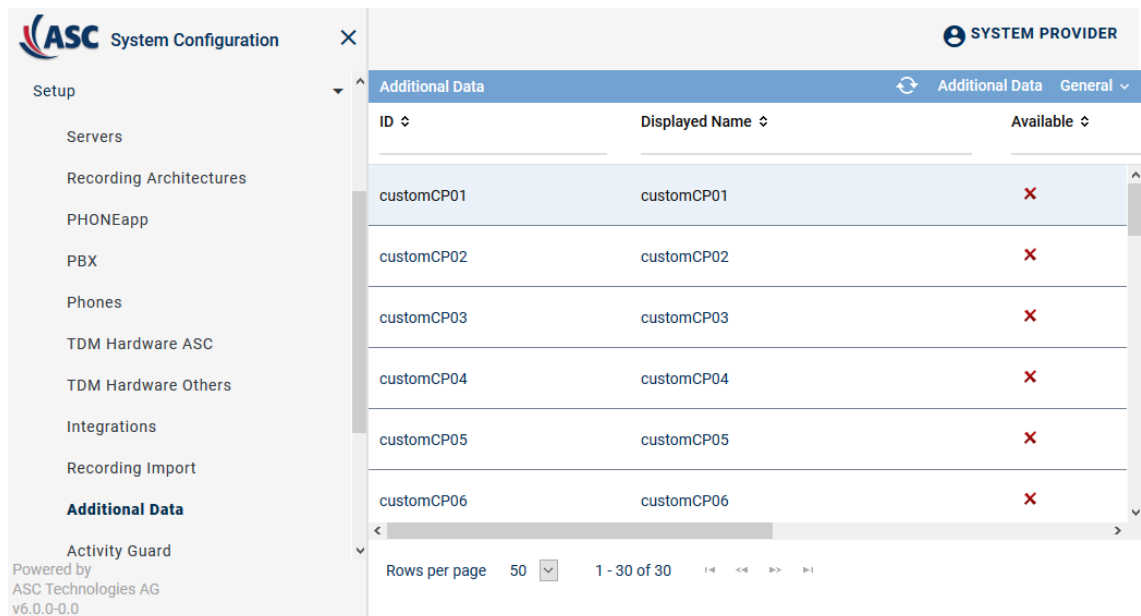


Fig. 134: Additional Data module main view

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

Change display name

Change Display Name
▼







Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 135: Configure additional data

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

Availability

Availability
▼

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

Save

Reset

Fig. 136: Additional data - configure availability

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



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



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

7.3.2.2.6 Create integration for All-in-one Failover

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

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

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

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

⇒ The following window appears:

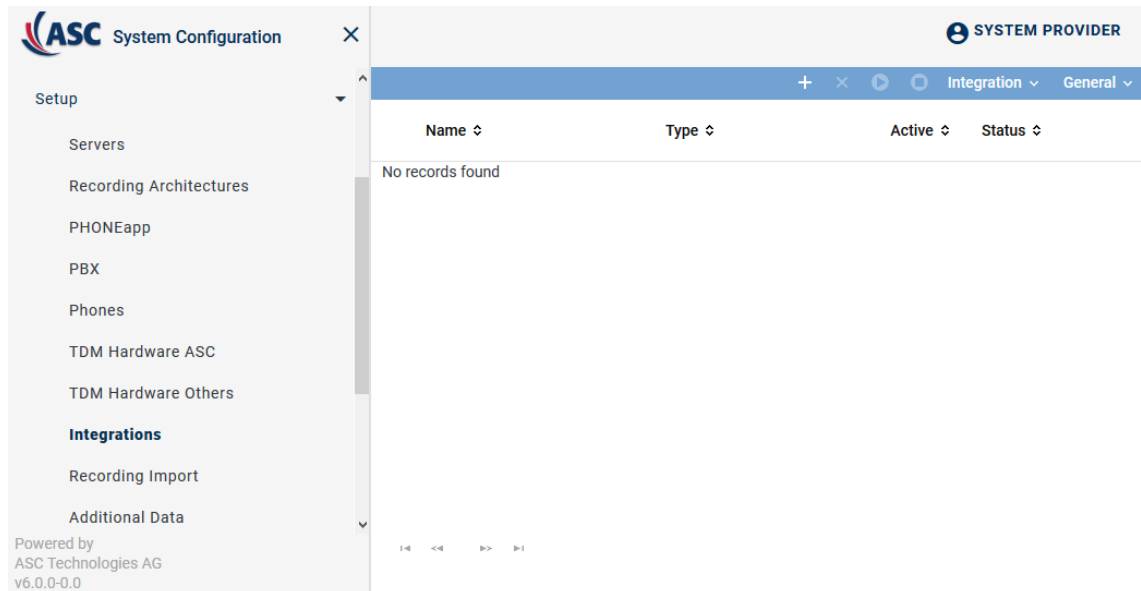




Fig. 137: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 138: Toolbar Integrations module

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

<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Import grammar

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

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

- To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.
⇒ The window *Upload File* appears.

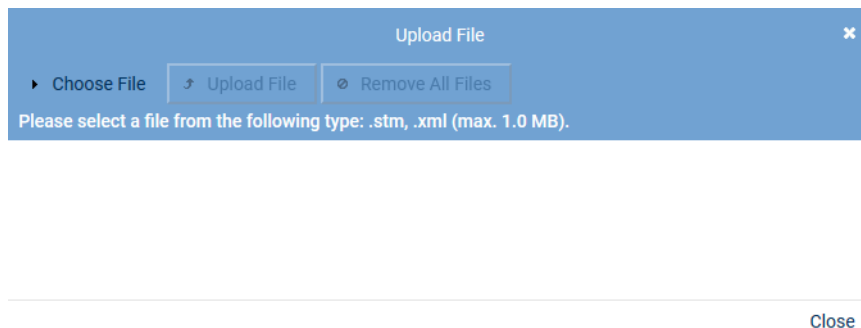


Fig. 139: Choose file

- Click on the button *Choose File*.
- Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
- Click on the button *Open*.
⇒ The selected file appears in the window *Upload File*.

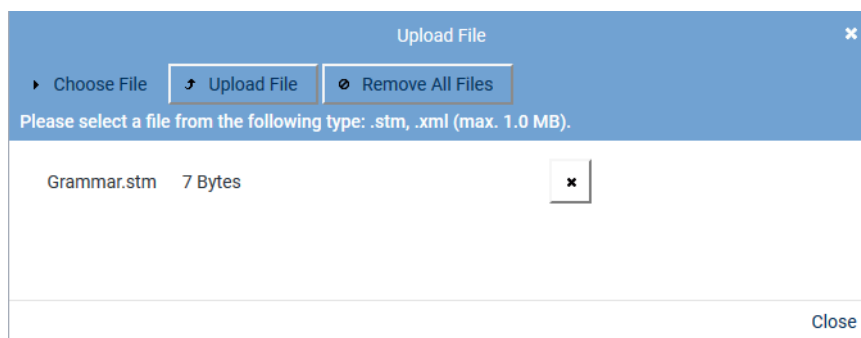




Fig. 140: Upload grammar

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

Assign integration type

- 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. 141: Create integration type

2. Enter the following parameters:

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

Tab. 30: Create integration type

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

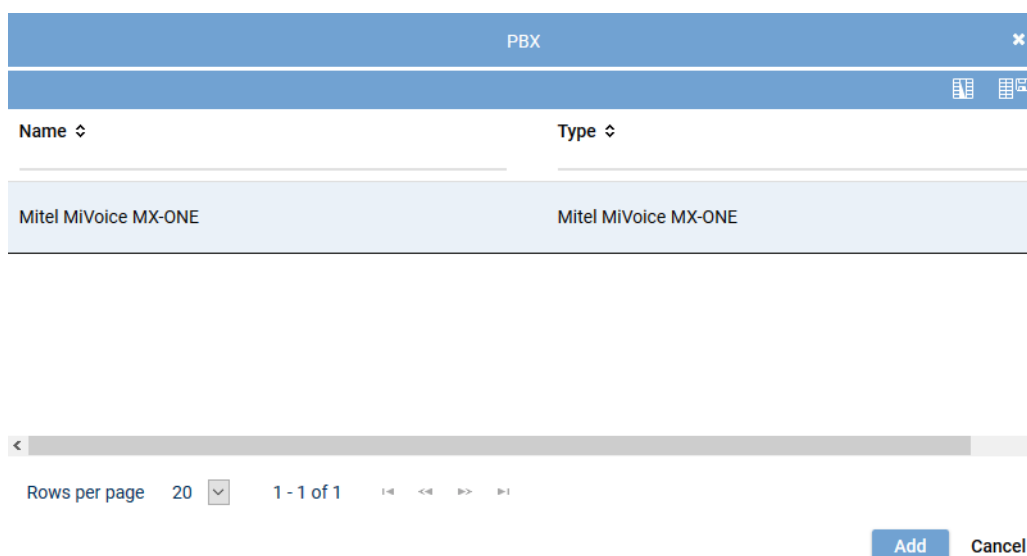


Fig. 142: Integrations - select PBX

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

Assign recording architecture for All-in-one Failover

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

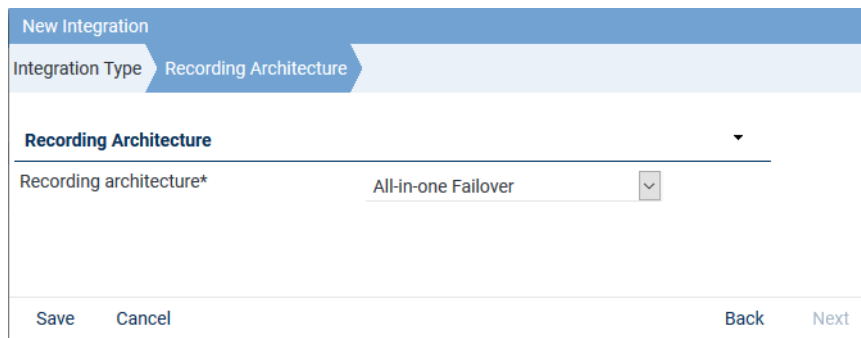


Fig. 143: Assign recording architecture - All-in-one Failover


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



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

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

Configuration steps

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








Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA		✖		⚙	
Step		Configuration					
Configure recording architecture		✓					
Configure CTI connection data		✖					
Configure monitor points		✖					
Global recording settings		✖					
Configure recording servers		✖					
Configure add-on		✓					
Configure miscellaneous settings		✓					

Fig. 144: 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. 145: Configuration step - Configure Recording Architecture


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

Configure CTI connection data

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.

In this configuration step, you configure grammars, connection data, and - if required - additional data.

CTIconnect module

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.
⇒ In the detail view, the tabs *Module 1* and *Module 2* appear.



After an update, this section must be configured again.

Tab module 1

- Select the tab *Module 1* to configure the **CSTA** connection to the PBX.

By configuring module 1, you configure the recording type *Active Stream Recording* and/or *Intrusion*.

The **CSTA** connection is used to monitor the configured monitor points and to start the recording via the intrusion feature.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

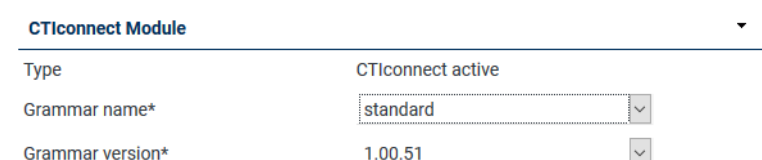


Fig. 146: Configure CTIconnect module

- Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.

Parameter	Value/Description
<i>Grammar name</i>	Select the name of the grammar from the drop-down list.
<i>Grammar version</i>	Select the current version of the grammar from the drop-down list.

Tab. 31: Configure CTIconnect module



After an update of the *neo* software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 1

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.



Fig. 147: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

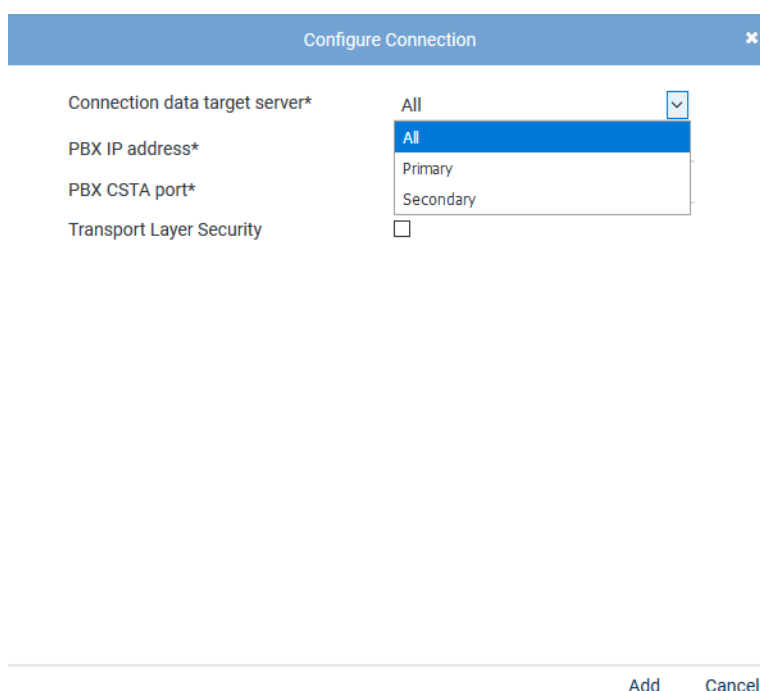


Fig. 148: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data target server</i>	In architectures with several servers, a menu appears for the servers for which this connection is meant.

Parameter	Value/Description
	From the drop-down list, select the server that the connection is meant for.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the CSTA connection is supposed to be run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate the check box to use the connection with TLS .

Tab. 32: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

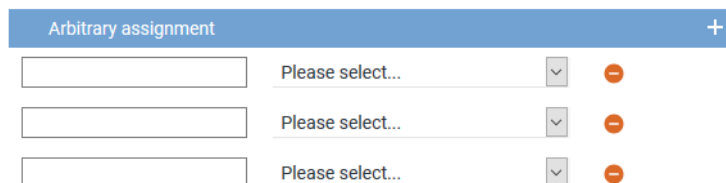



Fig. 149: Arbitrary assignment of the additional data

The following additional data are always available:

- Start time*
- End time*

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

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



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



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

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

1. Here, you can configure how long to wait for the CTI`connect` module to successfully connect with the PBX and how many connection attempts are to be made. If you have configured further connections, the system will switch to the next configured connection.



Only one CTI connection can be active at the same time. Connections cannot be established simultaneously.

Failover waiting time*	10
Failover repetitions*	3

Fig. 150: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI <code>connect</code> module attempts to establish another connection. Once this waiting time is over, new connection attempts are made depending on the configured number of failover repetitions.
<i>Failover repetitions</i>	Enter how many times the CTI <code>connect</code> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <code>connect</code> module makes as many connection attempts as have been configured for the failover repetitions. For each connection attempt, the configured failover waiting time is

observed. If all connection attempts for the first configured connection have failed, the system switches to the next configured connection.



When configuring a failover architecture, the configuration of the switching conditions for the CTI connections must be considered. If only the last of several configured connections is established, the waiting times and repeated connection attempts of the previous connections must be taken into account. If the overall failover time configured for the recording architecture is too short, then a system failover may be triggered even though there would be a CTI connection which could be established successfully.



After an update, this section must be configured again.

Automatic identification of the recording type

The recording type of an end device is identified by means of analyzing the "Switching Function Representation" determined by CSTA as well as by means of the intrusion flag set in the configuration of the monitor points. The regular expression which can be configured here serves to determine whether the end device with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (invitation) can be recorded. The "Switching Function Representation" is extracted from the CSTA information and interpreted on basis of the "Switching Function Representation Format" (N<DN!SA/EXT>NM). The NM section is checked by means of the regular expression. It is checked whether the end device type is contained in the expression. If the expression matches the NM section, then the above mentioned recording mode is used for this end device.

Regular expression for phone type identification*

```
^[A-Za-z]*\\s[0-9]{4}[a-zA-Z]?$|^*[0-9]{4}[a-zA-Z]?$|^*DBC[0-9]{5}$
```

Fig. 151: Configure regular expression for phone type identification

A sensible expression has been saved for the parameter; however, it may be necessary to adjust the parameter to support other phones.



When entering regular expressions, several characters must be added to form escape sequences so that the meaning remains intact when the software extracts them, see <https://docs.oracle.com/javase/tutorial/java/data/characters.html>. When they are not added to form escape sequences, a simple "\s", for instance, will be filtered out internally. When reading them in again, "\s" will then be interpreted as "s" only. Thus, the regular expression will not work anymore after reading them in. To retain the required "\s" upon reading the expression in, an additional "\\" must be added in the file to read "\\s".



For further information about regular expressions see https://en.wikipedia.org/wiki/Regular_expression..



A short introduction on regular expressions and a test tool to check the functionality of regular expression can be found at <https://www.freeformatter.com/java-regex-tester.html>.

The recording type is determined in the following order:

- *Intrusion*
If the feature Intrusion has been activated by means of the GUI, it is used for recording.
- *Invitation Pattern*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type.

- **SRC**
If the regular expression does not match for the respective phone, recording is done via **SRC**.

Tab Module 2

1. Select the tab *Module 2* to configure the connection data of the **MBG**.

By configuring module 2, you configure recording via the Mitel Border Gateway.



Fig. 152: Activate CTIconnect module 2

Active Tick the check box to display the configuration parameters and to activate the module.

☒ Module 2 has been activated.

☐ Module 2 has not been activated.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

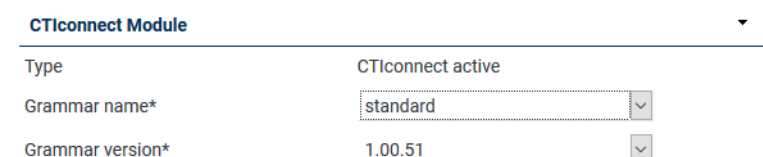


Fig. 153: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
<i>Type</i>	Is filled automatically.
<i>Grammar name</i>	Select the name of the grammar from the drop-down list.
<i>Grammar version</i>	Select the current version of the grammar from the drop-down list.

Tab. 33: Configure CTIconnect module



After an update of the **neo** software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 2

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the **MBG** continues with restricted additional data. Phone numbers and direction continue to be available.

Connection Data ▼

Connection data

No records found

[Add](#)
[Edit](#)
[Delete](#)

Fig. 154: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

Configure Connection
✕

Connection data* 192.168.170.136

PBX port* 6810

Activate indirect recording ☐

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

Fig. 155: Configure connection

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the connection data to the MBG or the SRC .
<i>PBX port</i>	Enter the port via which the MBG connection is supposed to run default <i>6810</i> .
<i>Activate indirect recording</i>	This option must not be activated for this type of recording.

Tab. 34: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

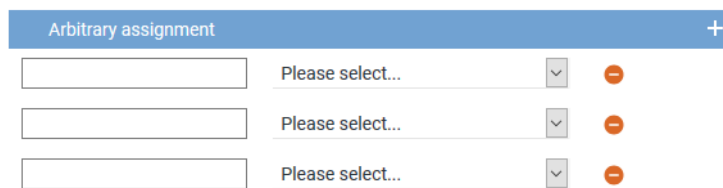



Fig. 156: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure monitor points

In this configuration step, the monitor points for the monitored end devices are configured.

1. In the main view in the line *Configure monitor points*, click on the button  (*Edit configuration step*).
⇒ The window *Step: Configure Monitor Points* appears in the detail view.

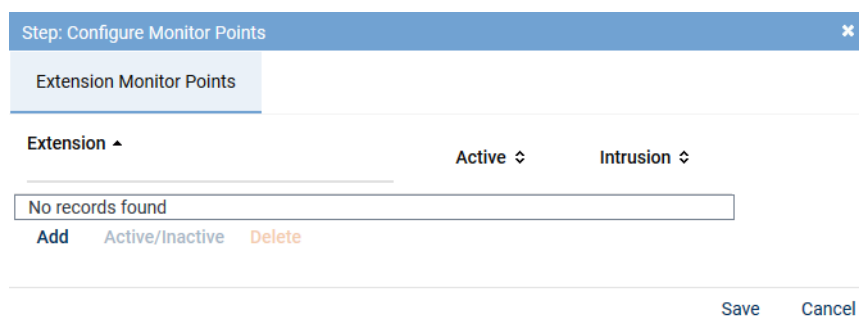


Fig. 157: Configuration step - configure monitor points

Extension monitor points



For the recording variant with **MBG** or **SRC**, the phones to be recorded must have been registered in the **SRC**. This does not apply to the recording variant with SIP Invite or Intrusion.

1. In the tab *Extension Monitor Points*, click on the button *Add* to add the extensions for the monitored end devices.
2. Select the menu item *Enter Extensions*.
⇒ The window *Add Extension Monitor Points* appears.

Add Extension Monitor Points
✕

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry





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

6000-6006

☐ Replace existing list of extensions

Add Cancel

Fig. 158: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
	<p>File contains a headline</p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p>

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

☒ = Function has been activated; all assignments of the PBXs which are listed in the detail view are overwritten and only the new assignment is applied.

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

3. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
4. If errors have been detected, the window *Result* appears.
Click on the button *Display Error Report* to open the window *Error Report*.
To close the window *Error Report*, click on the button *Close*.
To close the window *Result*, click on the button *Close*.
5. The configured extensions now appear in the detail view.

Step: Configure Monitor Points ✕		
Extension Monitor Points		
Extension ▲	Active ⇅	Intrusion ⇅
6000	✓	<input checked="" type="checkbox"/>
6001	✓	<input checked="" type="checkbox"/>
6002	✓	<input type="checkbox"/>
6003	✓	<input type="checkbox"/>
6004	✓	<input type="checkbox"/>
6005	✓	<input type="checkbox"/>
6006	✓	<input type="checkbox"/>
<a>Add <a>Active/Inactive <a>Delete		
Save Cancel		

Fig. 159: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Delete To delete extension monitor points, select the respective extension in the list and click on the button *Delete*. To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Intrusion To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column *Intrusion*.

☒ = Intrusion feature has been activated.

☐ = Intrusion feature has not been activated.

6. Click on the button *Save* to apply the settings and to finish this configuration step.



An extension which is supposed to be monitored and recorded by means of intrusion must be configured in the PBX to send an engaged signal if it is in a conversation. Only then, can the CTI^{connect} service initiate an intrude call and a silent conference.

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 15](#).

Global recording settings

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.

Step: Global Recording Settings

Details

Transport protocol	TCP	
Port SIP signaling*		5060
Remote SIP port*		7300
Activate SIP authentication	<input checked="" type="checkbox"/>	
User name for the SIP registration	#Extension	
Password for the SIP registration	••••••••	
Activate PBX connection	<input checked="" type="checkbox"/>	
SIP registration expiration*		3600
PBX IP address*	192.168.170.219	
PBX port*		5060

Save
Cancel

Fig. 160: Configuration step - Global Recording Settings

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

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

Parameter	Value/Description
	UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling. On this port, the recording server can reach the Mitel end devices for the Active Streaming Recording by means of SIP to start the recording. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices, default 7300.
<i>Activate SIP authentication</i>	Activate the check box if the SIP registration is supposed to be authenticated. The option <i>Activate SIP authentication</i> is only used together with or as an expansion of the option <i>Activate PBX connection</i> .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration for the recording of the extensions used with the intrusion feature. The user name is configured in the PBX and applies for all extensions to be registered.
<i>Password of the SIP registration</i>	Enter the password for the SIP registration for the recording of the extensions used with the intrusion feature. The password is configured in the PBX and applies for all extensions to be registered.
<i>Activate PBX connection</i>	Activate the check box if you would like to use the intrusion feature. When this option has been activated, the configured extensions of the recording server are registered on the PBX. Once the check box has been activated, the following parameters become active to be configured.
<i>SIP registration expiration</i>	Enter the period in seconds until the registration runs out.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port for the communication with the PBX, default 5060.


Tab. 35: Global recording settings

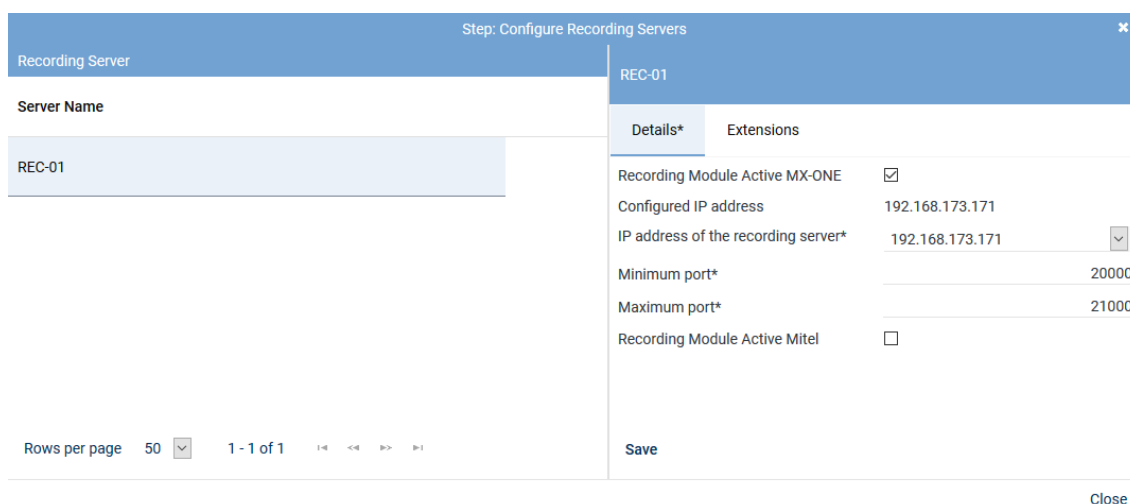
- Click on the button **Save** to apply the settings and to finish this configuration step.



After an update, this section must be configured again.

Configure recording servers

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



Step: Configure Recording Servers

Recording Server

Server Name

REC-01

REC-01

Details* Extensions

Recording Module Active MX-ONE ☒

Configured IP address 192.168.173.171

IP address of the recording server* 192.168.173.171

Minimum port* 20000

Maximum port* 21000

Recording Module Active Mitel ☐

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 161: Configuration step - Configure recording servers

2. Activate the check box *Recording Module Active MX-ONE* so that the configuration parameters appear.
3. Enter the following parameters:

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

Tab. 36: Configure recording servers



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*.

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



After an update, this section must be configured again.

Tab Extensions

If you would like to use the feature *Intrusion* you have to configure an extension for the recording server.

1. Select the tab *Extensions*.

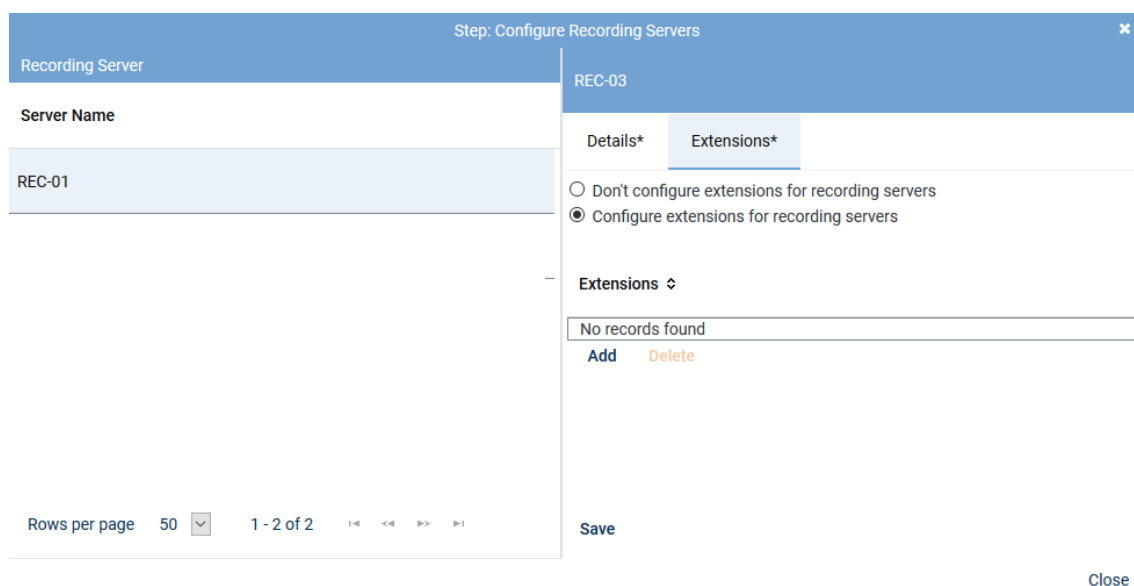


Fig. 162: Tab Extensions

Configure extensions of the recording server Activate this option if you would like to configure extensions for the recording server so make the feature call intrusion work.

If you use more than one recording server, assign separate extensions or extension ranges to the respective recording servers.

Make sure that the extensions for the recording server have not already been allocated to extension monitor points.

NOTICE! The extensions which have to be configured here are SIP extensions which have to be created on the PBX previously so that the recording server can register with these extensions on the PBX. These extensions are used exclusively for the intrusion feature.

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

⇒ The window *Add Extensions* appears.

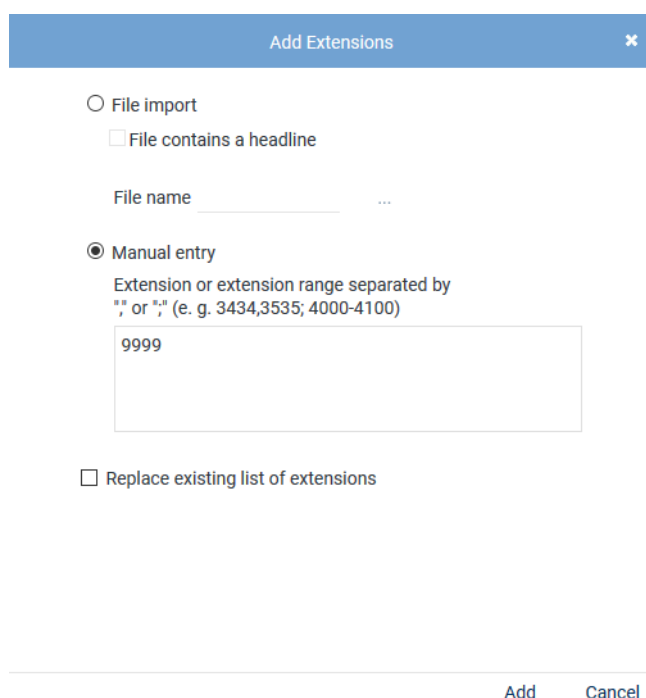


Fig. 163: Add extensions

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.

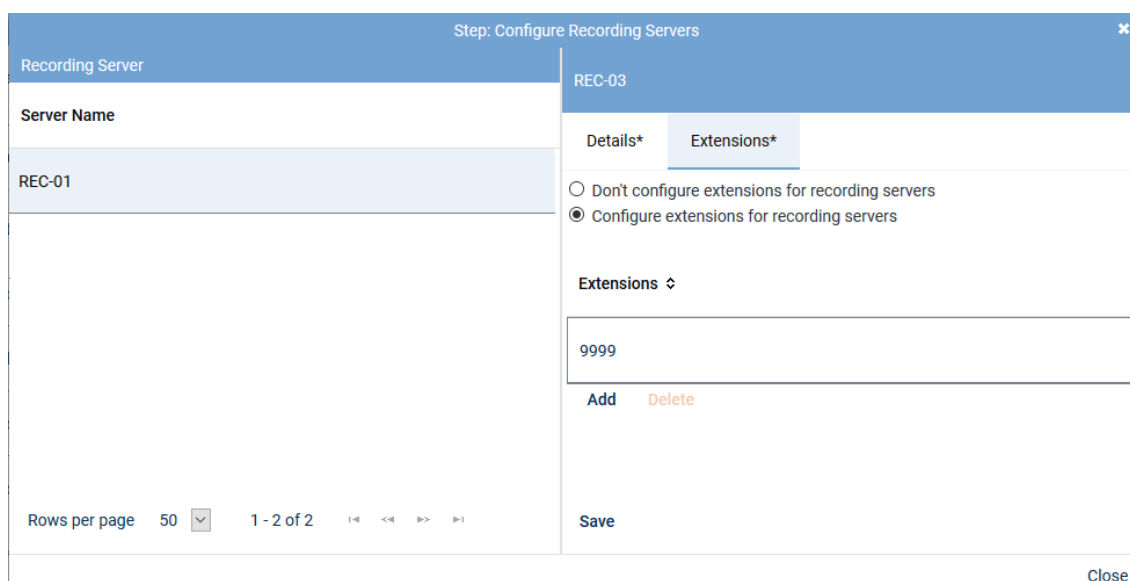


Fig. 164: Added extensions

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

Configure add-on



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

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



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

Configure add-on for MiContact Center Enterprise

The add-on refers to the usage of MiContact Center Enterprise and must only be configured if MiContact Center Enterprise is used.

The integration runs in combination with the PBX and the recording server which is responsible for the actual conversation recording. The conversation events and the additional data are captured via MiContact Center Enterprise and sent to the recording server.

1. Select the add-on *MiContact Center Enterprise* in the detail view.

Step: Configure Add-on
✕

Details *

Select add-on

☐ None

☒ MiContact Center Enterprise

CTIconnect Module

Type CTIconnect passive

Grammar name* standard ▼

Grammar version* 2.00.01 ▼

Connection Data ▼

Server name* 192.168.170.205

Port* 2601

Additional Data ▼

CALLID	Universal Call ID	▼
PRIVATEDATA	Please select...	▼
SERVICEGROUPID	Please select...	▼
SERVICEGROUPLIST	Please select...	▼
IVRDATA1	Please select...	▼
IVRLABEL1	Please select...	▼
IVRDATA2	Please select...	▼
IVRLABEL2	Please select...	▼
IVRDATA3	Please select...	▼
IVRLABEL3	Please select...	▼
OASID	Please select...	▼

Arbitrary assignment
+

	Please select...	▼	-
	Please select...	▼	-
	Please select...	▼	-

Save Cancel

Fig. 165: Configure add-on for MiContact Center Enterprise

Group field CTIconnect Module

- Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 37: Configure CTIconnect module

Group field Connection Data

- Set the following parameters in the group field *Connection Data*:

Parameter	Value/Description
Server Name	Enter the IP address or the name of the server that the MiContact Center Enterprise runs on.
Port	Enter the port for the connection to MiContact Center Enterprise.

Tab. 38: Configure connection data

Group field Additional Data

The following additional data is delivered in the protocol when using MiContact Center Enterprise:

- *CALLID*
- *PRIVATEDATA*
- *SERVICEGROUPLIST*
- *IVRDATA1*
- *IVRLABEL1*
- *IVRDATA2*
- *IVRLABEL2*
- *IVRDATA3*
- *IVRLABEL3*
- *OASID*

Arbitrary assignment

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



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

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



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

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

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

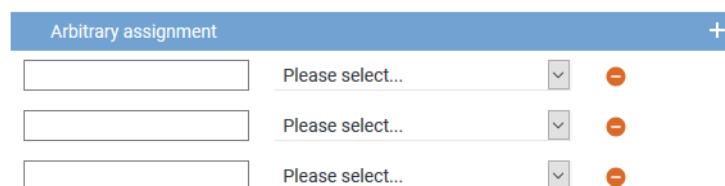



Fig. 166: Arbitrary assignment of the additional data

The following additional data are always available:

- *Start time*
- *End time*

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

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



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



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

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI^{connect} service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

CTIconnect for Genesys T-Server

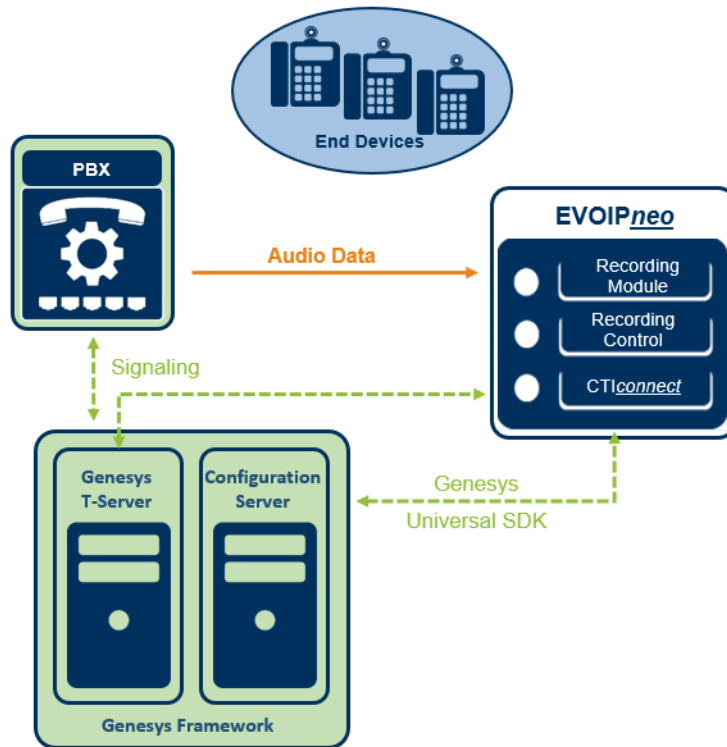


Fig. 167: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 311](#).

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.



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

When using a CTIconnect for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.


By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path
C:\ASC Product Suite\data\CTIConnectForGenesysT\.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button  (*Edit configuration step*) in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

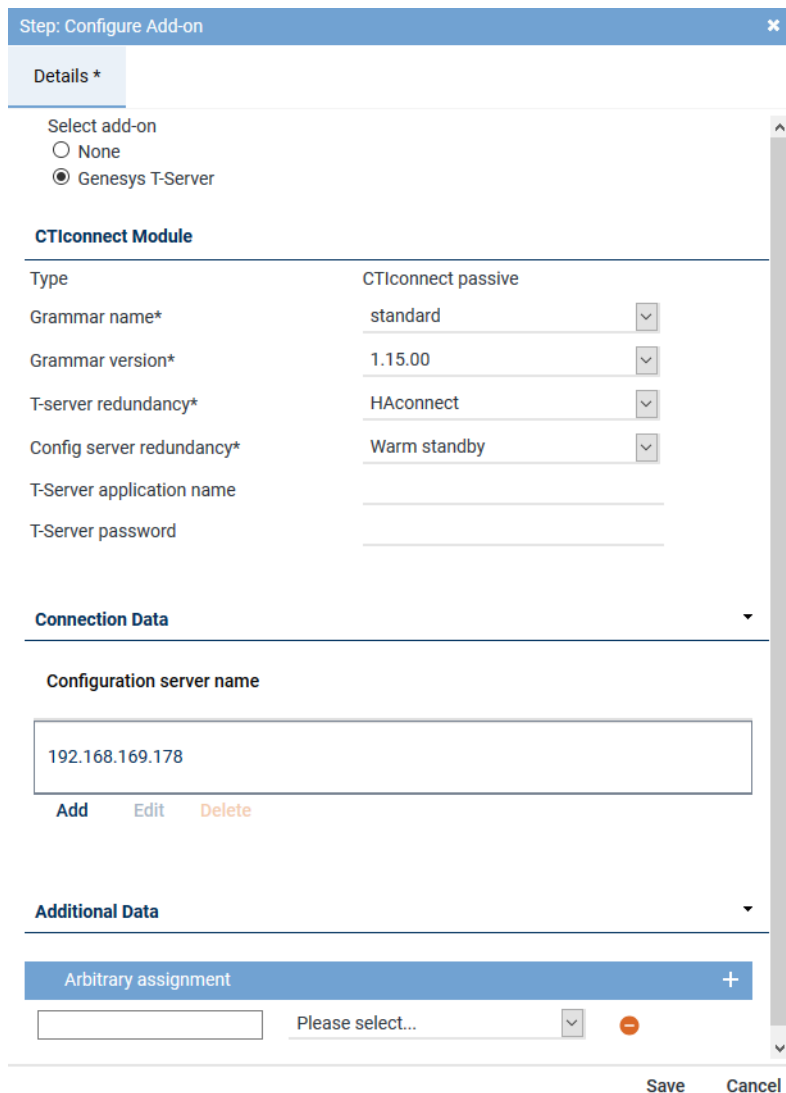


Fig. 168: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 39: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

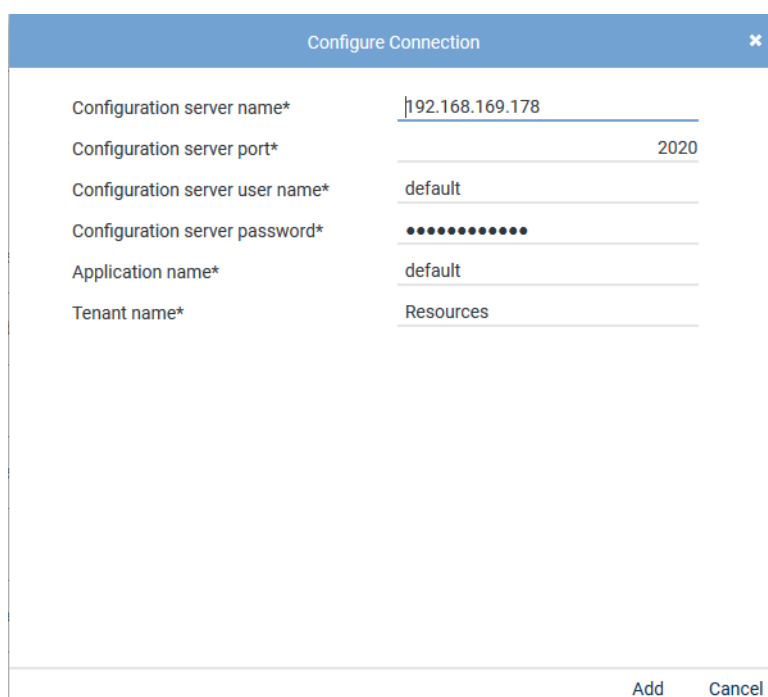


Fig. 169: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.

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

Tab. 40: Configure connection data

Group field Additional Data

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

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



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

Arbitrary assignment

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



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

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



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


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

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

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

Fig. 170: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select... ▼

Save

Cancel

Fig. 171: Configure miscellaneous settings

2. Enter the following parameter:


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





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

Activate integration

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

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

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

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





















	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		
Step		Configuration		
Configure recording architecture				
Configure CTI connection data				
Configure monitor points				
Global recording settings				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 172: Activate integration

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






+ ×   Integration ▾ General			
Name ▾	Type ▾	Active ▾	Status ▾
	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	 

Fig. 173: 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.



For updates, the integration is stopped and deactivated. Once the update has been completed successfully, you must configure the integration again. Once the configuration has been completed, start the recording architecture again and activate the integration so that the new configuration is applied.

Deactivate/Delete integration

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

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







+ ×   Integration ▾ General			
Name ↕	Type ↕	Active ↕	Status ↕
 Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		

Fig. 174: Deactivate integration

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

7.3.2.3 Configure recording solution Multi-Server Recording

7.3.2.3.1 Create recording architecture

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

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

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

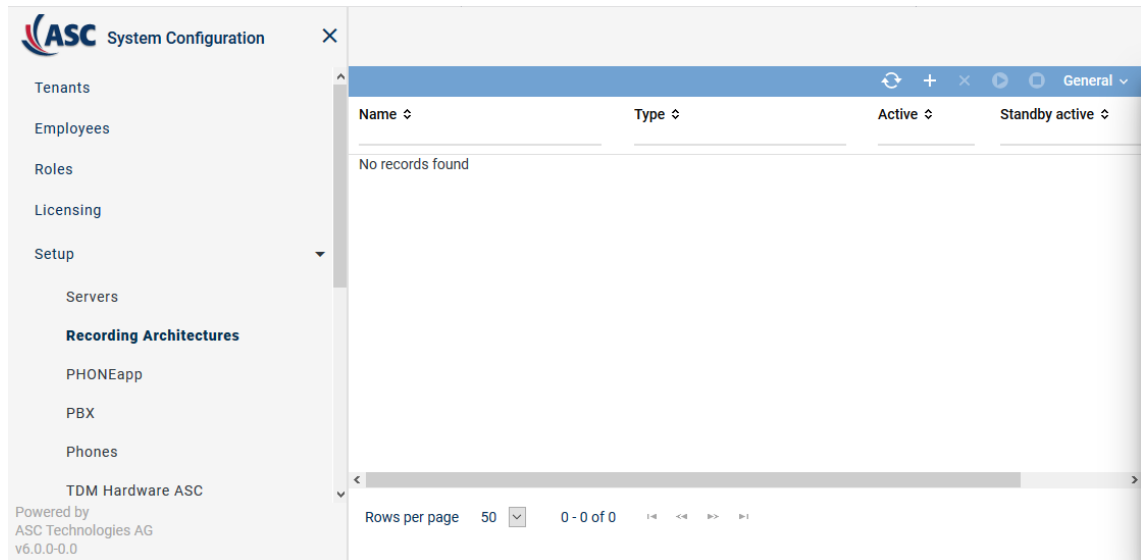





Fig. 175: Recording architectures - main view

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

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

Create recording architecture Multi-Server Recording

If there are several recording servers which are supposed to record different tracks, you have to create a recording architecture of the type *Multi-Server Recording*.

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

New Recording Architecture

Name*

Multi-Server Recording

Type

Multi-Server Recording

OK

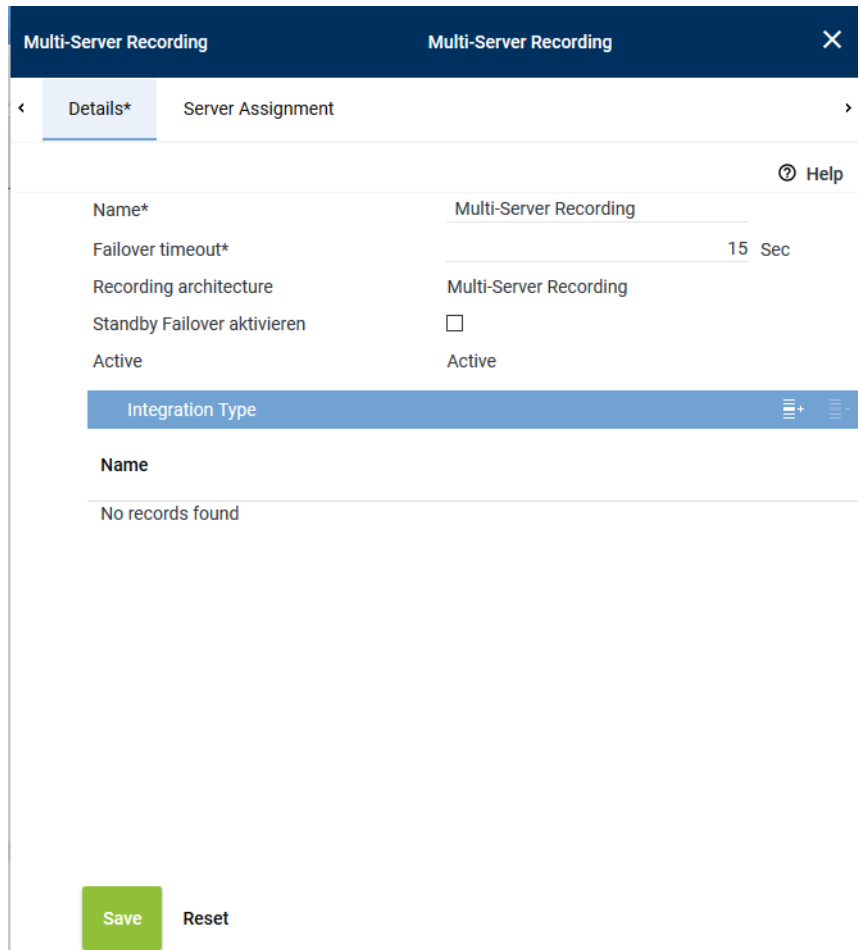
Cancel

Fig. 176: Create recording architecture - Multi-Server Recording

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

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

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



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

Name*	Multi-Server Recording
Failover timeout*	15 Sec
Recording architecture	Multi-Server Recording
Standby Failover aktivieren	<input type="checkbox"/>
Active	Active


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

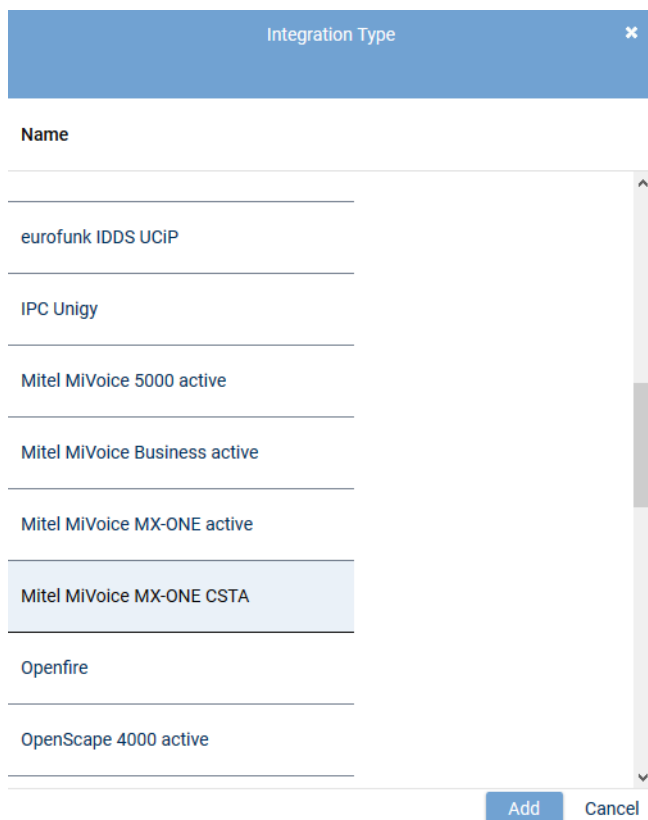
Fig. 177: Recording architecture - tab Details - Multi-Server Recording

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

5. Enter a failover timeout of a minimum of 15 seconds after which the failover process is supposed to start. Depending on the system architecture it may make sense to configure a longer timeout period. The timeout defines the elapse time until the failover process starts. If the status returns to *OK* within this time, then the failover process is not triggered.

Add integration type

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



The dialog box titled "Integration Type" contains a list of integration types. The list is as follows:

Name
eurofunk IDDS UCIP
IPC Unigy
Mitel MiVoice 5000 active
Mitel MiVoice Business active
Mitel MiVoice MX-ONE active
Mitel MiVoice MX-ONE CSTA
Openfire
OpenScape 4000 active

At the bottom right of the list are two buttons: "Add" and "Cancel". The "Mitel MiVoice MX-ONE CSTA" item is currently selected in the list.

Fig. 178: 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 *Mitel MiVoice MX-ONE CSTA* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign servers for Multi-Server Recording

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

Group field Recording Control and CTIconnect

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

Multi-Server Recording
Multi-Server Recording

Details*
Server Assignment*

Recording Control and CTIconnect

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

Recording Server


Recording Server

Server
Standby

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

Save
Reset

Fig. 179: Recording Architecture - tab Server Assignment


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

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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 180: Recording Architecture - assign server - example


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



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

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

Group field Recording Server

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

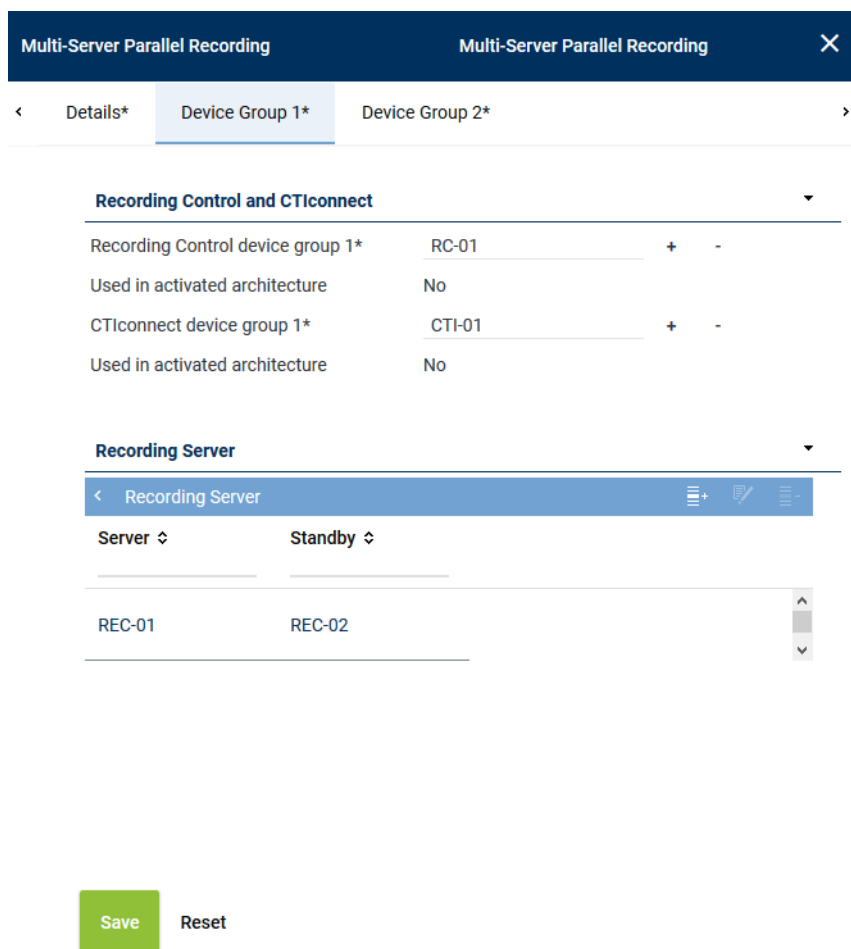









Fig. 181: Add Recording Server

2. As described in the previous steps, go to the entry field *Primary server* and click on the icon  to select the primary server on which the recording is supposed to run.
3. In the entry field *Standby server*, click on the icon  to select the standby server which is supposed to take over recording in case of an error.

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

Activate recording architecture

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










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

Fig. 182: 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 extension for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

7.3.2.3.2 Configure servers

Every server in your network that the *neo* software has been installed on is automatically identified as a server of the recording system and displayed in the main view of the Servers module. In the Servers module, you can configure the usage of the servers in your recording system.

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

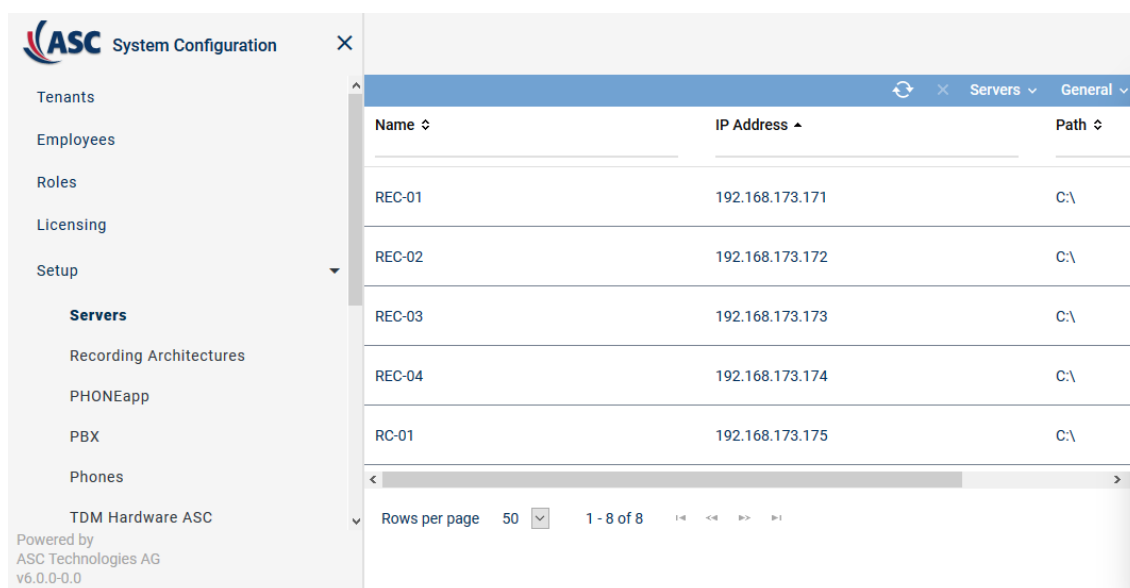


Fig. 183: Servers - main view

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

<i>Name</i>	Shows the name of the server.
<i>IP Address</i>	Shows the IP address of the server.
<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	Date on which the settings of the server were updated for the last time.

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

Toolbar of the Servers module

The toolbar offers the following functions.

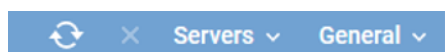




Fig. 184: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Delete</i>	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations" , p. 157.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see chapter "Administrate NTP server" , p. 173.
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view:

	<ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
<i>Save Table Configuration</i>	Saves the current table configuration of the main view as default view of the user.
<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
<i>Reset Search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
<i>General Help</i>	Opens the online help.
<i>Module Help</i>	Opens the module-specific online help.



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

Administrate server locations

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

Add server locations

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

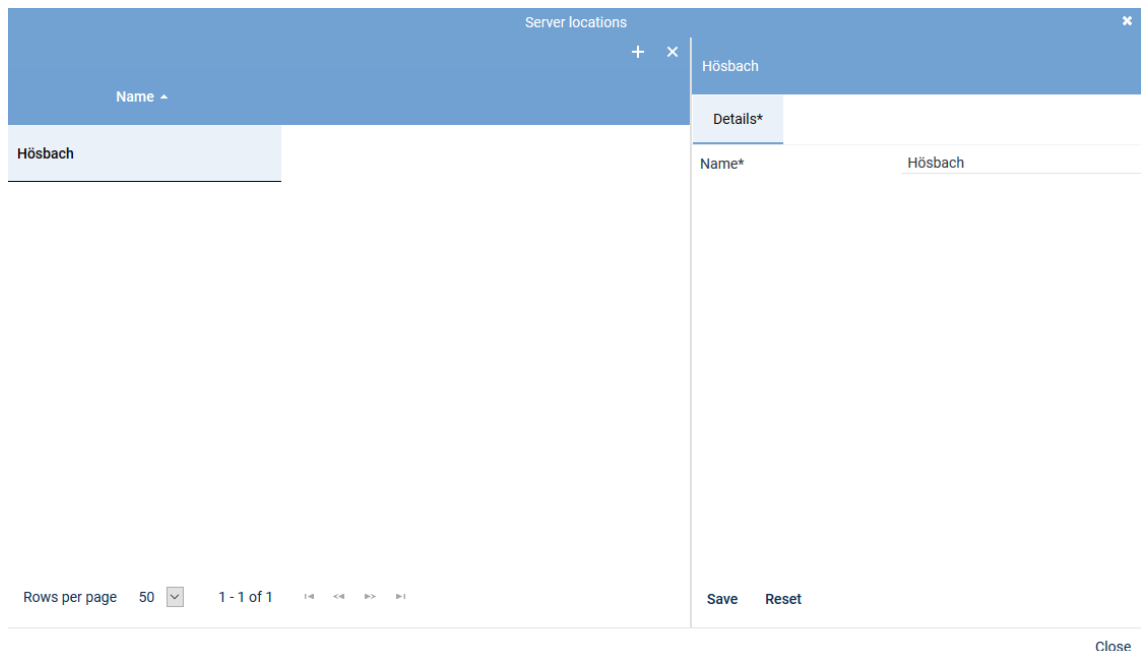



Fig. 185: Add server locations

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

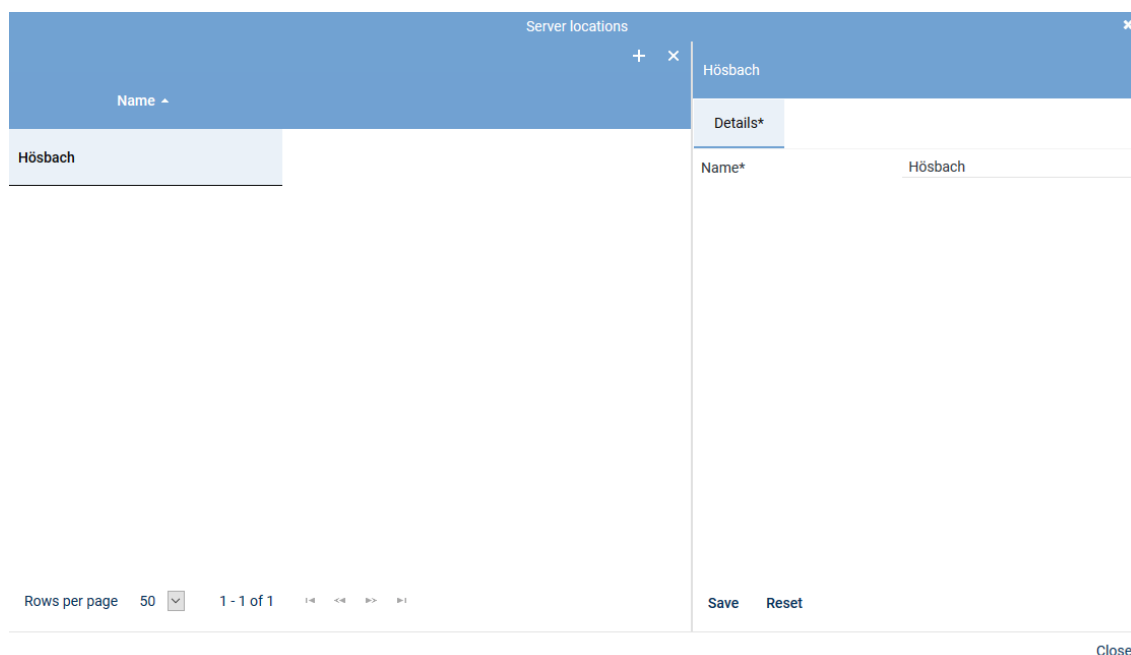
- To close the window, click on the button *Close*.

Delete server location




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

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



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

Fig. 186: Delete server location

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

Tab Details

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

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

? Help

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

Fig. 187: Servers - tab Details

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

Tab Usage

- Click on the tab *Usage* to configure the purpose of usage.



Since a server can be used for several recording solutions, all purposes of use are listed. Note that some purposes of use do not apply for some recording solutions. As an example: You cannot use audio analysis or replay via phone in a chat recording.

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

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

Fig. 188: Servers - tab Usage

Group field API Server

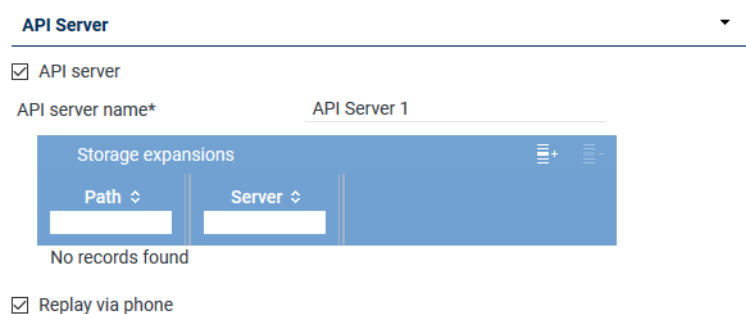


Fig. 189: Group field API Server


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




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


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

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

Parameter	Value/Description
<i>API server</i>	<p>Tick the check box to start the API server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>In order to be able to reach the API server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 169.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the storage expansions, see chapter "Add storage expansion for replay", p. 161.

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (<i>Remove</i>), you can remove the storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated. <input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> Application POWERplay Pro Application POWERplay Instant Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 168. To be able to do so, at least 1 PBX must have been configured in the system.</p>

Add storage expansion for replay

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

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

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 190: Select storage expansion

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

Group field Audio Analysis

Audio Analysis ▼

☒ Audio analysis (SAES mode)

Stream audio data from* + -

☐ Emotion detection

Stream audio data from* + -

Fig. 191: Group field Audio Analysis

Parameters	Value/Description
<i>Audio analysis</i>	<p>Activate this check box to use the server for audio analysis. The audio data is then streamed for audio analysis from the configured server to this server.</p> <ul style="list-style-type: none"> Stream audio data from From the list of available servers, select the server from which the audio data is supposed to be streamed for audio analysis via the button +.
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for the audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>

Tab. 41: Configure audio analysis

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☒ Recording control/Monitoring

Recording architecture ▼

☒ neo key management

Fig. 192: Group field Recording Control/Key Management

Parameters	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <u>CLIENT</u><i>command</i> or an API recording control or if you would like to use <i>Monitoring</i>. This feature is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the respective recording architecture you would like to use for the control.
- <i>neo key management</i>	<p>The function allows customer-specific encryption of the recordings. To be able to configure the key management, you have to activate the check box <i>Key management</i>.</p> <p>This function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p>

Parameters	Value/Description
	For further information about the configuration of the key management refer to the administration manual <i>Configuration of servers and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i> .

Tab. 42: Configure Recording Control/Key Management

Group field Data Processing

Data Processing

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address
No records found	

Activate period of time ☒

from 11:59:36

to 11:59:36

Receives data from

Name	Only Replay
No records found	



☒ Archiving





☒ Export

☒ Import

Recording architecture Please choose...


Fig. 193: Group field Data Processing

Parameter	Value/Description
<i>Data storage</i>	Activate the check box to allow the modification of the additional functions of data processing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 165. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which an API server and a replay server have been configured.</p>

Parameter	Value/Description
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 165. By clicking on the icon  (<i>Remove</i>), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which the function <i>Data Storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<i>Export</i>	Activate the check box <i>Export</i> to allow the export from this server.
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 43: 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.



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

Rows per page: 20 | 1 - 6 of 6 | << < > >>

Add Cancel

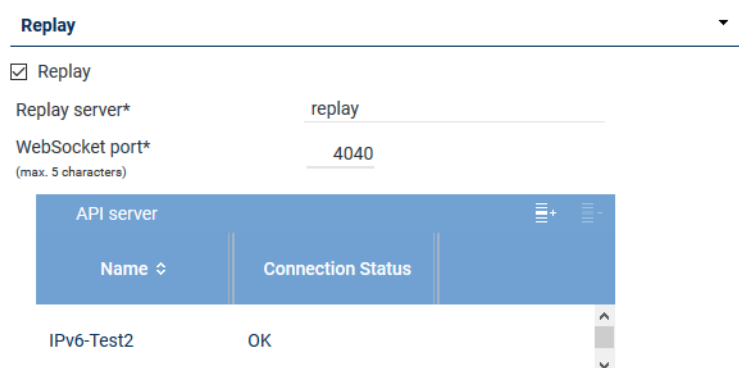
Fig. 194: Select server



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

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

Group field Replay



Replay

☒ Replay



Replay server* replay

WebSocket port* 4040
(max. 5 characters)

Name	Connection Status
IPv6-Test2	OK

Fig. 195: Group field Replay

Parameter	Value/Description
Replay	A replay server can replay recordings via the integrated <i>Replay Feature</i> . Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.

Parameter	Value/Description
	<p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 166. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 44: 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. 196: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 160](#).

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. 197: Group field Virtualization

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

Tab. 45: 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.

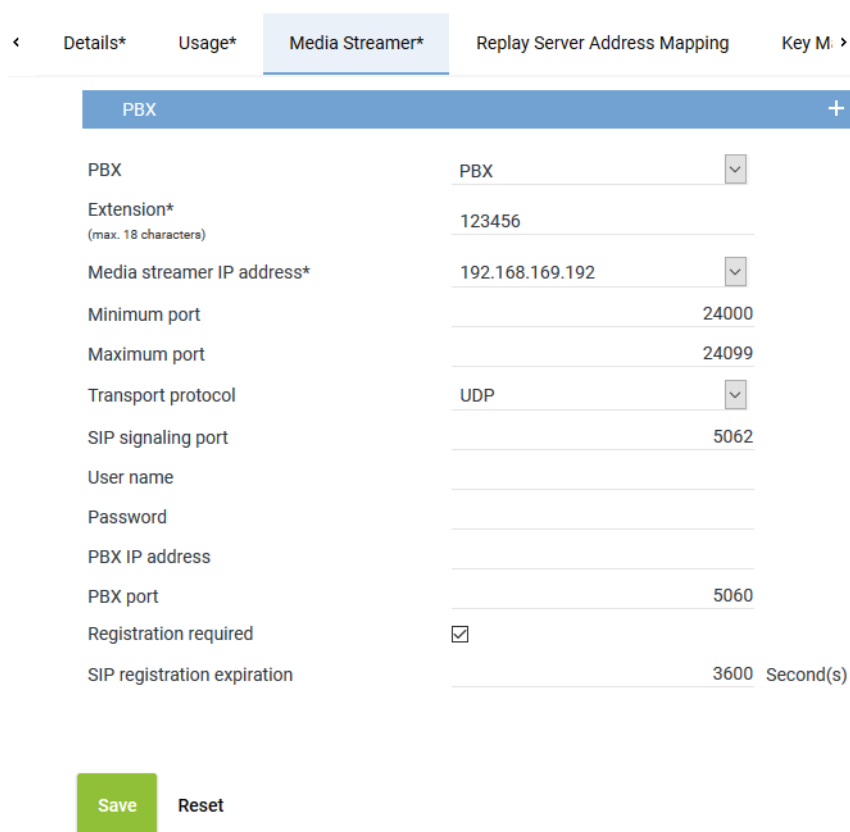
Tab Media Streamer

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*.



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

Save Reset

Fig. 198: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX, see chapter "Create PBX", p. 174.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>

<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. In the drop-down list, all IP addresses of the server are displayed.</p> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</p>
<i>Minimum port</i>	Enter the minimum port which is supposed to be used for the audio data exchange.
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p>
<i>Transport protocol</i>	<p>Select the transport protocol type you would like to use for the SIP communication from the drop-down list.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	<p>Enter the IP address of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the IP address 169.254.254.101.</p>
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box Registration required.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

Tab Replay Server Address Mapping

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

In this tab, you can configure the replay server address mapping. 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*.

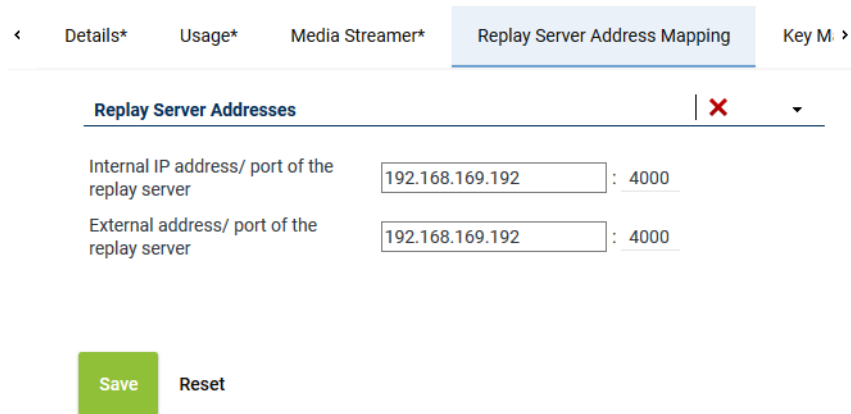


Fig. 199: Servers Module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



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

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



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



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

Tab Key Management

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

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

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

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage

until

0 Day(s)

0 Hour(s)

☐ Key expiration date

after

0 Day(s)

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

Save

Reset

Fig. 200: Servers module - tab Key Management

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

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

In case of an error ... automatically

Select whether simple key management is supposed to be used if the neo key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the neo key management has been activated but does not work.

☒ = In case of an error, simple key management is used as replacement.

☐ = In case of an error, no recording takes place as long as the neo key management has been activated. In this case, disable key management in the tab *Usage*.



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



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

Tab Keystore/Virtualization

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

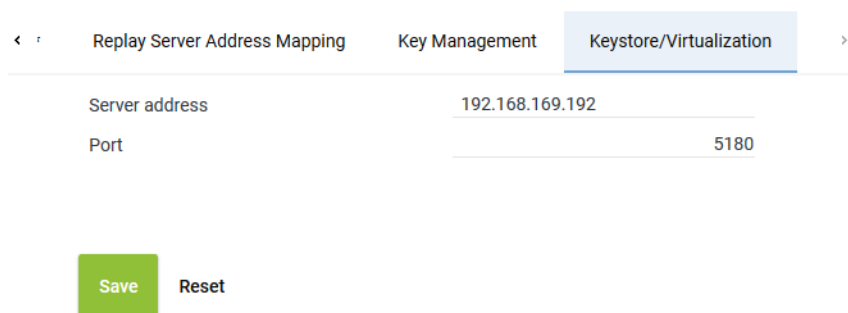
In this tab, you can configure the connection data for the service *DongleMan* for the neo key management and for the authentication of the VM.



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*.



Replay Server Address Mapping	Key Management	Keystore/Virtualization
Server address	192.168.169.192	
Port		5180

Save Reset

Fig. 201: 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

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

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

Administrate NTP server

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

Add NTP server

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

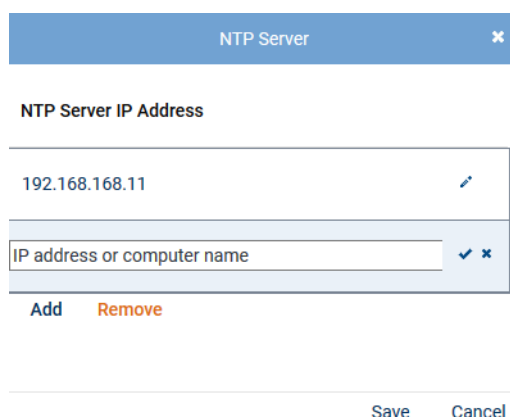





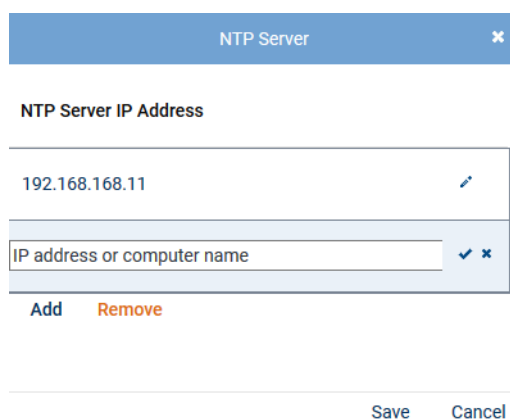
Fig. 202: Add NTP server

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

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




Edit IP address

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



NTP Server




NTP Server IP Address

192.168.168.11	
IP address or computer name	 

Add Remove

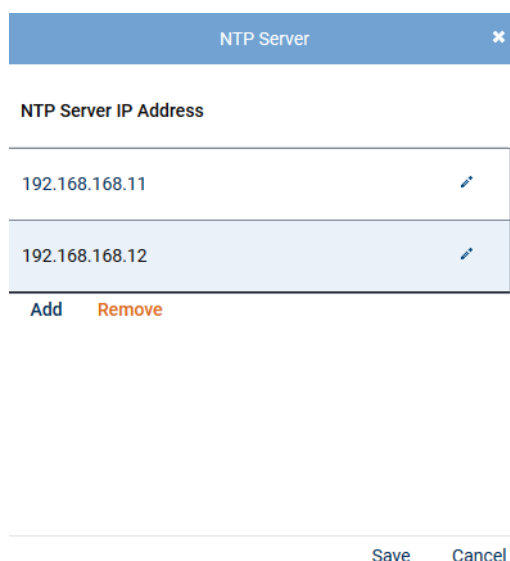
Save Cancel

Fig. 203: Edit IP address

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



Remove NTP server

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



NTP Server

NTP Server IP Address

192.168.168.11	
192.168.168.12	

Add Remove

Save Cancel

Fig. 204: Remove NTP server

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

7.3.2.3.3 Create PBX

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

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

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

⇒ The following window appears:

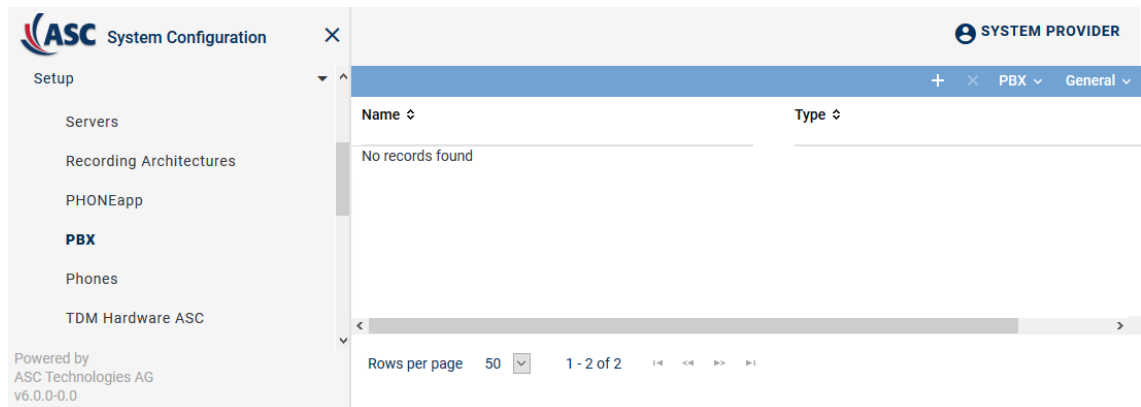




Fig. 205: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.



Fig. 206: Toolbar PBX module

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



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

Create new PBX

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

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

×

< Details* PHONEapp Configuration Web Service >

Name*

PBX type*

Maximum length of extensions

Country code ☒ Select from list

☐ Enter manually

Area code*

Net code*

Non Phone IPs

No records found

[Add](#) [Delete](#)

IPs to be Ignored

No records found

[Add](#) [Delete](#)

MACs to be Ignored

No records found

[Add](#) [Delete](#)

Save

Reset

Fig. 207: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 46: Create PBX

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

7.3.2.3.4 Assign recording resources

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

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

Assign extensions to tenants

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



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

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



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

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

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

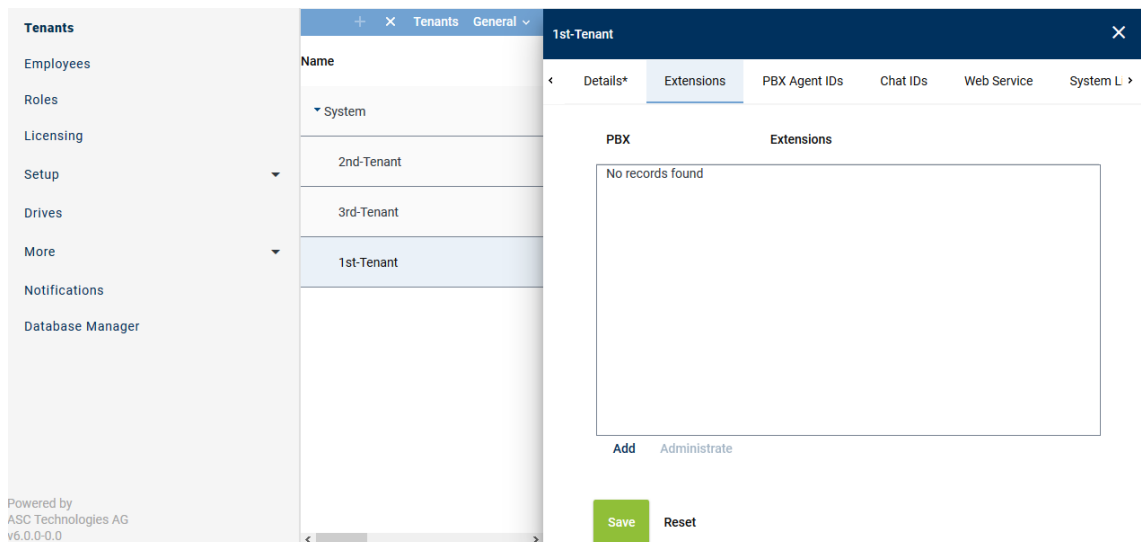


Fig. 208: Tenants - main view - tab Extensions

Add extensions

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

Add Extensions ✕

PBX PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 209: Assign extensions to tenants

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

<i>File import</i>	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The 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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p>

☐ = 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.

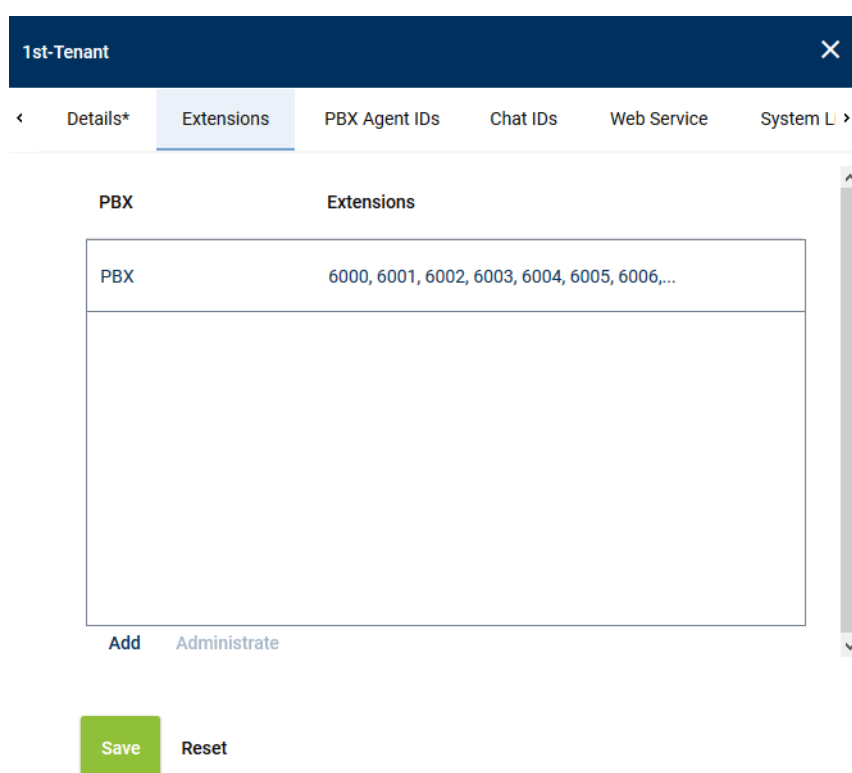


Fig. 210: Remove extensions

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. 211: 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.

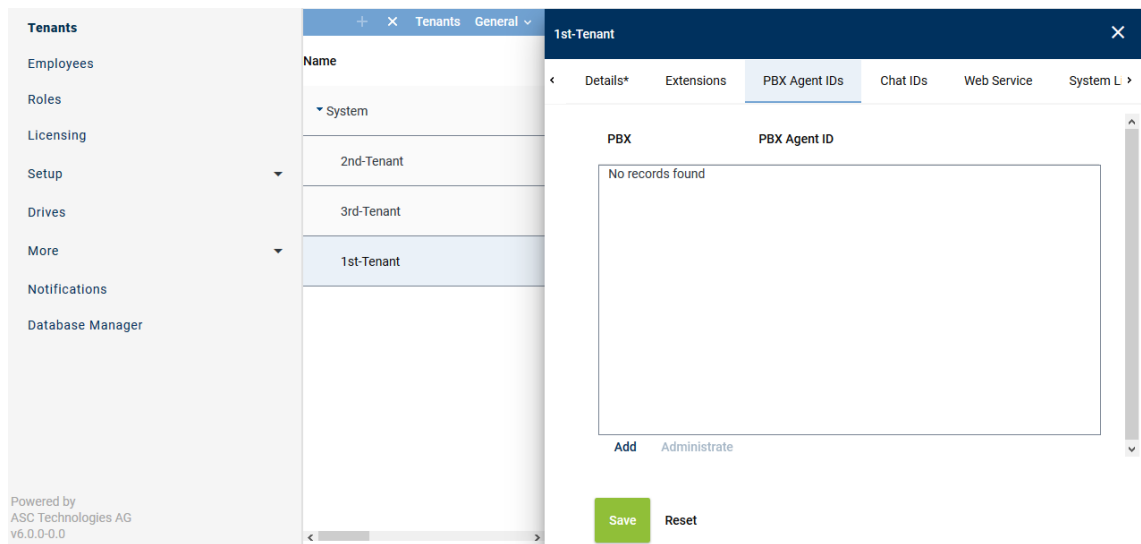


Fig. 212: Tenants - main view - tab PBX Agent ID

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:

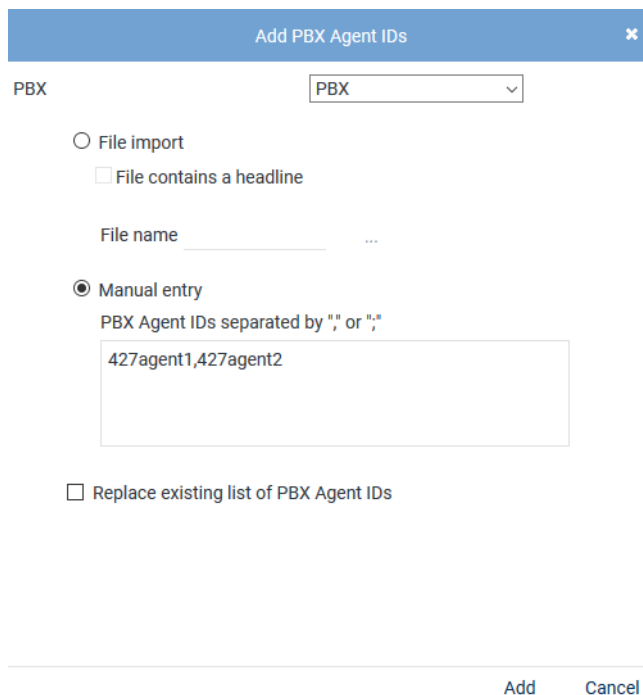


Fig. 213: Assign PBX Agent IDs to tenants

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

<i>File import</i>	Select this option to import the PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
Manual entry	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
Replace existing list of PBX Agent IDs	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = 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.</p>

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

Remove PBX Agent ID

- In the list, select the **PBX** for which you would like to remove the assigned PBX Agent IDs.
- Click the button *Administrate*.
- 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.

Administrate PBX Agent IDs
✕

ID

427agent1

427agent2

Remove Cancel

Fig. 214: 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*.

7.3.2.3.5 Configure additional data

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

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

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

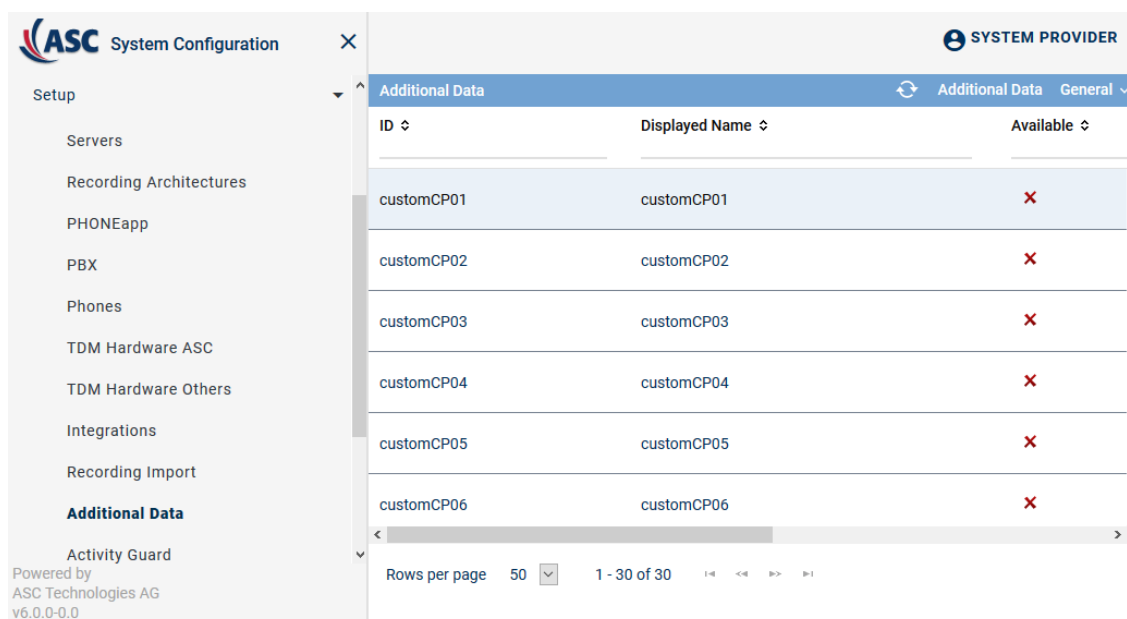


Fig. 215: Additional Data module main view

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

Change display name

Change Display Name
▼







Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 216: Configure additional data

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

Availability

Availability
▼

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

Save

Reset

Fig. 217: Additional data - configure availability

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



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



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

7.3.2.3.6 Create integration for Multi-Server Recording

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

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

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

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

⇒ The following window appears:

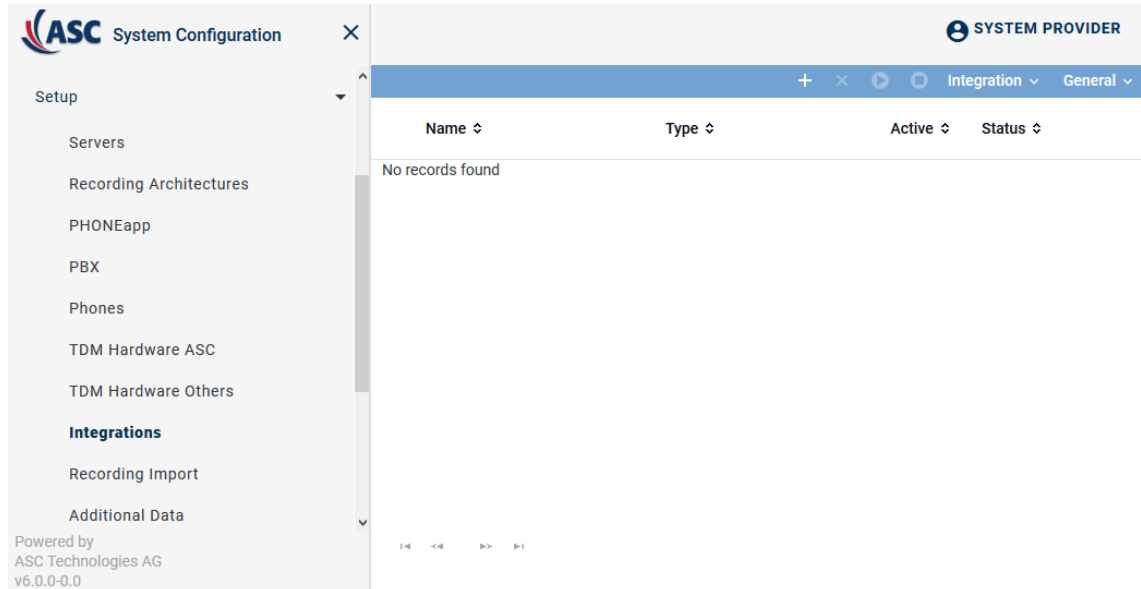




Fig. 218: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 219: Toolbar Integrations module

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

<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Import grammar

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

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

- To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.
⇒ The window *Upload File* appears.

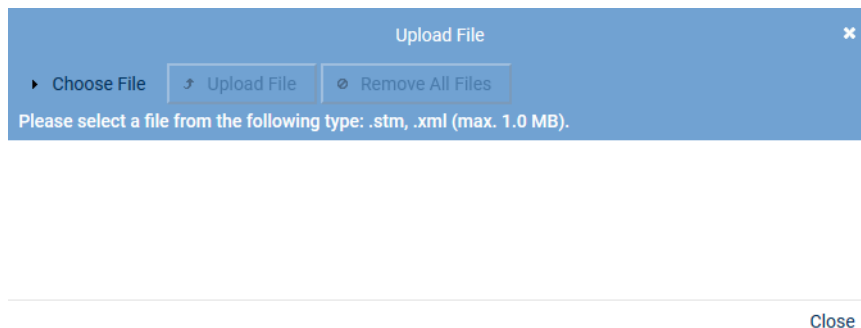


Fig. 220: Choose file

- Click on the button *Choose File*.
- Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
- Click on the button *Open*.
⇒ The selected file appears in the window *Upload File*.

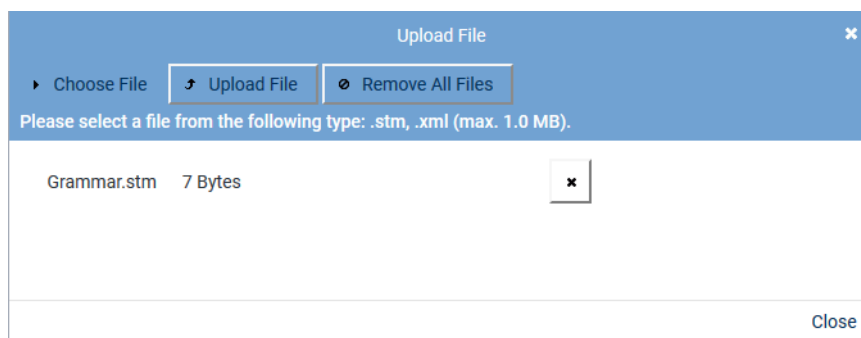



Fig. 221: Upload grammar

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

Assign integration type


- 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. 222: Create integration type

2. Enter the following parameters:

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

Tab. 47: Create integration type

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

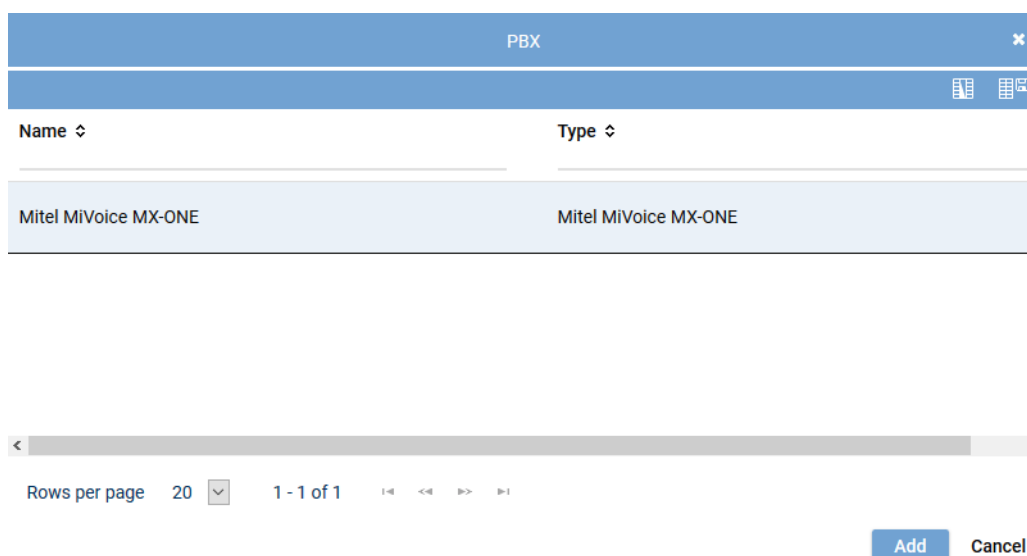


Fig. 223: Integrations - select PBX

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

Assign recording architecture for Multi-Server Recording

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

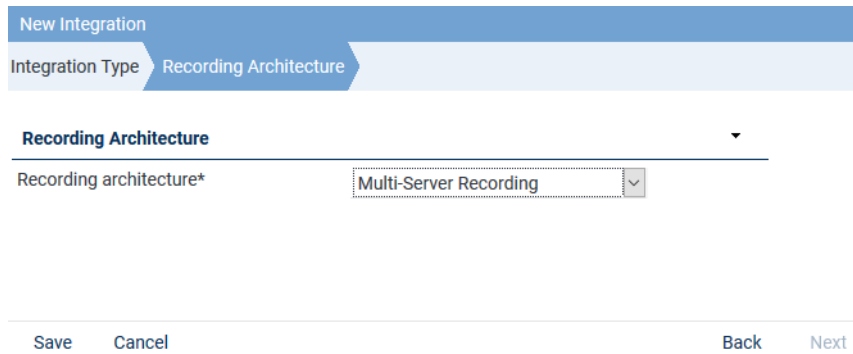


Fig. 224: Assign recording architecture - Multi-Server Recording

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




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

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



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

Configuration steps

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










Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA		X	
Step	Configuration				
Configure recording architecture	<div><div>✓</div><div></div></div>				
Configure CTI connection data	<div><div>✗</div><div></div></div>				
Configure monitor points	<div><div>✗</div><div></div></div>				
Global recording settings	<div><div>✗</div><div></div></div>				
Configure recording servers	<div><div>✗</div><div></div></div>				
Configure add-on	<div><div>✓</div><div></div></div>				
Configure miscellaneous settings	<div><div>✓</div><div></div></div>				

Fig. 225: Configuration steps of the integration

Configure recording architecture

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

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

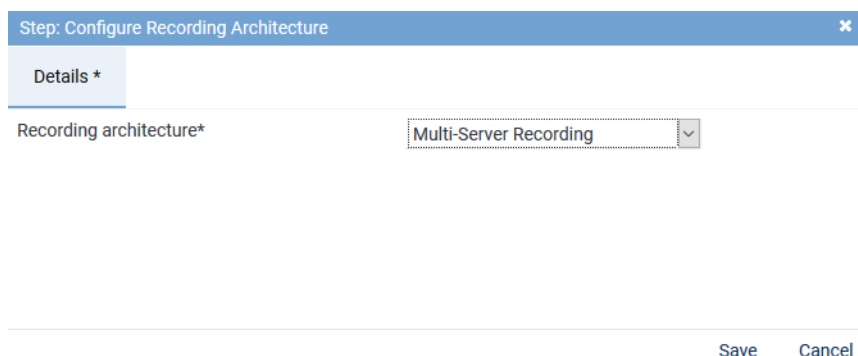



Fig. 226: Configuration step - Configure Recording Architecture


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

Configure CTI connection data

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.

In this configuration step, you configure grammars, connection data, and - if required - additional data.

CTIconnect module

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.
 - ⇒ In the detail view, the tabs *Module 1* and *Module 2* appear.



After an update, this section must be configured again.

Tab module 1

- Select the tab *Module 1* to configure the **CSTA** connection to the PBX.

By configuring module 1, you configure the recording type *Active Stream Recording* and/or *Intrusion*.

The **CSTA** connection is used to monitor the configured monitor points and to start the recording via the intrusion feature.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

CTIconnect Module ▼

Type CTIconnect active

Grammar name* ▼

Grammar version* ▼

Fig. 227: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 48: Configure CTIconnect module



After an update of the neo software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 1

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.

Connection Data ▼

PBX IP address

[Add](#) [Edit](#) [Delete](#)

Fig. 228: Configure connection data

1. In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

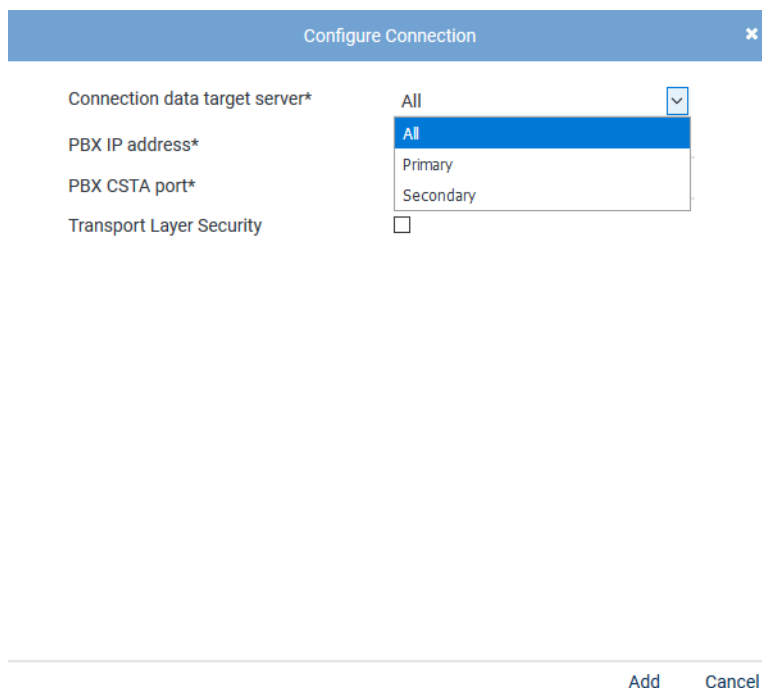


Fig. 229: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data target server</i>	In architectures with several servers, a menu appears for the servers for which this connection is meant. From the drop-down list, select the server that the connection is meant for.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the CSTA connection is supposed to be run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate the check box to use the connection with TLS .

Tab. 49: Configure connection data



A maximum of 20 MBG connections are possible.

3. Click on the button *Add* to apply the entries and to close the window.
4. If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

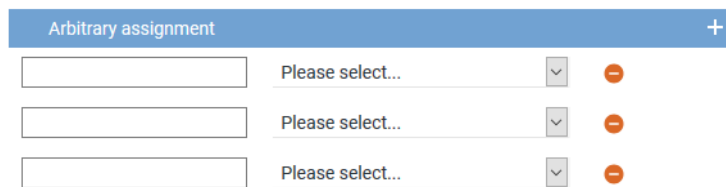
For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.



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

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


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



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

Fig. 230: Arbitrary assignment of the additional data

The following additional data are always available:

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

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



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



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

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

- Here, you can configure how long to wait for the CTI`connect` module to successfully connect with the PBX and how many connection attempts are to be made. If you have configured further connections, the system will switch to the next configured connection.



Only one CTI connection can be active at the same time. Connections cannot be established simultaneously.

Failover waiting time*	10
Failover repetitions*	3

Fig. 231: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI <code>connect</code> module attempts to establish another connection. Once this waiting time is over, new connection attempts are made depending on the configured number of failover repetitions.
<i>Failover repetitions</i>	Enter how many times the CTI <code>connect</code> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <code>connect</code> module makes as many connection attempts as have been configured for the failover repetitions. For each connection attempt, the configured failover waiting time is observed. If all connection attempts for the first configured connection have failed, the system switches to the next configured connection.



When configuring a failover architecture, the configuration of the switching conditions for the CTI connections must be considered. If only the last of several configured connections is established, the waiting times and repeated connection attempts of the previous connections must be taken into account. If the overall failover time configured for the recording architecture is too short, then a system failover may be triggered even though there would be a CTI connection which could be established successfully.



After an update, this section must be configured again.

Automatic identification of the recording type

The recording type of an end device is identified by means of analyzing the "Switching Function Representation" determined by CSTA as well as by means of the intrusion flag set in the configuration of the monitor points. The regular expression which can be configured here serves to determine whether the end device with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (invitation) can be recorded. The "Switching Function Representation" is extracted from the CSTA information and interpreted on basis of the "Switching Function Representation Format" (N<DN!SA/EXT>NM). The NM section is checked by means of the regular expression. It is checked whether the end device type is contained in the expression. If the expression matches the NM section, then the above mentioned recording mode is used for this end device.

Regular expression for phone type identification*

```
^[A-Za-z]*\\s[0-9]{4}[a-zA-Z]?$|^([0-9]{4})[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 232: Configure regular expression for phone type identification

A sensible expression has been saved for the parameter; however, it may be necessary to adjust the parameter to support other phones.

When entering regular expressions, several characters must be added to form escape sequences so that the meaning remains intact when the software extracts them, see <https://docs.oracle.com/javase/tutorial/java/data/characters.html>. When they are not added to form escape sequences, a simple "\", for instance, will be filtered out internally. When reading them in again, "\s" will then be interpreted as "s" only. Thus, the regular expression will not work anymore after reading them in. To retain the required "\s" upon reading the expression in, an additional "\\" must be added in the file to read "\\s".

For further information about regular expressions see https://en.wikipedia.org/wiki/Regular_expression.

A short introduction on regular expressions and a test tool to check the functionality of regular expression can be found at <https://www.freeformatter.com/java-regex-tester.html>.

The recording type is determined in the following order:

- *Intrusion*
If the feature Intrusion has been activated by means of the GUI, it is used for recording.
- *Invitation Pattern*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type.
- *SRC*
If the regular expression does not match for the respective phone, recording is done via [SRC](#).

Tab Module 2

1. Select the tab *Module 2* to configure the connection data of the [MBG](#).

By configuring module 2, you configure recording via the Mitel Border Gateway.

Step: Configure CTI Connection Data	
Module 1*	Module 2
Active	<input checked="" type="checkbox"/>

Fig. 233: Activate CTIconnect module 2

Active Tick the check box to display the configuration parameters and to activate the module.

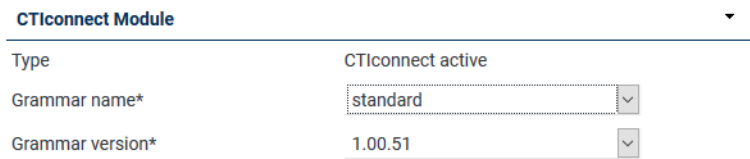
- ☒ Module 2 has been activated.
- ☐ Module 2 has not been activated.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.



CTIconnect Module	
Type	CTIconnect active
Grammar name*	standard
Grammar version*	1.00.51

Fig. 234: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 50: Configure CTIconnect module

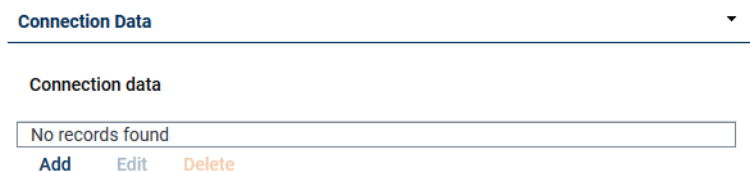


After an update of the neo software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 2

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.



Connection Data	
Connection data	
No records found	
Add	Edit Delete

Fig. 235: Configure connection data

1. In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

Configure Connection
✕

Connection data*
192.168.170.136

PBX port*
6810

Activate indirect recording
☐

Add Cancel

Fig. 236: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the connection data to the MBG or the SRC .
<i>PBX port</i>	Enter the port via which the MBG connection is supposed to run default 6810 .
<i>Activate indirect recording</i>	This option must not be activated for this type of recording.

Tab. 51: Configure connection data



A maximum of 20 MBG connections are possible.

3. Click on the button *Add* to apply the entries and to close the window.
4. If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

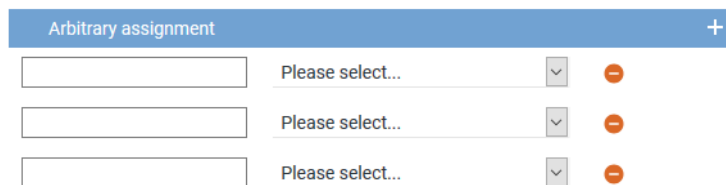



Fig. 237: Arbitrary assignment of the additional data

The following additional data are always available:

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

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



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



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

Configure monitor points

In this configuration step, the monitor points for the monitored end devices are configured.

1. In the main view in the line *Configure monitor points*, click on the button  (*Edit configuration step*).

⇒ The window *Step: Configure Monitor Points* appears in the detail view.

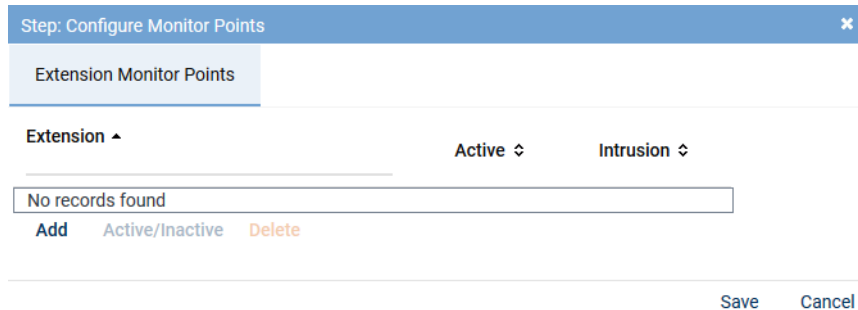


Fig. 238: Configuration step - configure monitor points

Extension monitor points



For the recording variant with **MBG** or **SRC**, the phones to be recorded must have been registered in the **SRC**. This does not apply to the recording variant with SIP Invite or Intrusion.

1. In the tab *Extension Monitor Points*, click on the button *Add* to add the extensions for the monitored end devices.
2. Select the menu item *Enter Extensions*.

⇒ The window *Add Extension Monitor Points* appears.

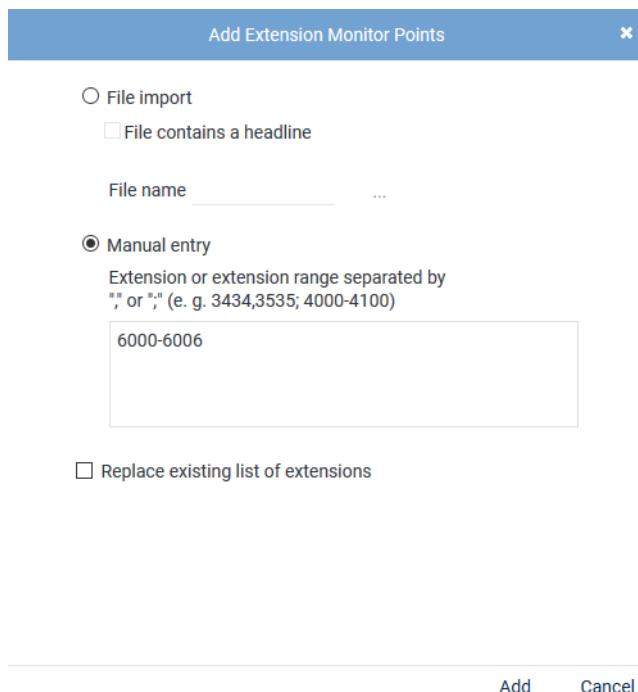






Fig. 239: Add extension monitor points

File import

Select this option to import extensions from an existing **CSV** file and add them to the table of extensions.

To import the file, proceed as follows:

- Click on the button  behind the field *File name*.

	<ul style="list-style-type: none"> Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>). <p><i>File contains a headline</i></p> <p>Activate this option so that this structure is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button  behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>).
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; all assignments of the PBXs which are listed in the detail view are overwritten and only the new assignment is applied.</p> <p><input type="checkbox"/> = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.</p>

- Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
- If errors have been detected, the window *Result* appears.
Click on the button *Display Error Report* to open the window *Error Report*.
To close the window *Error Report*, click on the button *Close*.
To close the window *Result*, click on the button *Close*.
- The configured extensions now appear in the detail view.

Step: Configure Monitor Points ✕

Extension Monitor Points

Extension ▾	Active ⇅	Intrusion ⇅
6000	✓	<input checked="" type="checkbox"/>
6001	✓	<input checked="" type="checkbox"/>
6002	✓	<input type="checkbox"/>
6003	✓	<input type="checkbox"/>
6004	✓	<input type="checkbox"/>
6005	✓	<input type="checkbox"/>
6006	✓	<input type="checkbox"/>

Add
Active/Inactive
Delete

Save
Cancel

Fig. 240: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Delete	To delete extension monitor points, select the respective extension in the list and click on the button <i>Delete</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Intrusion	<p>To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column <i>Intrusion</i>.</p> <p><input checked="" type="checkbox"/> = Intrusion feature has been activated.</p> <p><input type="checkbox"/> = Intrusion feature has not been activated.</p>


6. Click on the button *Save* to apply the settings and to finish this configuration step.



An extension which is supposed to be monitored and recorded by means of intrusion must be configured in the PBX to send an engaged signal if it is in a conversation. Only then, can the CTI^{connect} service initiate an intrude call and a silent conference.

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 15](#).

Global recording settings

- Click on the button  (*Edit configuration step*) in the line *Global recording settings* in the main view.

⇒ The window *Step: Global Recording Settings* appears.

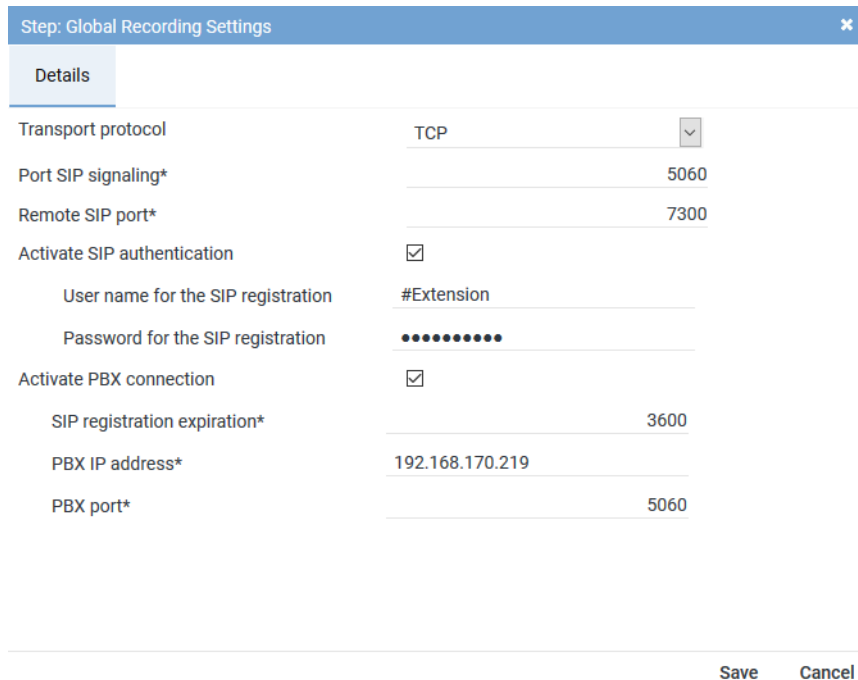


Fig. 241: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	From the drop-down list, select the used transport protocol for the SIP signaling between the recording server and the PBX. The following protocols are available: TCP = unencrypted UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling. On this port, the recording server can reach the Mitel end devices for the Active Streaming Recording by means of SIP to start the recording. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices, default 7300.
<i>Activate SIP authentication</i>	Activate the check box if the SIP registration is supposed to be authenticated. The option <i>Activate SIP authentication</i> is only used together with or as an expansion of the option <i>Activate PBX connection</i> .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration for the recording of the extensions used with the intrusion feature. The user name is configured in the PBX and applies for all extensions to be registered.
<i>Password of the SIP registration</i>	Enter the password for the SIP registration for the recording of the extensions used with the intrusion feature. The password is configured in the PBX and applies for all extensions to be registered.

Parameter	Value/Description
<i>Activate PBX connection</i>	Activate the check box if you would like to use the intrusion feature. When this option has been activated, the configured extensions of the recording server are registered on the PBX. Once the check box has been activated, the following parameters become active to be configured.
<i>SIP registration expiration</i>	Enter the period in seconds until the registration runs out.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port for the communication with the PBX, default 5060.


Tab. 52: Global recording settings

- Click on the button **Save** to apply the settings and to finish this configuration step.



After an update, this section must be configured again.

Configure recording servers

- Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.

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

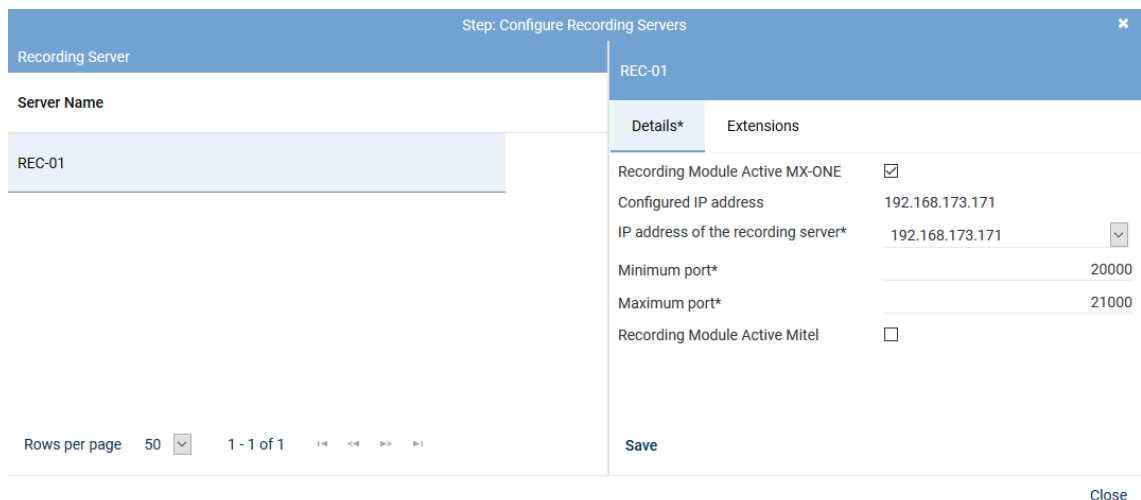


Fig. 242: Configuration step - Configure recording servers

- Activate the check box *Recording Module Active MX-ONE* so that the configuration parameters appear.
- Enter the following parameters:

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

Parameter	Value/Description
<i>Maximum port</i>	Enter the highest port configured on the PBX that is used to receive the RTP data from the recording server, e. g. 21000.

Tab. 53: Configure recording servers



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*.

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



After an update, this section must be configured again.

Tab Extensions

If you would like to use the feature *Intrusion* you have to configure an extension for the recording server.

- Select the tab *Extensions*.

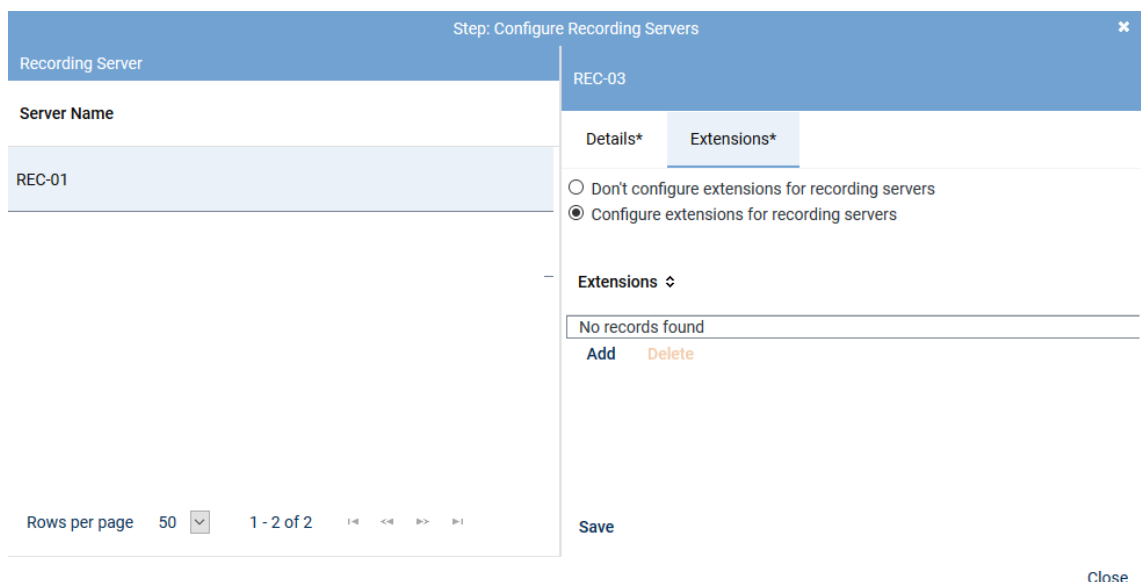


Fig. 243: Tab Extensions

Configure extensions of the recording server Activate this option if you would like to configure extensions for the recording server so make the feature call intrusion work.

If you use more than one recording server, assign separate extensions or extension ranges to the respective recording servers.

Make sure that the extensions for the recording server have not already been allocated to extension monitor points.

NOTICE! The extensions which have to be configured here are SIP extensions which have to be created on the PBX previously so that the recording server can register with these extensions on the PBX. These extensions are used exclusively for the intrusion feature.

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

Add Extensions ✕

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

9999

☐ Replace existing list of extensions

Add Cancel

Fig. 244: Add extensions

- In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.

Step: Configure Recording Servers ✕

Recording Server	REC-03
<p>Server Name</p> <p>REC-01</p>	<div style="background-color: #4f81bd; color: white; padding: 2px; text-align: center;"> Details* Extensions* </div> <p><input type="radio"/> Don't configure extensions for recording servers</p> <p><input checked="" type="radio"/> Configure extensions for recording servers</p> <p>Extensions ⇅</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 30px;"> 9999 </div> <p style="text-align: center;"> Add Delete </p> <p style="text-align: center;">Save</p>

Rows per page 50 ▼ 1 - 2 of 2 |< << >> >|

Close

Fig. 245: Added extensions

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

Configure add-on



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

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



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

Configure add-on for MiContact Center Enterprise

The add-on refers to the usage of MiContact Center Enterprise and must only be configured if MiContact Center Enterprise is used.

The integration runs in combination with the PBX and the recording server which is responsible for the actual conversation recording. The conversation events and the additional data are captured via MiContact Center Enterprise and sent to the recording server.

1. Select the add-on *MiContact Center Enterprise* in the detail view.

Step: Configure Add-on

Details *

Select add-on
☐ None
☒ MiContact Center Enterprise

CTIconnect Module

TypeCTIconnect passive
Grammar name*standard
Grammar version*2.00.01

Connection Data

Server name*192.168.170.205
Port*2601

Additional Data

CALLIDUniversal Call ID
PRIVATEDATAPlease select...
SERVICEGROUPIDPlease select...
SERVICEGROUPLISTPlease select...
IVRDATA1Please select...
IVRLABEL1Please select...
IVRDATA2Please select...
IVRLABEL2Please select...
IVRDATA3Please select...
IVRLABEL3Please select...
OASIDPlease select...

Arbitrary assignment

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

SaveCancel

Fig. 246: Configure add-on for MiContact Center Enterprise

Group field CTIconnect Module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 54: Configure CTIconnect module

Group field Connection Data

1. Set the following parameters in the group field *Connection Data*:

Parameter	Value/Description
Server Name	Enter the IP address or the name of the server that the MiContact Center Enterprise runs on.
Port	Enter the port for the connection to MiContact Center Enterprise.

Tab. 55: Configure connection data

Group field Additional Data

The following additional data is delivered in the protocol when using MiContact Center Enterprise:

- CALLID
- PRIVATEDATA
- SERVICEGROUPLIST
- IVRDATA1
- IVRLABEL1
- IVRDATA2
- IVRLABEL2
- IVRDATA3
- IVRLABEL3
- OASID

Arbitrary assignment

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



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

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



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


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

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

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

Fig. 247: Arbitrary assignment of the additional data

The following additional data are always available:

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

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



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



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

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI^{connect} service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

CTIconnect for Genesys T-Server

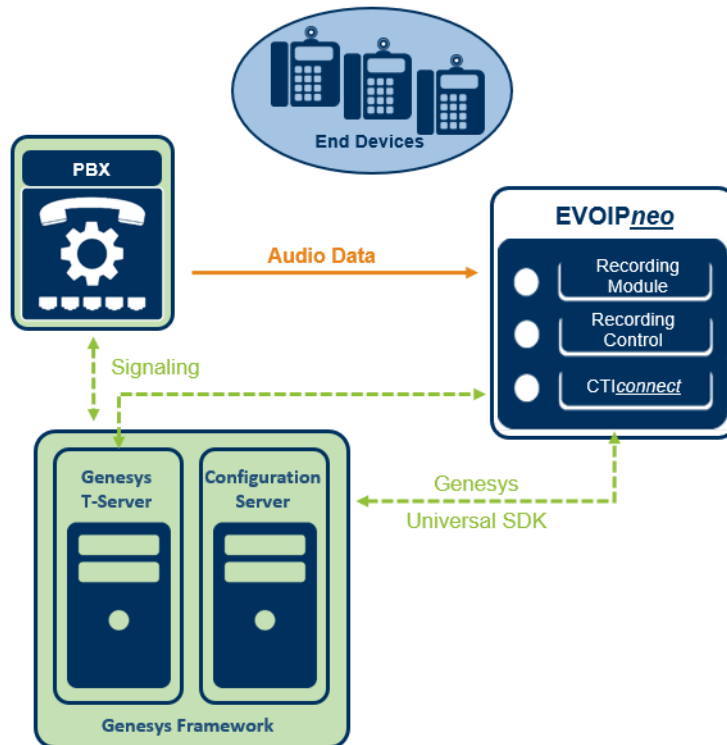


Fig. 248: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 311](#).

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.



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

When using a CTIconnect for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.


By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

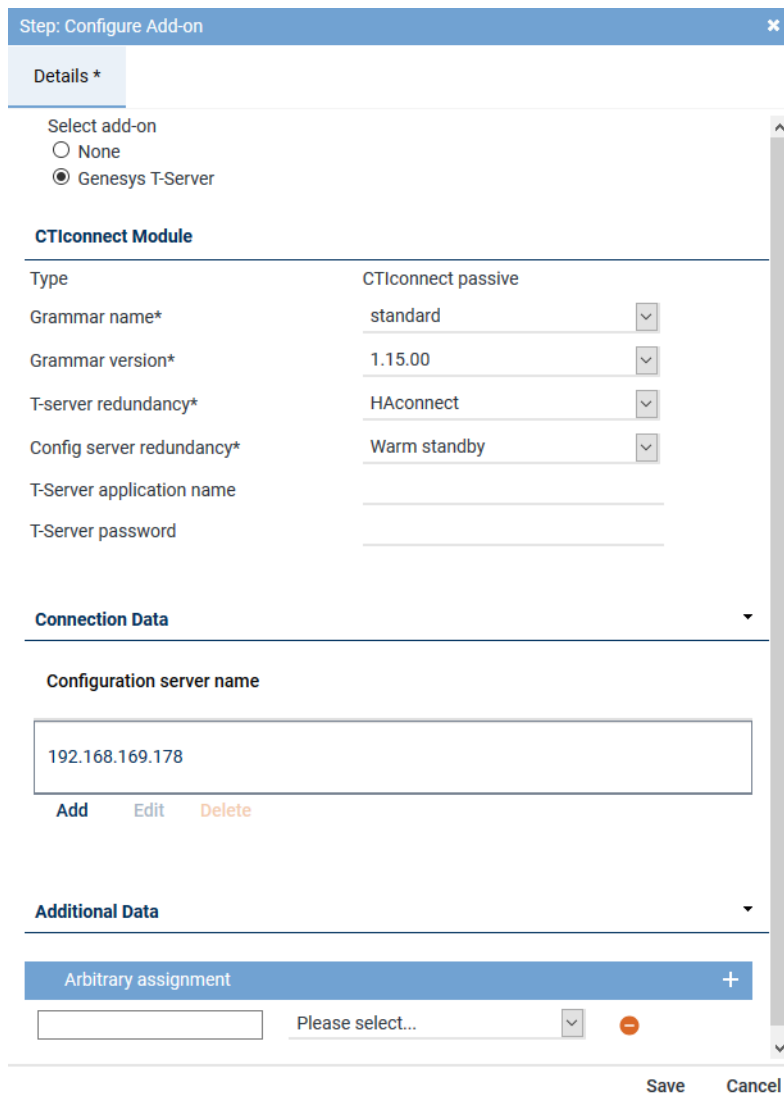
Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path
C:\ASC Product Suite\data\CTIConnectForGenesysT\.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button  (*Edit configuration step*) in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ Genesys T-Server

CTIconnect Module

Type CTIconnect passive

Grammar name* standard

Grammar version* 1.15.00

T-server redundancy* HAconnect

Config server redundancy* Warm standby

T-Server application name

T-Server password

Connection Data

Configuration server name

192.168.169.178

Add Edit Delete

Additional Data

Arbitrary assignment

Please select...

Save Cancel

Fig. 249: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 56: Configure add-on for Genesys T-Server

Group field Connection Data

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

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

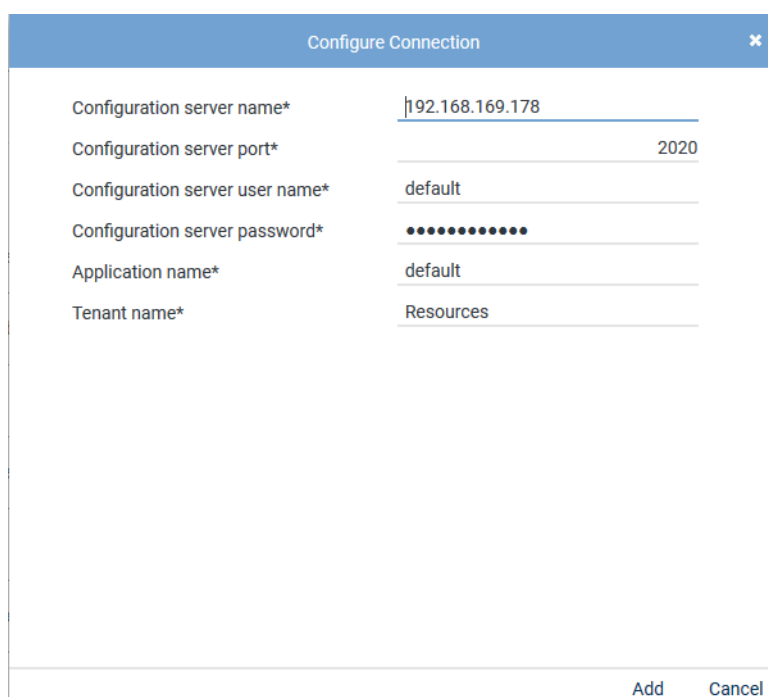


Fig. 250: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.

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

Tab. 57: Configure connection data

Group field Additional Data

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

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



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

Arbitrary assignment

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



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

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



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


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

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

Arbitrary assignment		+
<input type="text"/>	Please select...	⌵ -
<input type="text"/>	Please select...	⌵ -
<input type="text"/>	Please select...	⌵ -

Fig. 251: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

⌵

Save

Cancel

Fig. 252: Configure miscellaneous settings

2. Enter the following parameter:


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





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

Activate integration

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

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

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

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





















	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		
Step		Configuration		
Configure recording architecture				
Configure CTI connection data				
Configure monitor points				
Global recording settings				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 253: Activate integration

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






+ ×   Integration ▾ General			
Name ▾	Type ▾	Active ▾	Status ▾
	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	 

Fig. 254: 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.



For updates, the integration is stopped and deactivated. Once the update has been completed successfully, you must configure the integration again. Once the configuration has been completed, start the recording architecture again and activate the integration so that the new configuration is applied.

Deactivate/Delete integration

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

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









    Integration ▾ General			
Name ↕	Type ↕	Active ↕	Status ↕
 Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		

Fig. 255: Deactivate integration

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

7.3.2.4 Configure recording solution Multi-Server Failover

7.3.2.4.1 Create recording architecture

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

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

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

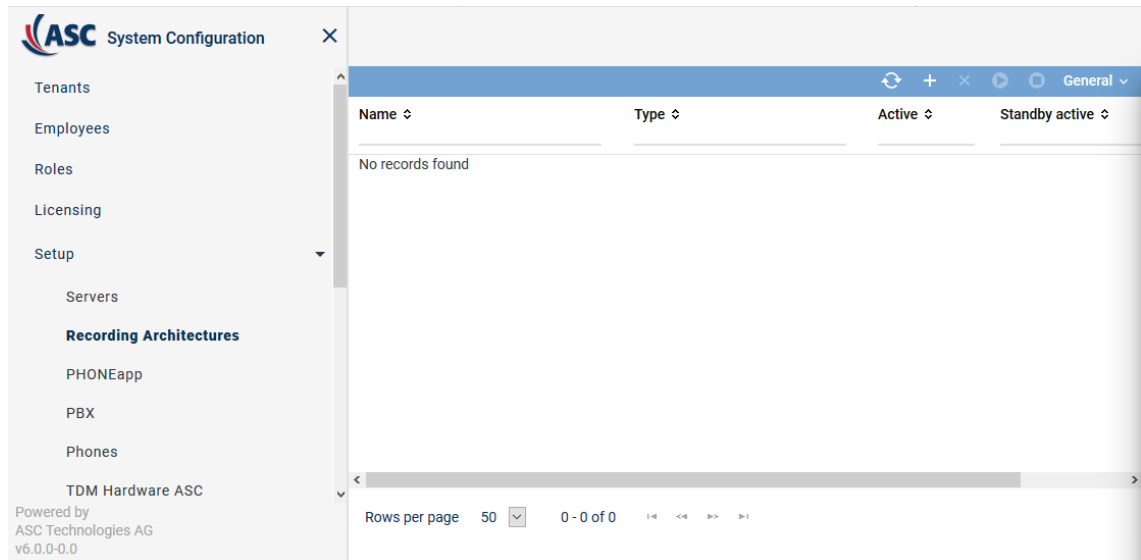





Fig. 256: Recording architectures - main view

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

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

Create recording architecture Multi-Server Failover

If there are several recording servers which are supposed to take over the tasks of another recording server in case of an error, you have to create a recording architecture of the type *Multi-Server Failover*.

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

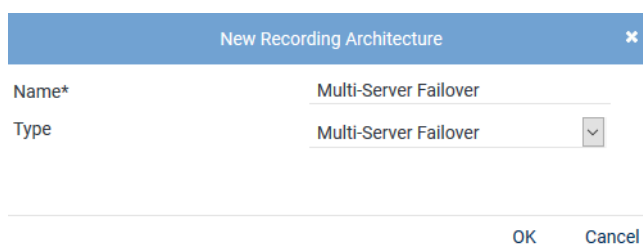


Fig. 257: Create recording architecture - Multi-Server Failover

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

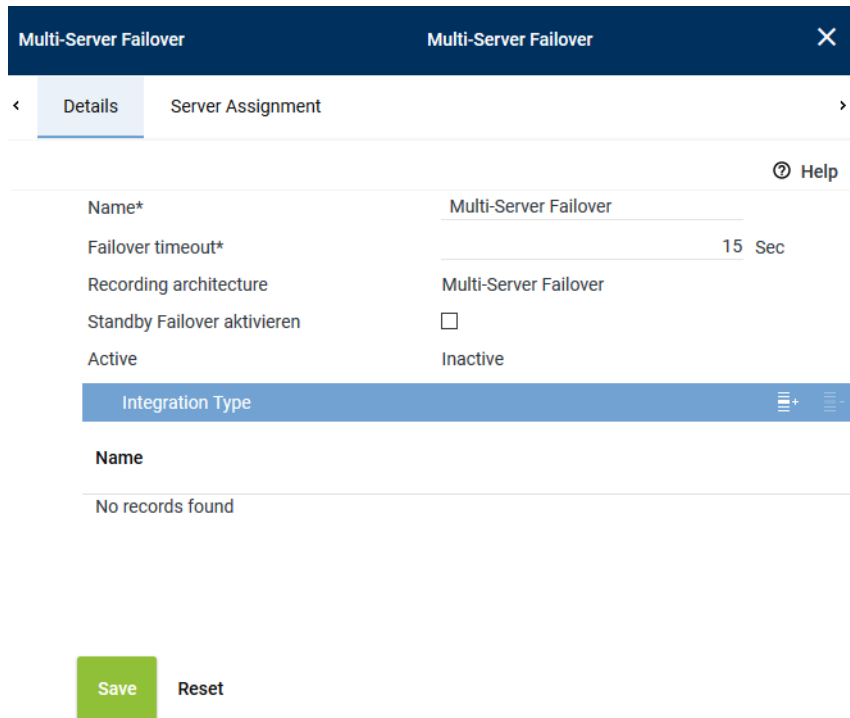



Fig. 258: Recording architecture - tab Details - Multi-Server Failover

As standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For further information about the configuration of failover architectures, see [chapter "Standby management for failover architectures"](#), p. 284.

<i>Failover timeout</i>	<p>Enter a timeout of a minimum of 15 seconds after which the failover process is supposed to start. Depending on the system architecture it may make sense to configure a longer timeout period. The timeout defines the elapse time until the failover process starts. If the status returns to <i>OK</i> within this time, then the failover process is not triggered.</p> <p>NOTICE! Check these parameters after an update and set the timeout to 15 seconds, if required.</p>
<i>Activate standby failover</i>	<p>Activate this option if you would like to ensure that the system switches back to the primary server in case of an error of the standby server.</p> <p>NOTICE! There is no check whether the primary database is working properly before switching back. As a result it is possible that both databases are in an undefined state.</p> <p>NOTICE! After switching back to the original primary server from the standby server, this option is deactivated. If the switching process is supposed to be carried out automatically in the event of a new error, you must activate this option again.</p>
<i>Active</i>	Shows the status of the recording architecture.

Add integration type

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

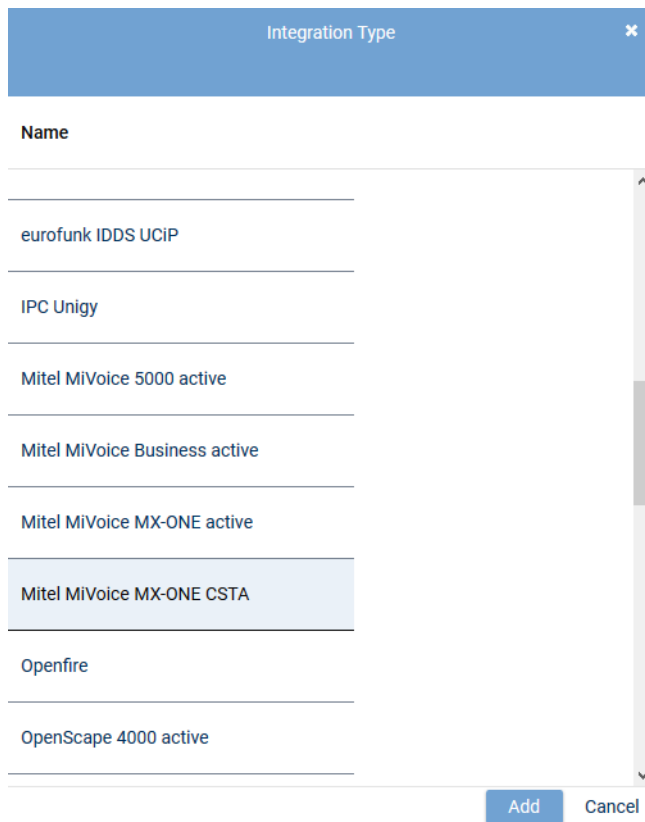


Fig. 259: Select integration type



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



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

- Select *Mitel MiVoice MX-ONE CSTA* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign servers for Multi-Server Failover

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

Group field Recording Control and CTIconnect

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

Multi-Server Failover

Multi-Server Failover

×

< Details*

Server Assignment*

>

Recording Control and CTIconnect

▼

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

Standby Server

▼

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

Recording Server

▼

< Recording Server

+

✎

⋮

Server ↕	Standby ↕
REC-01	REC-02

↑

↓

Save

Reset

Fig. 260: Recording Architecture - tab Server Assignment


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

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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 261: Recording Architecture - assign server - example



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




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

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

Group field Standby Server

1. Click on the button  behind the entry field *Recording control*.
2. Select the standby server for the *recording control module*.
3. Click on the button *Add*.
⇒ The name of the server now appears in the detail view.
4. Click on the button  behind the entry field *CTIconnect*.
5. Select the standby server for the *CTIconnect module*.
6. Click on the button *Add*.
⇒ The name of the server now appears in the detail view.

Group field Recording Server

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

Multi-Server Parallel Recording

Multi-Server Parallel Recording

×

<

Details*

Device Group 1*

Device Group 2*

>

Recording Control and CTIconnect

▼

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

Recording Server

▼

<

Recording Server

+

✎



⋮

Server ↕	Standby ↕
REC-01	REC-02

Save



Reset

Fig. 262: Add Recording Server




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



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



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

Activate recording architecture

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

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

Fig. 263: Recording architecture - activate recording architecture

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



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



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



For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See [chapter "Standby management for failover architectures"](#), p. 284.



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

7.3.2.4.2 Configure servers

Every server in your network that the *neo* software has been installed on is automatically identified as a server of the recording system and displayed in the main view of the Servers module. In the Servers module, you can configure the usage of the servers in your recording system.

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

ASC

System Configuration

Tenants

Employees

Roles

Licensing

Setup

Servers

Recording Architectures

PHONEapp

PBX

Phones

TDM Hardware ASC

Fig. 264: Servers - main view

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

Name Shows the name of the server.

IP Address Shows the **IP** address of the server.

<i>Path</i>	Shows the path of the server.
<i>Creation Date</i>	Date on which the server was installed.
<i>Updated</i>	Date on which the settings of the server were updated for the last time.

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

Toolbar of the Servers module

The toolbar offers the following functions.

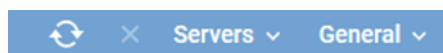




Fig. 265: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Delete</i>	Deletes the selected server configuration. This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see chapter "Administrate server locations" , p. 222.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see chapter "Administrate NTP server" , p. 239.
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>Save Table Configuration</i>	Saves the current table configuration of the main view as default view of the user.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
	<i>Reset Search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

Administrate server locations

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

Add server locations

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

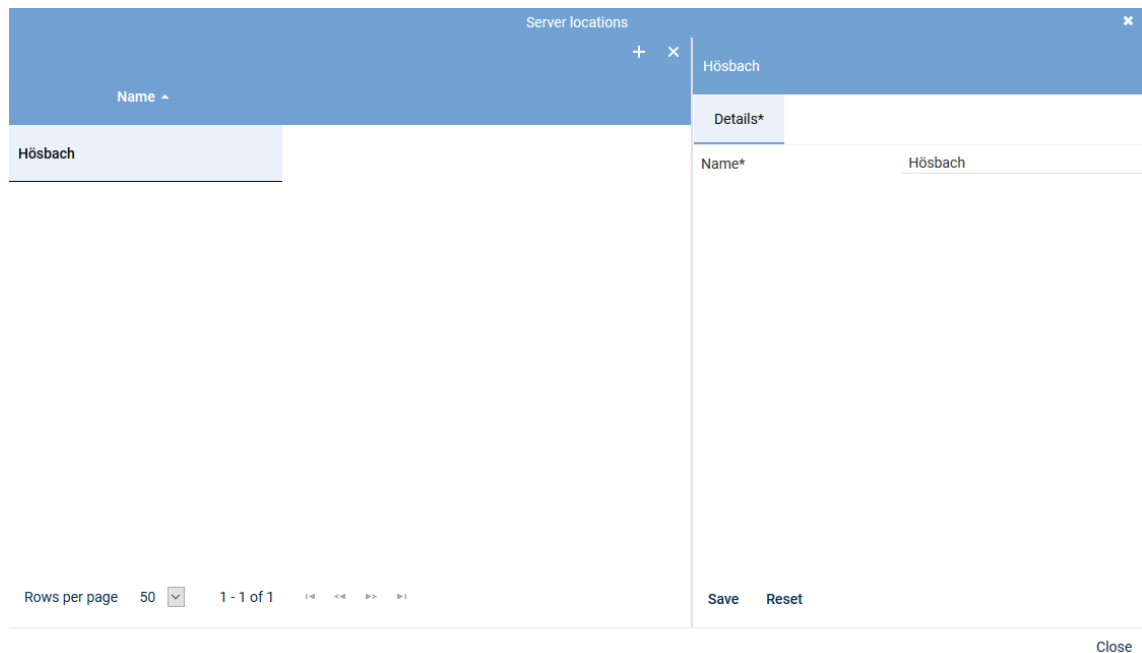



Fig. 266: Add server locations

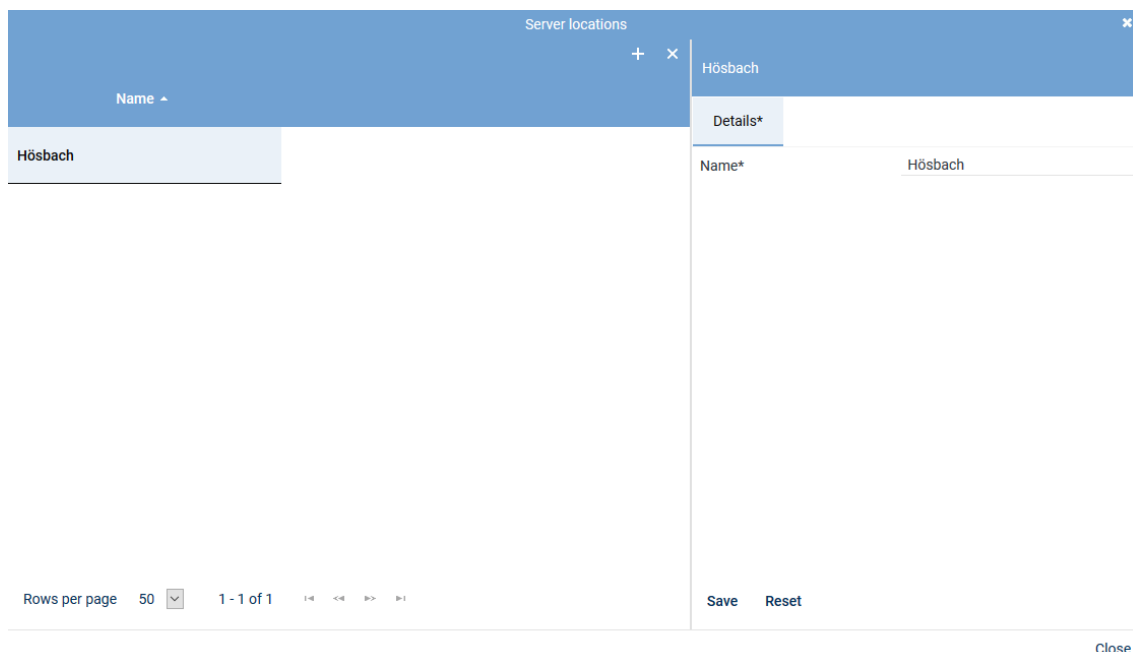
- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.
- To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
- To add further locations, repeat the last 3 steps.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

Delete server location




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

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



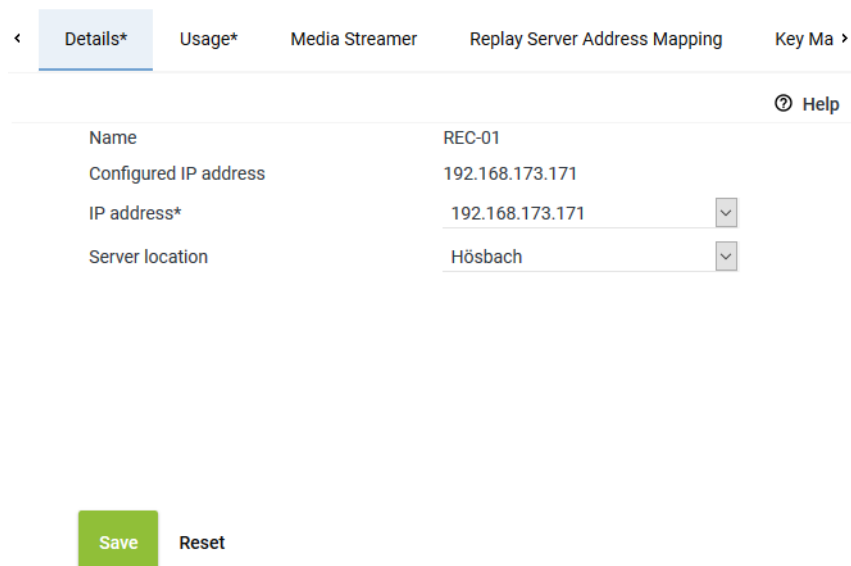
The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a table with one row containing the name "Hösbach". To the right of the table is a "Details*" tab. Below the tab, there is a form with a label "Name*" and a text input field containing "Hösbach". At the bottom of the window, there is a "Save" button and a "Reset" button. A "Close" button is located at the bottom right of the window frame.

Fig. 267: Delete server location



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

Tab Details

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



The screenshot shows a window titled "Servers - tab Details" with a close button (x) in the top right corner. Below the title bar is a tabbed interface with tabs: "Details*", "Usage*", "Media Streamer", "Replay Server Address Mapping", and "Key Ma". The "Details*" tab is active. Below the tabs is a form with the following fields:

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

At the bottom of the window, there is a "Save" button and a "Reset" button.

Fig. 268: Servers - tab Details

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

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

Tab Usage

- Click on the tab **Usage** to configure the purpose of usage.



Since a server can be used for several recording solutions, all purposes of use are listed. Note that some purposes of use do not apply for some recording solutions. As an example: You cannot use audio analysis or replay via phone in a chat recording.

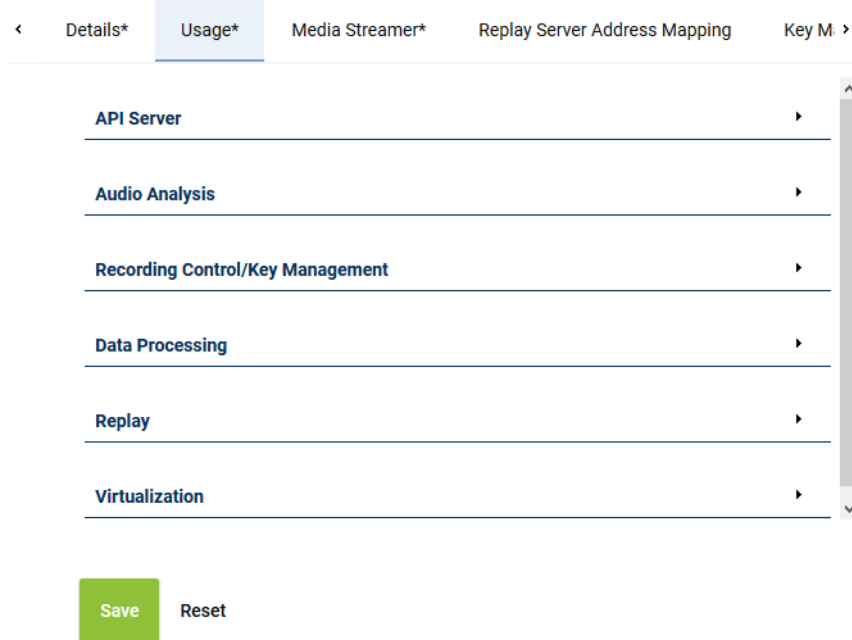


Fig. 269: Servers - tab Usage

Group field API Server

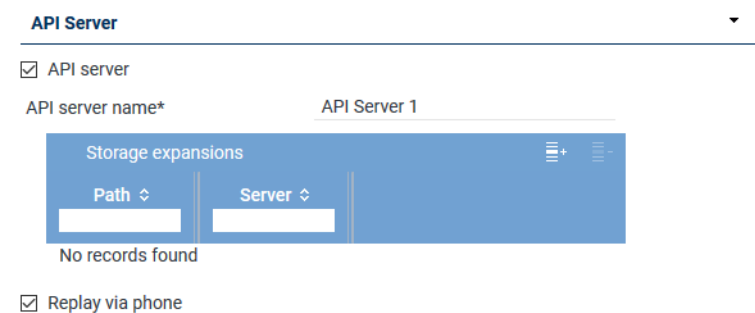


Fig. 270: Group field API Server



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



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


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

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

Parameter	Value/Description
<i>API server</i>	<p>Tick the check box to start the API server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>In order to be able to reach the API server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see chapter "Tab Replay Server Address Mapping", p. 235.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the storage expansions, see chapter "Add storage expansion for replay", p. 227. By clicking on the icon  (<i>Remove</i>), you can remove the storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> Application POWERplay<i>play</i> Pro Application POWERplay<i>play</i> Instant Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p>

Parameter	Value/Description
	NOTICE! In the tab <i>Media Streamer</i> , you have to assign this function to a PBX , see chapter "Tab Media Streamer", p. 234 . 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.

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

Rows per page 20 1 - 1 of 1

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

Fig. 271: Select storage expansion

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

Group field Audio Analysis

Audio Analysis


☒ Audio analysis (SAES mode)

Stream audio data from* + -

☐ Emotion detection

Stream audio data from* + -

Fig. 272: Group field Audio Analysis

Parameters	Value/Description
<i>Audio analysis</i>	<p>Activate this check box to use the server for audio analysis. The audio data is then streamed for audio analysis from the configured server to this server.</p> <ul style="list-style-type: none"> Stream audio data from From the list of available servers, select the server from which the audio data is supposed to be streamed for audio analysis via the button .

Parameters	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for the audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>

Tab. 58: Configure audio analysis

Group field Recording Control/Key Management

Recording Control/Key Management ▼

☒ Recording control/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 273: Group field Recording Control/Key Management

Parameters	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <u>CLIENT</u><i>command</i> or an API recording control or if you would like to use <i>Monitoring</i>. This feature is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the respective recording architecture you would like to use for the control.
- <i>neo key management</i>	<p>The function allows customer-specific encryption of the recordings. To be able to configure the key management, you have to activate the check box <i>Key management</i>.</p> <p>This function can only be activated if the license <code>ASC_KEY_MANAGEMENT</code> is available.</p> <p>For further information about the configuration of the key management refer to the administration manual <i>Configuration of servers and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 59: Configure Recording Control/Key Management

Group field Data Processing

Data Processing ▼

☒ Data storage

☒ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

from 11:59:36

to 11:59:36

Receives data from

Name	Only Replay
No records found	



☒ Archiving





☒ Export

☒ Import

Recording architecture Please choose... ▼


Fig. 274: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to allow the modification of the additional functions of data processing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer data only for replay to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay. The data is not stored on the target server but deposited in a cache temporarily in order to be replayed.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 230. By clicking on the icon  (<i>Remove</i>), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer data for storage to another server.</p> <p>If the function has been activated, you can select a server from the list <i>Target Server</i> to which the recorded data is supposed to be transferred for data storage purposes. In the drop-down list, all servers are displayed on which the function <i>Data Storage</i> has been activated. The data is copied to the target server and stored there.</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 230. By clicking on the icon  (Remove), you can remove the target server from the list. <p>NOTICE! Only those servers are displayed on which the function <i>Data Storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> Activate period of time <input checked="" type="checkbox"/> = Function has been activated. The fields for entering the time become active. Select the time via the rotating field for the period from – to. Active period of time <input type="checkbox"/> = Function has not been activated. <p>NOTICE! In distributed systems with slow network connections, the storage interval for the data transfer can be adjusted. The storage interval for the data transfer has to be configured by an ASC service technician or by an authorized partner company.</p>
<i>Receives data from</i>	<p>This table contains those servers which transfer data to this server.</p> <p>In the column <i>Name</i>, the name of the server appears from which data has been transferred.</p> <p>In the column <i>Only Replay</i>, the purpose of the transfer is displayed:</p> <p> = Data is transferred only for replay.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.
<i>Export</i>	Activate the check box <i>Export</i> to allow the export from this server.
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be stored on this server.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the recording architecture that fulfills this function. In the drop-down list, all recording architectures are displayed which enable this function as well. <p>NOTICE! If you would like to use a server for the import function on which no recording is supposed to take place, you can configure an architecture exclusively for the import.</p>

Tab. 60: Configure data storage

Add target server to a list

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



Target Server

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

Rows per page 20 1 - 6 of 6

Add Cancel

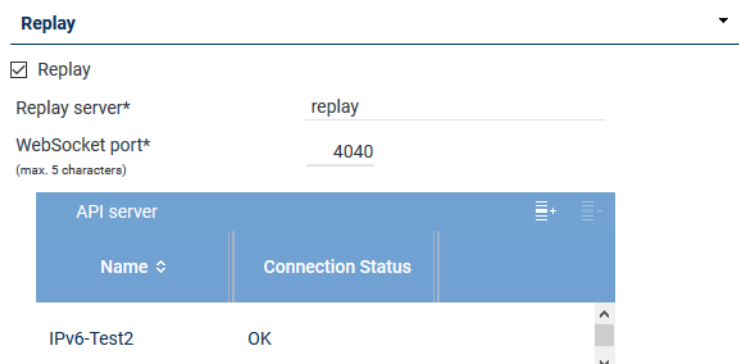
Fig. 275: Select server



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

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

Group field Replay



Replay

☒ Replay



Replay server* replay

WebSocket port* 4040
(max. 5 characters)

API server	
Name ↕	Connection Status
IPv6-Test2	OK

Fig. 276: Group field Replay

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

Parameter	Value/Description
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port (maximum of 5 characters)</i>	Enter the port via which the data to be replayed in <i>POWERplay</i> Web are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 232. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

Tab. 61: Configure replay

Search and replay functions



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

Add API server to a list

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


- If the replay server runs on a server with a local [API](#) server, it must not necessarily be assigned as the replay server always addresses the local [API](#) server first.
 - If the replay server runs on a separate server, you must assign at least one [API](#) server that the replay server can address.
 - If several [API](#) servers are available in the network, you can assign further [API](#) servers in addition to the local [API](#) server. The assigned [API](#) servers are addressed in order. For this reason, the local [API](#) server should always be first in the list.
- To assign an [API](#) server, click on the icon  (*Add*) in the toolbar of the list *API Server*.
 - Select the server from the list on which the [API](#) service is running.



Fig. 277: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 225](#).

- 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. 278: Group field Virtualization

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

Tab. 62: 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.

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

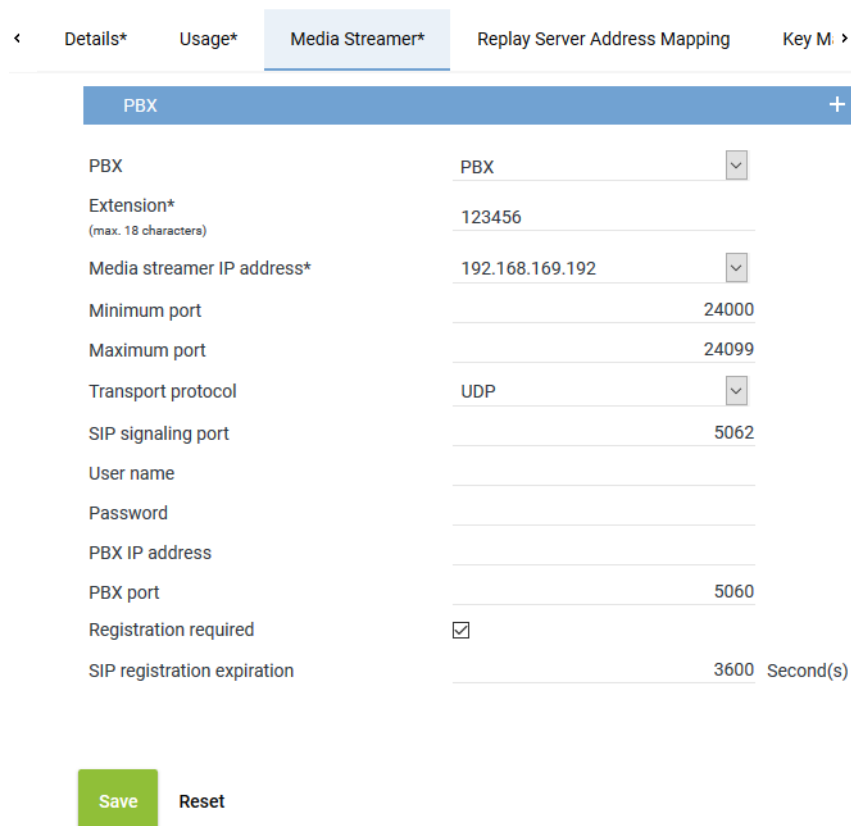
Tab Media Streamer

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

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



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



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

PBX +

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

Save Reset

Fig. 279: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX, see chapter "Create PBX", p. 240.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. In the drop-down list, all IP addresses of the server are displayed.</p> <p>If an external analog gateway has been integrated, select the IP address 169.254.254.100 in the drop-down list.</p>

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

Tab Replay Server Address Mapping

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

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



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

<

Details*

Usage*

Media Streamer*

Replay Server Address Mapping

Key M. >

Replay Server Addresses

| ✖

▼

Internal IP address/ port of the
replay server

192.168.169.192

:

4000

External address/ port of the
replay server

192.168.169.192

:

4000

Save

Reset

Fig. 280: Servers Module - tab Replay Server Address Mapping

Group field **Replay Server Addresses**

1. Enter the following parameters:

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

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



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

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



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



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

Tab Key Management

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

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

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

Key creation interval

☒ All

365 Day(s)

☐ Create key manually

Delay usage
until

0 Day(s)

0 Hour(s)

☐ Key expiration date
after

0 Day(s)

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

Save Reset

Fig. 281: Servers module - tab Key Management

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

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

In case of an error ... automatically

Select whether simple key management is supposed to be used if the neo key management does not work (e. g. if the service *DongleMan* fails). If you have not activated the option, no recording takes place as long as the neo key management has been activated but does not work.

☒ = In case of an error, simple key management is used as replacement.

☐ = In case of an error, no recording takes place as long as the neo key management has been activated. In this case, disable key management in the tab *Usage*.



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



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

Tab Keystore/Virtualization

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

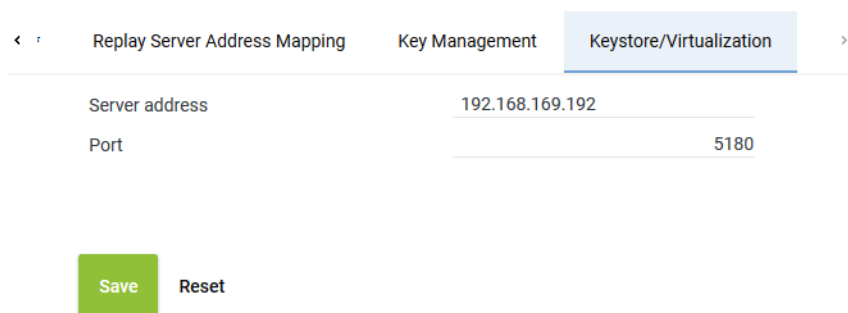
In this tab, you can configure the connection data for the service *DongleMan* for the neo key management and for the authentication of the VM.



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*.



Navigation: < Replay Server Address Mapping Key Management **Keystore/Virtualization** >

Server address	192.168.169.192
Port	5180

Buttons: Save Reset

Fig. 282: 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

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

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

Administrate NTP server

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

Add NTP server

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

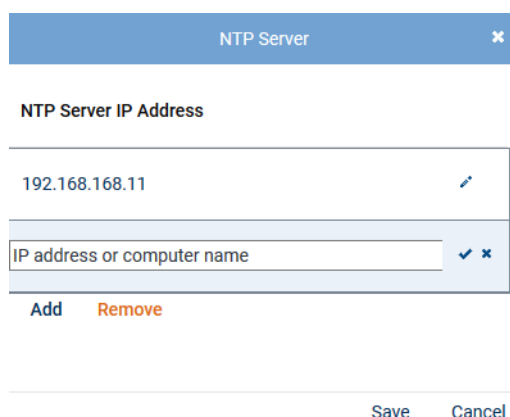





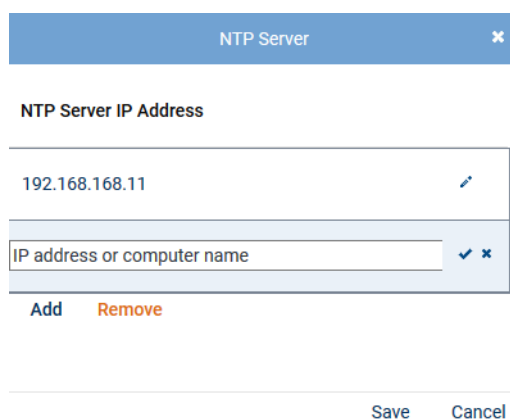
Fig. 283: Add NTP server

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

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




Edit IP address

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



NTP Server




NTP Server IP Address

192.168.168.11	
IP address or computer name	 

Add Remove

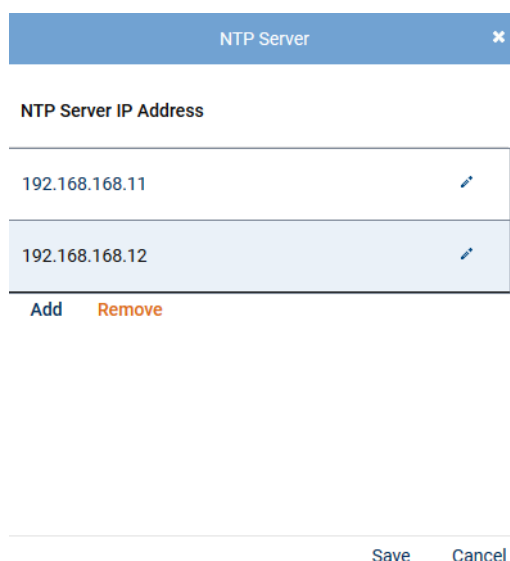
Save Cancel

Fig. 284: Edit IP address

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



Remove NTP server

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



NTP Server

NTP Server IP Address

192.168.168.11	
192.168.168.12	

Add Remove

Save Cancel

Fig. 285: Remove NTP server

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

7.3.2.4.3 Create PBX

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

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

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

⇒ The following window appears:

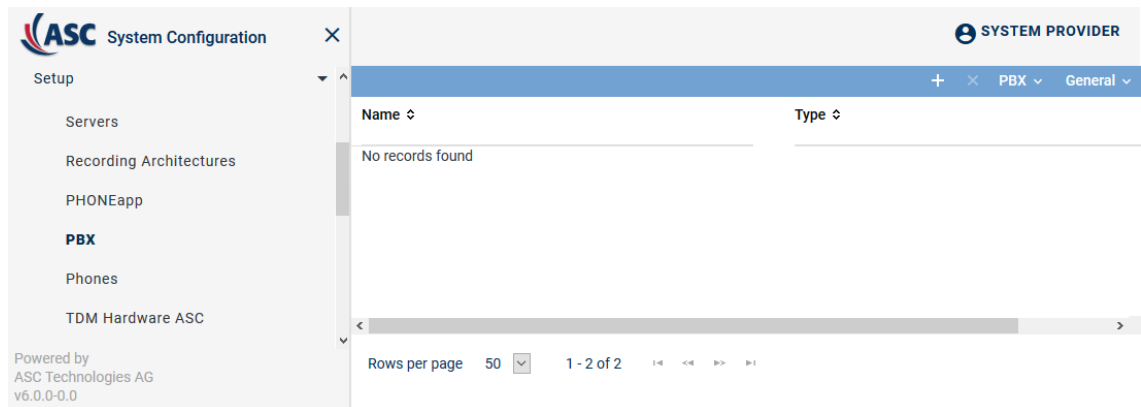


Fig. 286: Create new PBX

Toolbar of the PBX module

The toolbar offers the following functions.

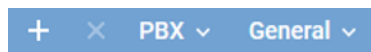




Fig. 287: Toolbar PBX module

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



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

Create new PBX

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

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

×

< Details* PHONEapp Configuration Web Service >

Name* Mitel MiVoice MX-ONE

PBX type* Mitel MiVoice MX-ONE ▼

Maximum length of extensions 4 ▼

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

Area code* 6021

Net code* 5963

Non Phone IPs

No records found
Add Delete

IPs to be Ignored

No records found
Add Delete

MACs to be Ignored

No records found
Add Delete

Save
Reset

Fig. 288: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 63: Create PBX

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

7.3.2.4.4 Assign recording resources

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

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

Assign extensions to tenants

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



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

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



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

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

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

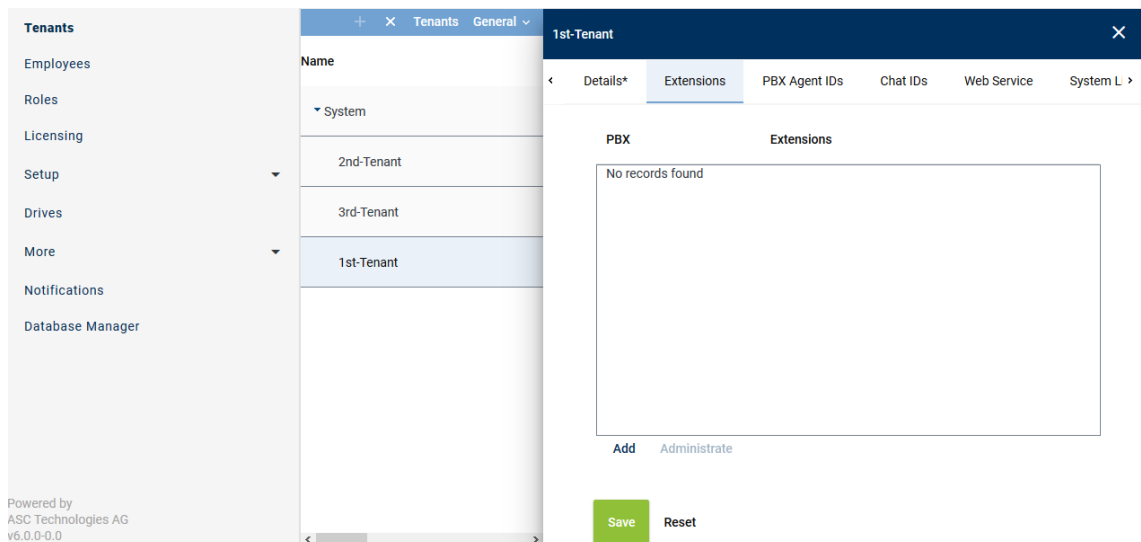


Fig. 289: Tenants - main view - tab Extensions

Add extensions

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

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 290: Assign extensions to tenants

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

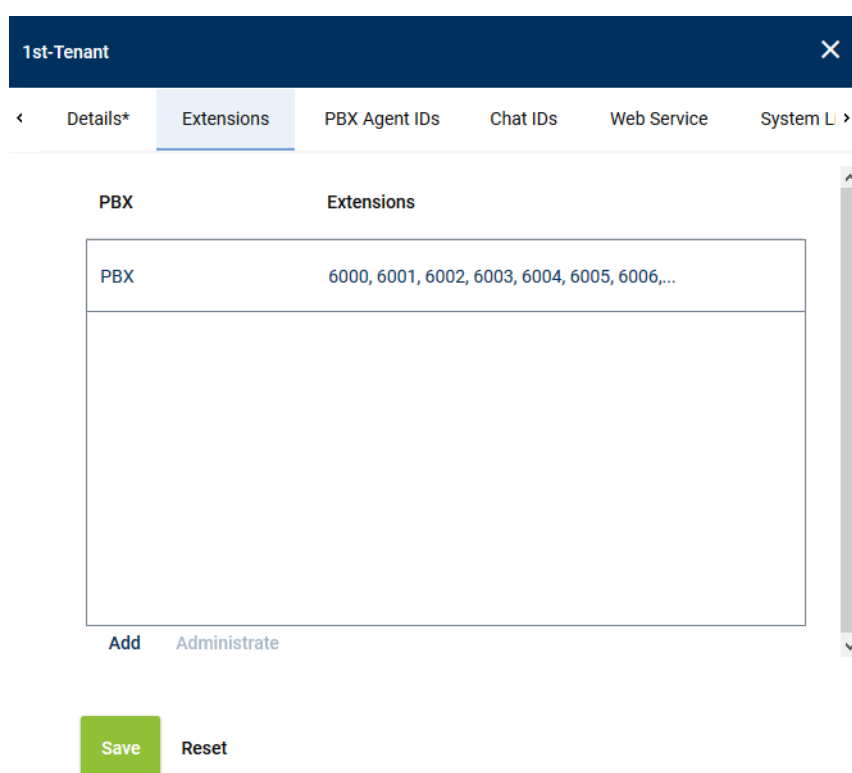
<i>File import</i>	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain 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.</p> <p>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.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p>

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

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

Remove extensions

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



1st-Tenant

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

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

Add Administrate

Save Reset

Fig. 291: 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.

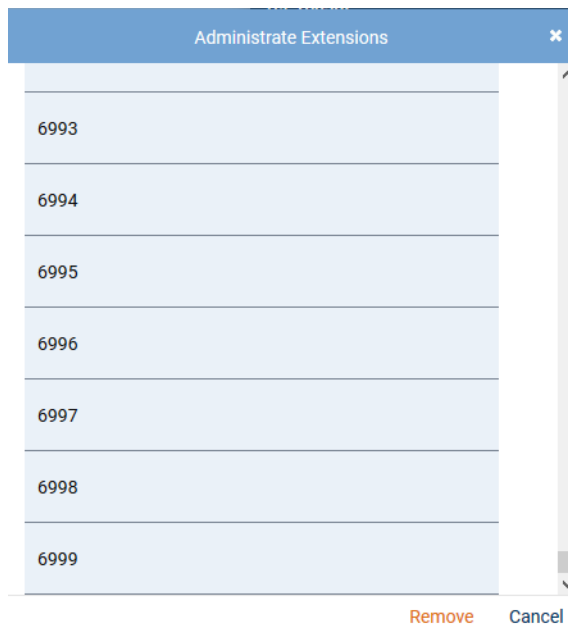


Fig. 292: Select extensions

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.

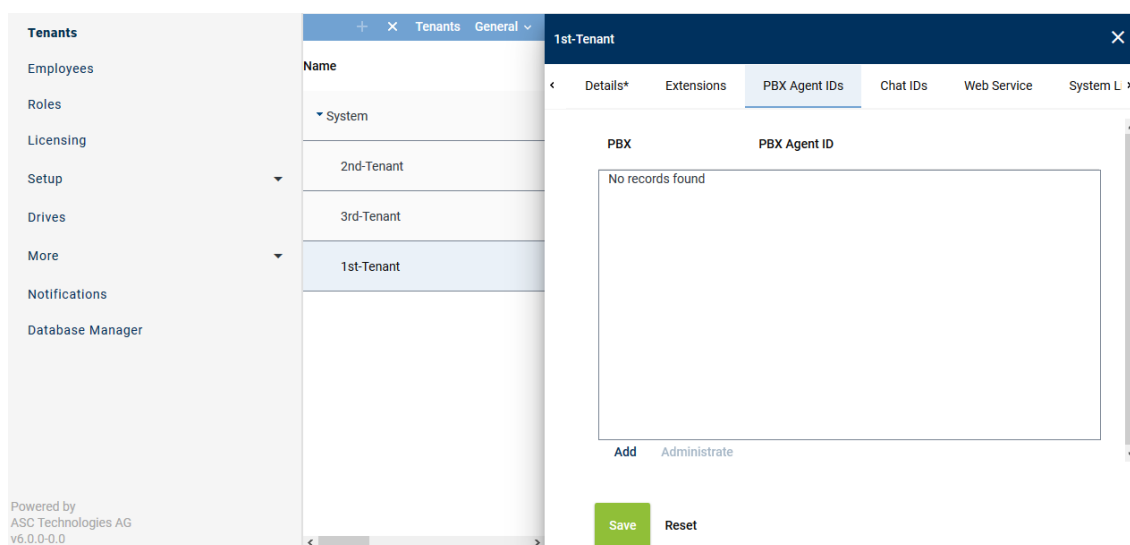


Fig. 293: Tenants - main view - tab PBX Agent ID

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:

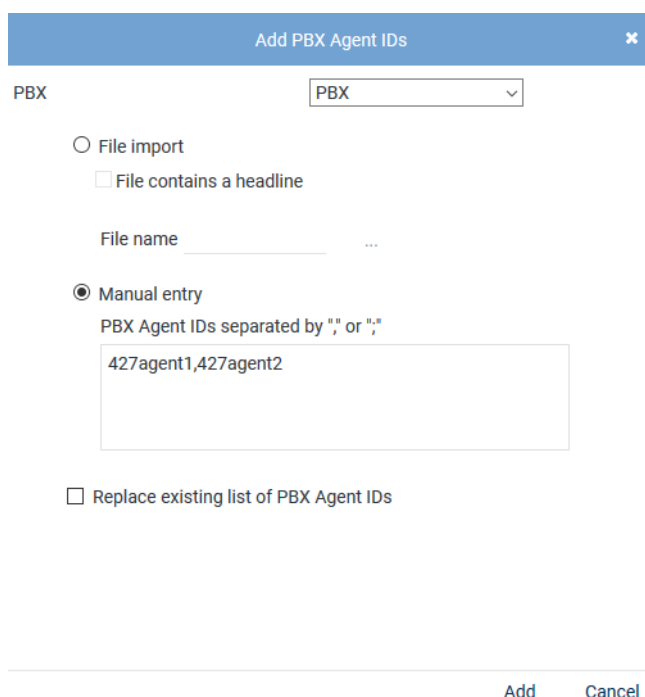


Fig. 294: Assign PBX Agent IDs to tenants

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

<i>File import</i>	Select this option to import the PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
Manual entry	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
Replace existing list of PBX Agent IDs	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = 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.</p>

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

Remove PBX Agent ID

- In the list, select the **PBX** for which you would like to remove the assigned PBX Agent IDs.
- Click the button *Administrate*.
- 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.

Administrate PBX Agent IDs
✕

ID

427agent1

427agent2

Remove Cancel

Fig. 295: 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*.

7.3.2.4.5 Configure additional data

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

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

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

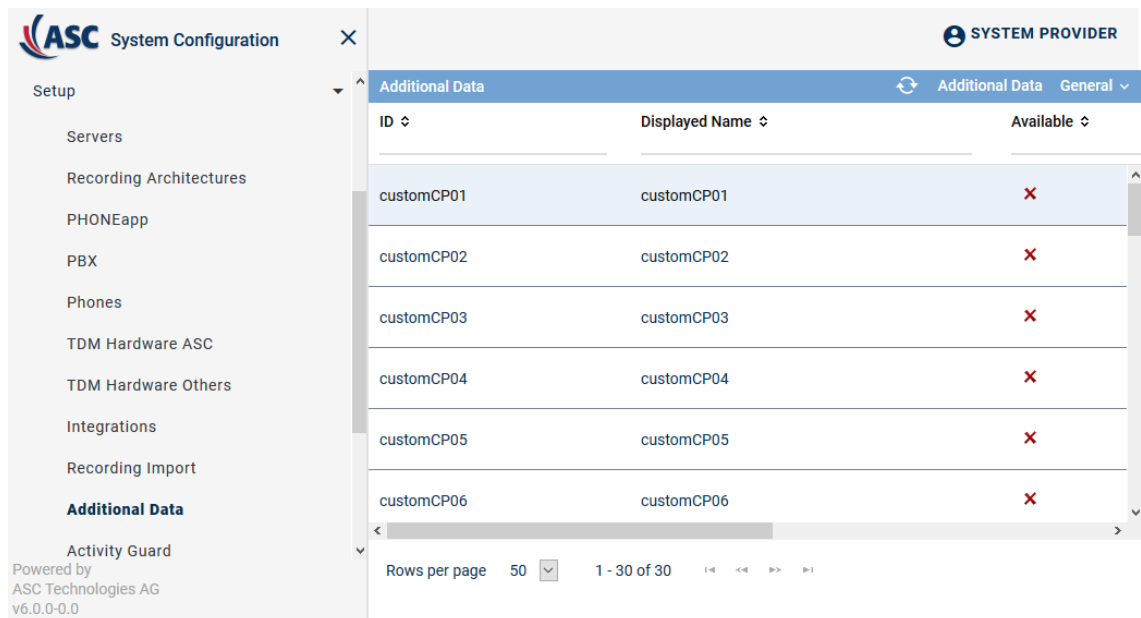


Fig. 296: Additional Data module main view

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

Change display name

Change Display Name
▼







Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 297: Configure additional data

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

Availability

Availability
▼

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

Save

Reset

Fig. 298: Additional data - configure availability

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



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



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

7.3.2.4.6 Create integration for Multi-Server Failover

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

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

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

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

⇒ The following window appears:

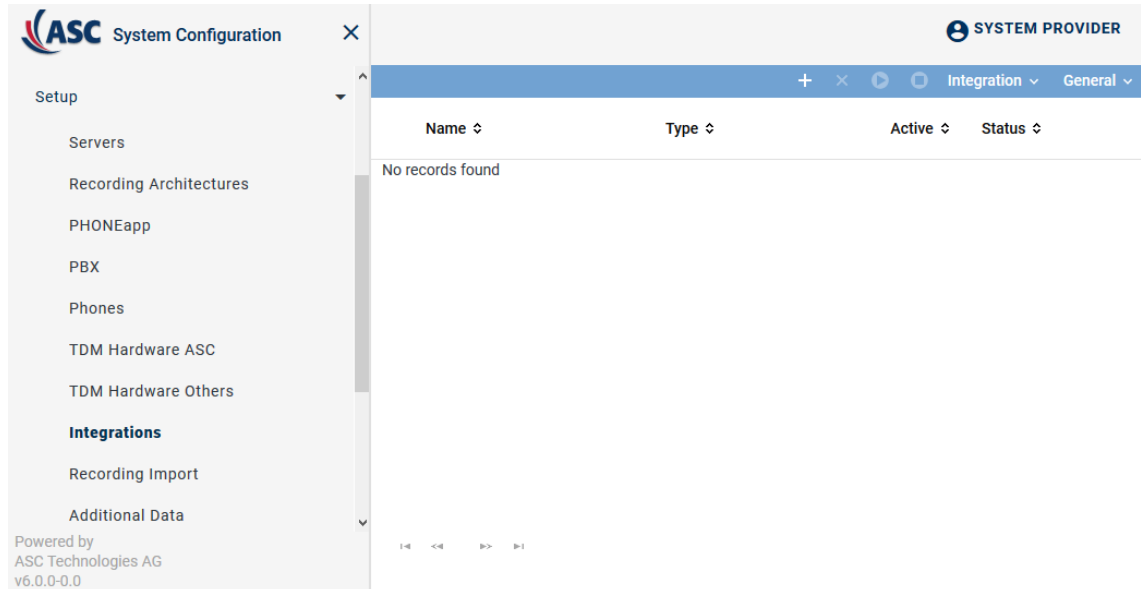




Fig. 299: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 300: Toolbar Integrations module

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

<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

Import grammar

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

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

1. To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.
⇒ The window *Upload File* appears.

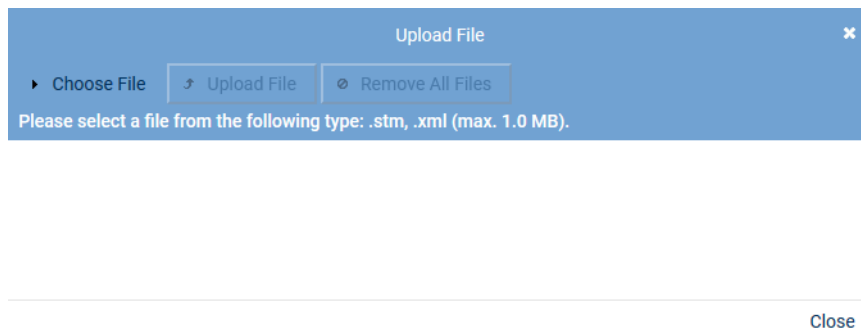


Fig. 301: Choose file

2. Click on the button *Choose File*.
3. Select the respective grammar of the file type *.stm* or *.xml* via the Explorer.
4. Click on the button *Open*.
⇒ The selected file appears in the window *Upload File*.

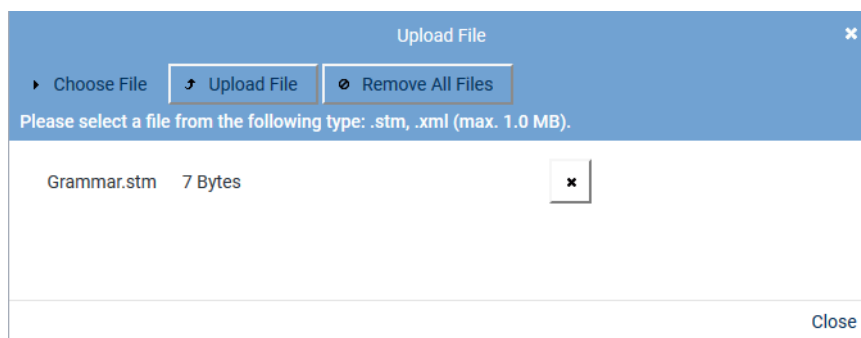




Fig. 302: Upload grammar

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

Assign integration type

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





Fig. 303: Create integration type

2. Enter the following parameters:

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

Tab. 64: Create integration type

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

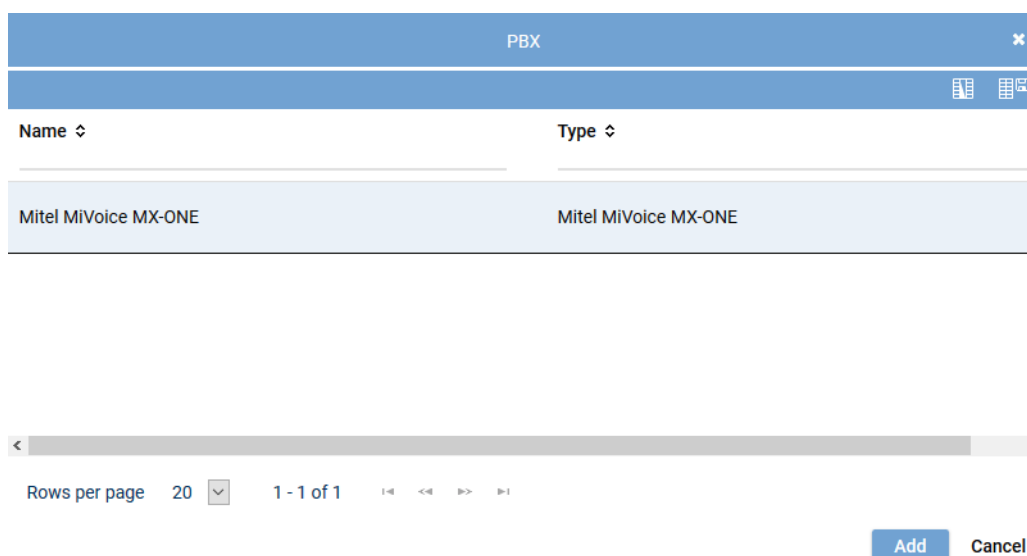
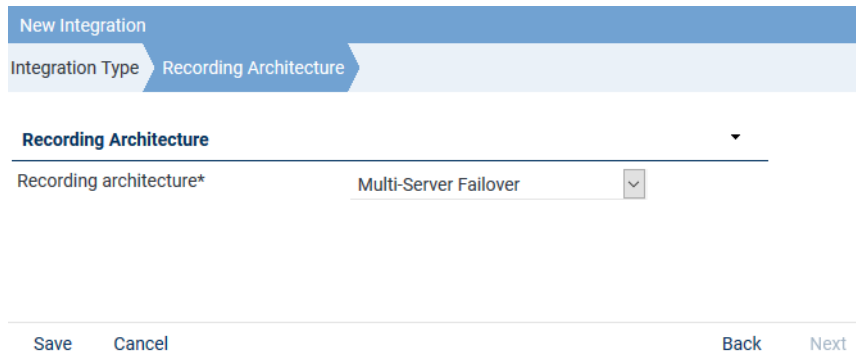


Fig. 304: Integrations - select PBX

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

Assign recording architecture for Multi-Server Failover

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Failover

Save Cancel Back Next

Fig. 305: Assign recording architecture - Multi-Server Failover


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



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

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

Configuration steps

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









Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA		✖		⚙	
Step	Configuration						
Configure recording architecture	✓						
Configure CTI connection data	✖						
Configure monitor points	✖						
Global recording settings	✖						
Configure recording servers	✖						
Configure add-on	✓						
Configure miscellaneous settings	✓						

Fig. 306: 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.

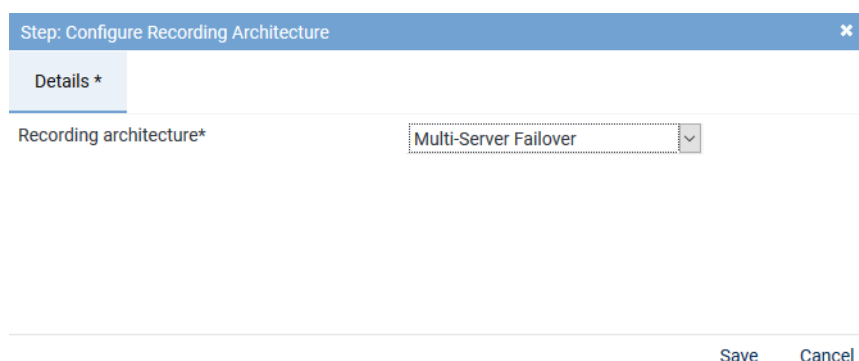



Fig. 307: Configuration step - Configure Recording Architecture


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

Configure CTI connection data

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.

In this configuration step, you configure grammars, connection data, and - if required - additional data.

CTIconnect module

- In the main view in the line *Configure CTI connection data*, click on the button  (*Edit configuration step*) to configure the CTI connection data.
⇒ In the detail view, the tabs *Module 1* and *Module 2* appear.



After an update, this section must be configured again.

Tab module 1

- Select the tab *Module 1* to configure the **CSTA** connection to the PBX.

By configuring module 1, you configure the recording type *Active Stream Recording* and/or *Intrusion*.

The **CSTA** connection is used to monitor the configured monitor points and to start the recording via the intrusion feature.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

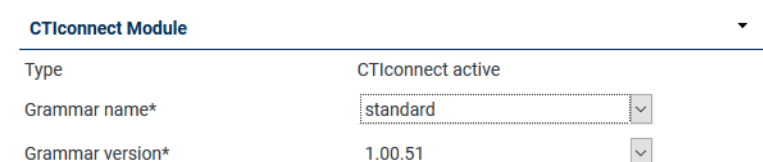


Fig. 308: Configure CTIconnect module

- Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 65: Configure CTIconnect module



After an update of the *neo* software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 1

In this group field, you can configure the connection data to the CTI*connect* module.

In case, the connection to the CTI*connect* module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.

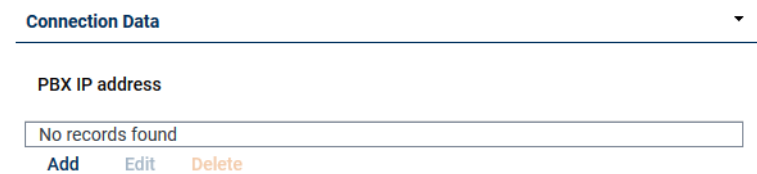


Fig. 309: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

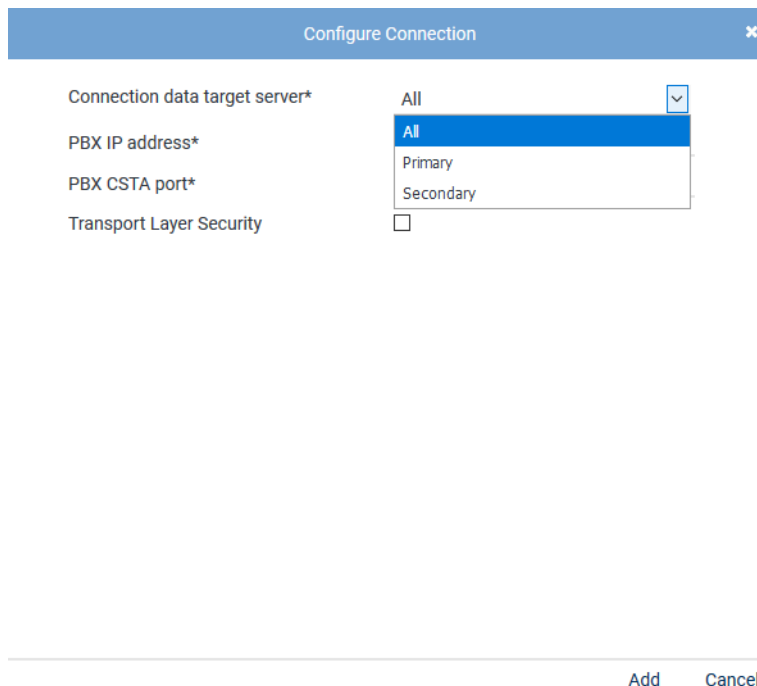


Fig. 310: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
Connection data target server	In architectures with several servers, a menu appears for the servers for which this connection is meant.

Parameter	Value/Description
	From the drop-down list, select the server that the connection is meant for.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the CSTA connection is supposed to be run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate the check box to use the connection with TLS .

Tab. 66: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

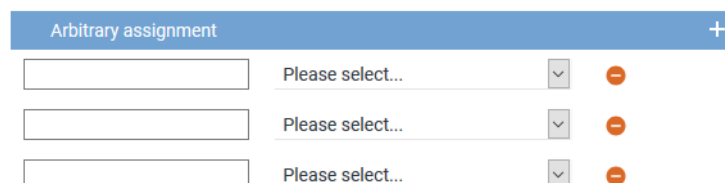



Fig. 311: Arbitrary assignment of the additional data

The following additional data are always available:

- Start time*
- End time*

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

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



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



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

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

1. Here, you can configure how long to wait for the CTI`connect` module to successfully connect with the PBX and how many connection attempts are to be made. If you have configured further connections, the system will switch to the next configured connection.



Only one CTI connection can be active at the same time. Connections cannot be established simultaneously.

Failover waiting time*	10
Failover repetitions*	3

Fig. 312: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI <code>connect</code> module attempts to establish another connection. Once this waiting time is over, new connection attempts are made depending on the configured number of failover repetitions.
<i>Failover repetitions</i>	Enter how many times the CTI <code>connect</code> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <code>connect</code> module makes as many connection attempts as have been configured for the failover repetitions. For each connection attempt, the configured failover waiting time is

observed. If all connection attempts for the first configured connection have failed, the system switches to the next configured connection.



When configuring a failover architecture, the configuration of the switching conditions for the CTI connections must be considered. If only the last of several configured connections is established, the waiting times and repeated connection attempts of the previous connections must be taken into account. If the overall failover time configured for the recording architecture is too short, then a system failover may be triggered even though there would be a CTI connection which could be established successfully.



After an update, this section must be configured again.

Automatic identification of the recording type

The recording type of an end device is identified by means of analyzing the "Switching Function Representation" determined by CSTA as well as by means of the intrusion flag set in the configuration of the monitor points. The regular expression which can be configured here serves to determine whether the end device with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (invitation) can be recorded. The "Switching Function Representation" is extracted from the CSTA information and interpreted on basis of the "Switching Function Representation Format" (N<DN!SA/EXT>NM). The NM section is checked by means of the regular expression. It is checked whether the end device type is contained in the expression. If the expression matches the NM section, then the above mentioned recording mode is used for this end device.

Regular expression for phone type identification*

```
^[A-Za-z]*\\s[0-9]{4}[a-zA-Z]?$|^*[0-9]{4}[a-zA-Z]?$|^*DBC[0-9]{5}$
```

Fig. 313: Configure regular expression for phone type identification

A sensible expression has been saved for the parameter; however, it may be necessary to adjust the parameter to support other phones.



When entering regular expressions, several characters must be added to form escape sequences so that the meaning remains intact when the software extracts them, see <https://docs.oracle.com/javase/tutorial/java/data/characters.html>. When they are not added to form escape sequences, a simple "\s", for instance, will be filtered out internally. When reading them in again, "\s" will then be interpreted as "s" only. Thus, the regular expression will not work anymore after reading them in. To retain the required "\s" upon reading the expression in, an additional "\\" must be added in the file to read "\\s".



For further information about regular expressions see https://en.wikipedia.org/wiki/Regular_expression..



A short introduction on regular expressions and a test tool to check the functionality of regular expression can be found at <https://www.freeformatter.com/java-regex-tester.html>.

The recording type is determined in the following order:

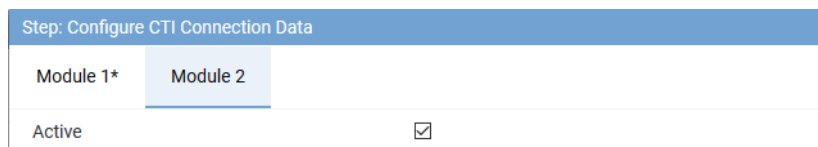
- *Intrusion*
If the feature Intrusion has been activated by means of the GUI, it is used for recording.
- *Invitation Pattern*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type.

- **SRC**
If the regular expression does not match for the respective phone, recording is done via **SRC**.

Tab Module 2

1. Select the tab *Module 2* to configure the connection data of the **MBG**.

By configuring module 2, you configure recording via the Mitel Border Gateway.



Step: Configure CTI Connection Data

Module 1* Module 2

Active ☒

Fig. 314: Activate CTIconnect module 2

Active Tick the check box to display the configuration parameters and to activate the module.

☒ Module 2 has been activated.

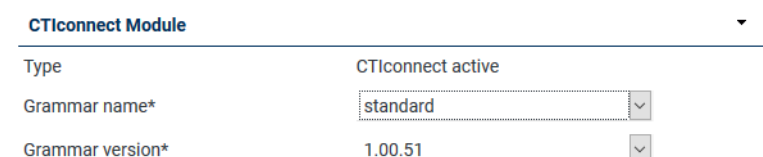
☐ Module 2 has not been activated.



After an update, this section must be configured again.

Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.



CTIconnect Module

Type CTIconnect active

Grammar name* standard

Grammar version* 1.00.51

Fig. 315: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
<i>Type</i>	Is filled automatically.
<i>Grammar name</i>	Select the name of the grammar from the drop-down list.
<i>Grammar version</i>	Select the current version of the grammar from the drop-down list.

Tab. 67: Configure CTIconnect module



After an update of the **neo** software, you must check the grammar versions. After the update, select the latest grammar from the drop-down list. If a customer-specifically adjusted grammar had been imported, check whether it continues to meet the requirements.

Group field Connection Data Module 2

In this group field, you can configure the connection data to the CTIconnect module.

In case, the connection to the CTIconnect module fails, the recording with the recording variant via the **MBG** continues with restricted additional data. Phone numbers and direction continue to be available.

Connection Data ▼

Connection data

No records found

[Add](#)
[Edit](#)
[Delete](#)

Fig. 316: Configure connection data

- In the group field *Connection Data* in the table *PBX IP address*, click on the button *Add*.
⇒ The window *Configure Connection* appears.

Configure Connection
✕

Connection data*	192.168.170.136
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>

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

Fig. 317: Configure connection

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the connection data to the MBG or the SRC .
<i>PBX port</i>	Enter the port via which the MBG connection is supposed to run default <i>6810</i> .
<i>Activate indirect recording</i>	This option must not be activated for this type of recording.

Tab. 68: Configure connection data



A maximum of 20 MBG connections are possible.

- Click on the button *Add* to apply the entries and to close the window.
- If you use additional modules, another device group or multiple connections, repeat the configuration steps accordingly.

Group field Additional Data

In this group field, you can select fields in which additional data delivered for a conversation by the PBX or by an application's add-on is supposed to be displayed.

The content of the database fields is then displayed in the respective column in the players.

Depending on the PBX type, different parameters are available and can be assigned independently.

Arbitrary assignment

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



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

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



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

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

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

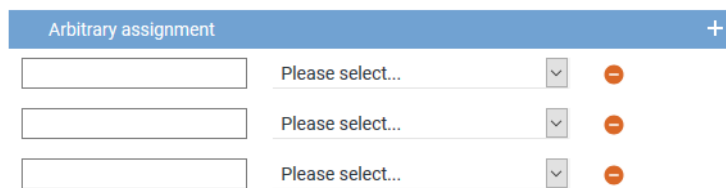



Fig. 318: Arbitrary assignment of the additional data

The following additional data are always available:

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

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




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



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

Configure monitor points

In this configuration step, the monitor points for the monitored end devices are configured.

1. In the main view in the line *Configure monitor points*, click on the button  (*Edit configuration step*).
⇒ The window *Step: Configure Monitor Points* appears in the detail view.

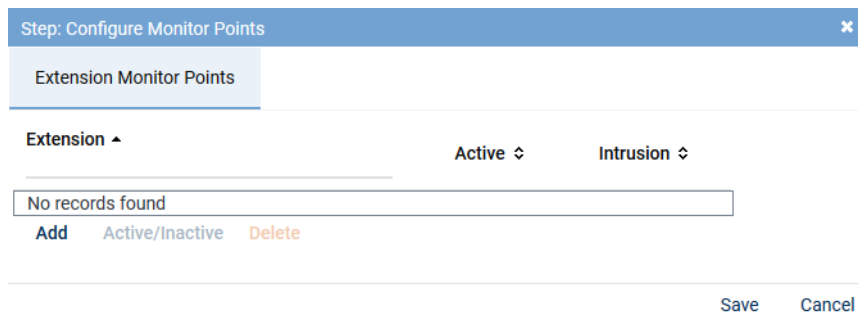


Fig. 319: Configuration step - configure monitor points

Extension monitor points



For the recording variant with **MBG** or **SRC**, the phones to be recorded must have been registered in the **SRC**. This does not apply to the recording variant with SIP Invite or Intrusion.

1. In the tab *Extension Monitor Points*, click on the button *Add* to add the extensions for the monitored end devices.
2. Select the menu item *Enter Extensions*.
⇒ The window *Add Extension Monitor Points* appears.

Add Extension Monitor Points
✕

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry





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

6000-6006

☐ Replace existing list of extensions

Add Cancel

Fig. 320: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
	<p>File contains a headline</p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>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.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p>

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

☒ = Function has been activated; all assignments of the PBXs which are listed in the detail view are overwritten and only the new assignment is applied.

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

3. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
4. If errors have been detected, the window *Result* appears.
Click on the button *Display Error Report* to open the window *Error Report*.
To close the window *Error Report*, click on the button *Close*.
To close the window *Result*, click on the button *Close*.
5. The configured extensions now appear in the detail view.

Step: Configure Monitor Points
✕

Extension Monitor Points

Extension ▲	Active ⇅	Intrusion ⇅
6000	✓	<input checked="" type="checkbox"/>
6001	✓	<input checked="" type="checkbox"/>
6002	✓	<input type="checkbox"/>
6003	✓	<input type="checkbox"/>
6004	✓	<input type="checkbox"/>
6005	✓	<input type="checkbox"/>
6006	✓	<input type="checkbox"/>

Add
Active/Inactive
Delete

Save
Cancel

Fig. 321: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Delete To delete extension monitor points, select the respective extension in the list and click on the button *Delete*. To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.

Intrusion To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column *Intrusion*.

☒ = Intrusion feature has been activated.

☐ = Intrusion feature has not been activated.

6. Click on the button *Save* to apply the settings and to finish this configuration step.



An extension which is supposed to be monitored and recorded by means of intrusion must be configured in the PBX to send an engaged signal if it is in a conversation. Only then, can the CTI^{connect} service initiate an intrude call and a silent conference.

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 15](#).

Global recording settings

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.

Step: Global Recording Settings

Details

Transport protocol	TCP	
Port SIP signaling*		5060
Remote SIP port*		7300
Activate SIP authentication	<input checked="" type="checkbox"/>	
User name for the SIP registration	#Extension	
Password for the SIP registration	••••••••	
Activate PBX connection	<input checked="" type="checkbox"/>	
SIP registration expiration*		3600
PBX IP address*	192.168.170.219	
PBX port*		5060

Save
Cancel

Fig. 322: Configuration step - Global Recording Settings

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

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

Parameter	Value/Description
	UDP = unencrypted TLS = encrypted
<i>Port SIP signaling</i>	Enter the port for the SIP signaling. On this port, the recording server can reach the Mitel end devices for the Active Streaming Recording by means of SIP to start the recording. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices, default 7300.
<i>Activate SIP authentication</i>	Activate the check box if the SIP registration is supposed to be authenticated. The option <i>Activate SIP authentication</i> is only used together with or as an expansion of the option <i>Activate PBX connection</i> .
<i>User name of the SIP registration</i>	Enter the user name for the SIP registration for the recording of the extensions used with the intrusion feature. The user name is configured in the PBX and applies for all extensions to be registered.
<i>Password of the SIP registration</i>	Enter the password for the SIP registration for the recording of the extensions used with the intrusion feature. The password is configured in the PBX and applies for all extensions to be registered.
<i>Activate PBX connection</i>	Activate the check box if you would like to use the intrusion feature. When this option has been activated, the configured extensions of the recording server are registered on the PBX. Once the check box has been activated, the following parameters become active to be configured.
<i>SIP registration expiration</i>	Enter the period in seconds until the registration runs out.
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX port</i>	Enter the port for the communication with the PBX, default 5060.


Tab. 69: Global recording settings

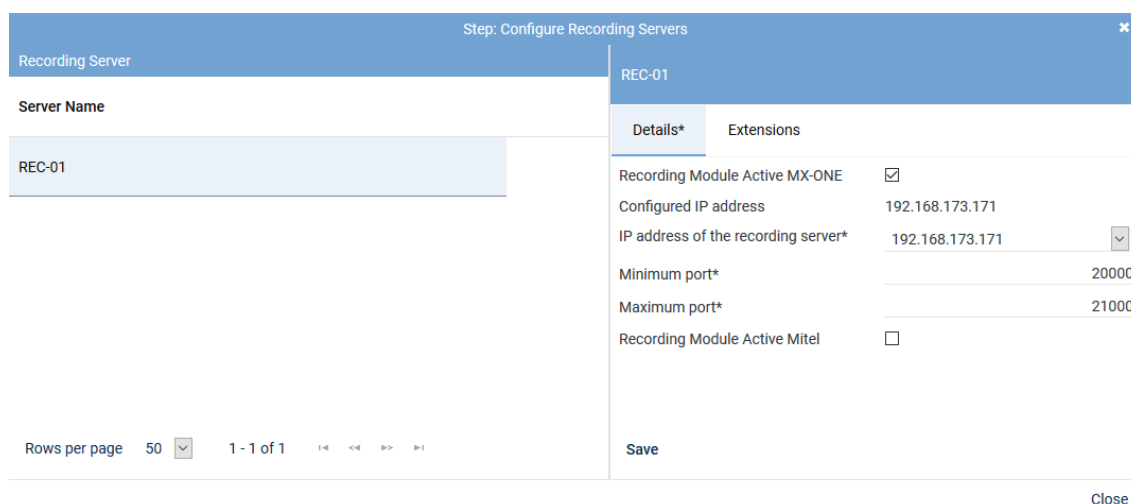
- Click on the button **Save** to apply the settings and to finish this configuration step.



After an update, this section must be configured again.

Configure recording servers

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



Step: Configure Recording Servers

Recording Server

Server Name

REC-01

REC-01

Details* Extensions

Recording Module Active MX-ONE ☒

Configured IP address 192.168.173.171

IP address of the recording server* 192.168.173.171

Minimum port* 20000

Maximum port* 21000

Recording Module Active Mitel ☐

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 323: Configuration step - Configure recording servers

2. Activate the check box *Recording Module Active MX-ONE* so that the configuration parameters appear.
3. Enter the following parameters:

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

Tab. 70: Configure recording servers



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*.

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



After an update, this section must be configured again.

Tab Extensions

If you would like to use the feature *Intrusion* you have to configure an extension for the recording server.

1. Select the tab *Extensions*.

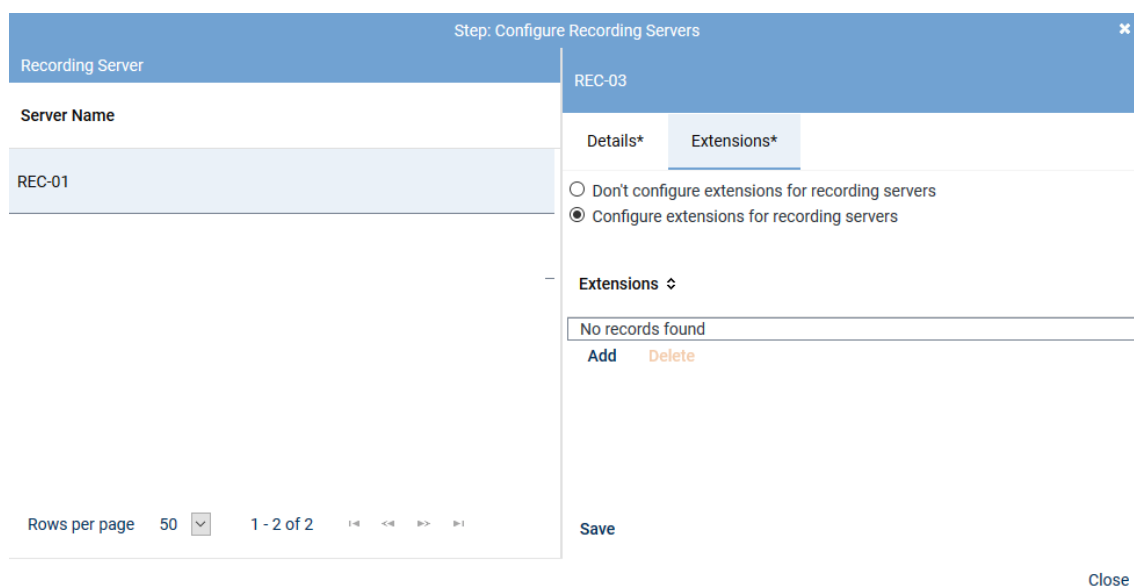


Fig. 324: Tab Extensions

Configure extensions of the recording server Activate this option if you would like to configure extensions for the recording server so make the feature call intrusion work.

If you use more than one recording server, assign separate extensions or extension ranges to the respective recording servers.

Make sure that the extensions for the recording server have not already been allocated to extension monitor points.

NOTICE! The extensions which have to be configured here are SIP extensions which have to be created on the PBX previously so that the recording server can register with these extensions on the PBX. These extensions are used exclusively for the intrusion feature.

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

⇒ The window *Add Extensions* appears.

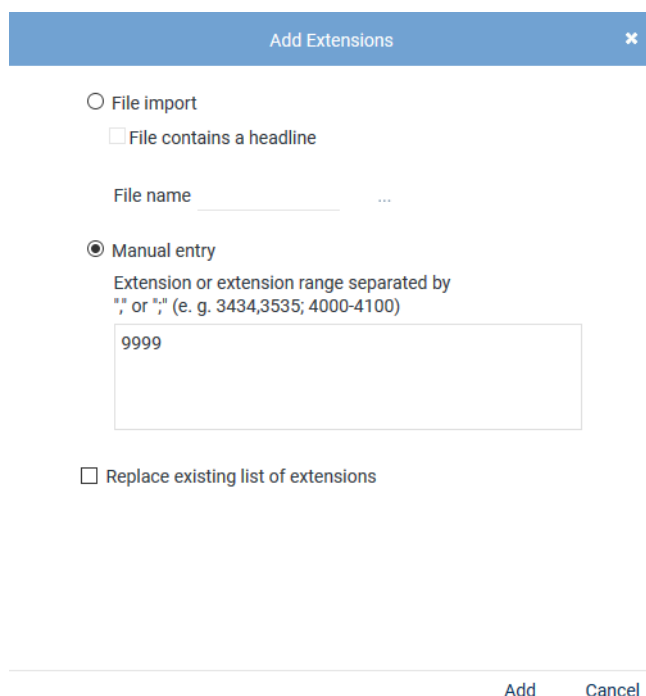


Fig. 325: Add extensions

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.

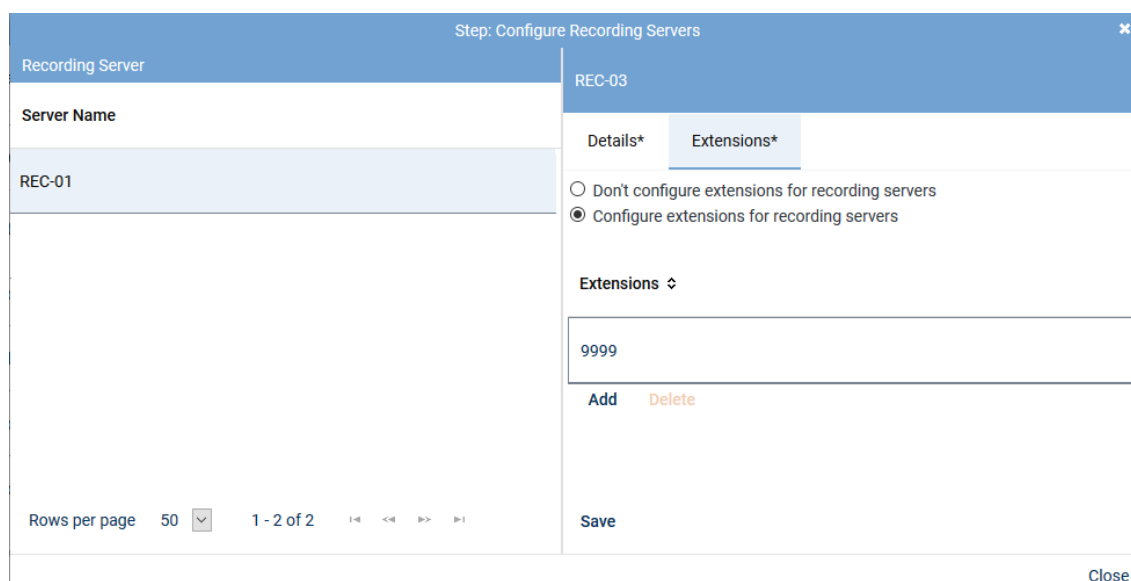


Fig. 326: Added extensions

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

Configure add-on



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

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



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

Configure add-on for MiContact Center Enterprise

The add-on refers to the usage of MiContact Center Enterprise and must only be configured if MiContact Center Enterprise is used.

The integration runs in combination with the PBX and the recording server which is responsible for the actual conversation recording. The conversation events and the additional data are captured via MiContact Center Enterprise and sent to the recording server.

1. Select the add-on *MiContact Center Enterprise* in the detail view.

Step: Configure Add-on

Details *

Select add-on
☐ None
☒ MiContact Center Enterprise

CTIconnect Module

TypeCTIconnect passive
Grammar name*standard
Grammar version*2.00.01

Connection Data

Server name*192.168.170.205
Port*2601

Additional Data

CALLIDUniversal Call ID
PRIVATEDATAPlease select...
SERVICEGROUPIDPlease select...
SERVICEGROUPLISTPlease select...
IVRDATA1Please select...
IVRLABEL1Please select...
IVRDATA2Please select...
IVRLABEL2Please select...
IVRDATA3Please select...
IVRLABEL3Please select...
OASIDPlease select...

Arbitrary assignment

Please select...
Please select...
Please select...

SaveCancel

Fig. 327: Configure add-on for MiContact Center Enterprise

Group field CTIconnect Module

- Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	Select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 71: Configure CTIconnect module

Group field Connection Data

- Set the following parameters in the group field *Connection Data*:

Parameter	Value/Description
Server Name	Enter the IP address or the name of the server that the MiContact Center Enterprise runs on.
Port	Enter the port for the connection to MiContact Center Enterprise.

Tab. 72: Configure connection data

Group field Additional Data

The following additional data is delivered in the protocol when using MiContact Center Enterprise:

- *CALLID*
- *PRIVATEDATA*
- *SERVICEGROUPLIST*
- *IVRDATA1*
- *IVRLABEL1*
- *IVRDATA2*
- *IVRLABEL2*
- *IVRDATA3*
- *IVRLABEL3*
- *OASID*

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.



The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.



The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ► to expand the group field and to assign the additional data to the data fields of the search and replay applications.

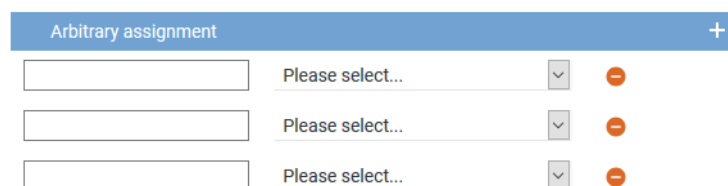



Fig. 328: Arbitrary assignment of the additional data

The following additional data are always available:

- *Start time*
- *End time*

- *Duration*
 - *Calling Party Phone Number*
 - *Called Party Phone Number*
 - *Conversation Direction*
2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
 3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
 4. To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.
 - ⇒ An additional row appears to assign another additional data type.
 5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.



To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.



For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure add-on for Genesys T-Server (optional)

The add-on refers to the usage of Genesys T-Servers and must only be configured if you use Genesys T-Servers.

The integration runs in combination with the PBX and the recording server. The CTI^{connect} service receives the information which Genesys T-Server the monitor points have been assigned to from the Genesys Configuration Server. The monitor points must register on the respective Genesys T-Server. Upon successful registration, the respective Genesys T-Server sends all conversation events and additional data of the agents to the recording server.

CTIconnect for Genesys T-Server

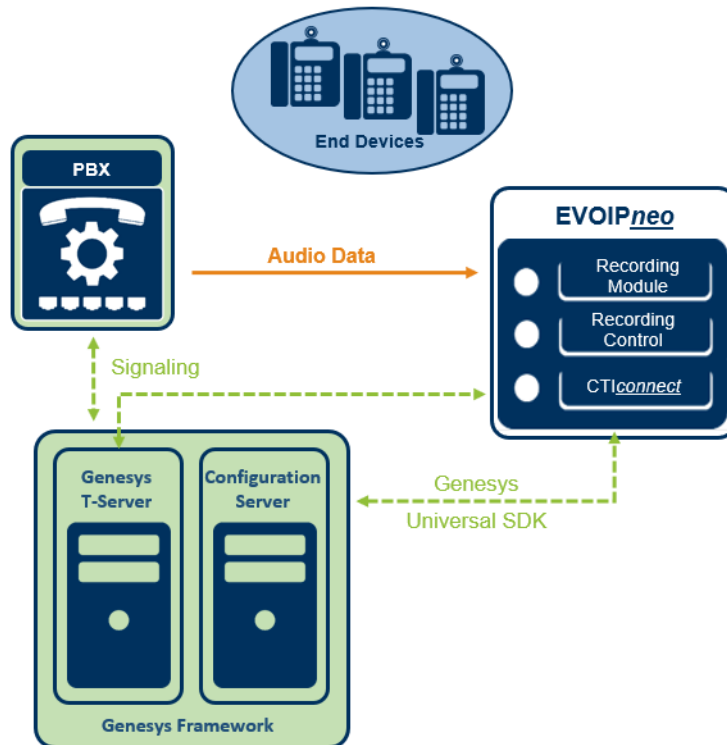


Fig. 329: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 311](#).

The Genesys add-on uses either a unique call ID or the extension to unambiguously identify the conversations to be recorded.



The additional data delivered by an add-on supplements the additional data which is delivered by the CTIconnect module of the integration.

When using a CTIconnect for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.


By default, the Genesys data field *CallID* has been selected as identifier. If a different data field is supposed to be used for internal control, this can be changed in the configuration file *basic.pif.properties*.

Adjust configuration file for Genesys add-on

The data field which is supposed to be used by the Genesys add-on is selected by means of the parameter *pifgenesys.call_identifier*.

1. To adjust the identifier, change to the path
C:\ASC Product Suite\data\CTIConnectForGenesysT\.
2. Open the file *basic.pif.properties*.
3. Enter the respective data field for the parameter *pifgenesys.call_identifier*.
4. Save the changes in the file.
5. Restart the recording architecture after completing the change.

Configure add-on in the integration

1. To configure the add-on, click on the button  (*Edit configuration step*) in the main view in the line *Configure add-on*.
2. In the detail view, select the add-on *Genesys T-Server*.

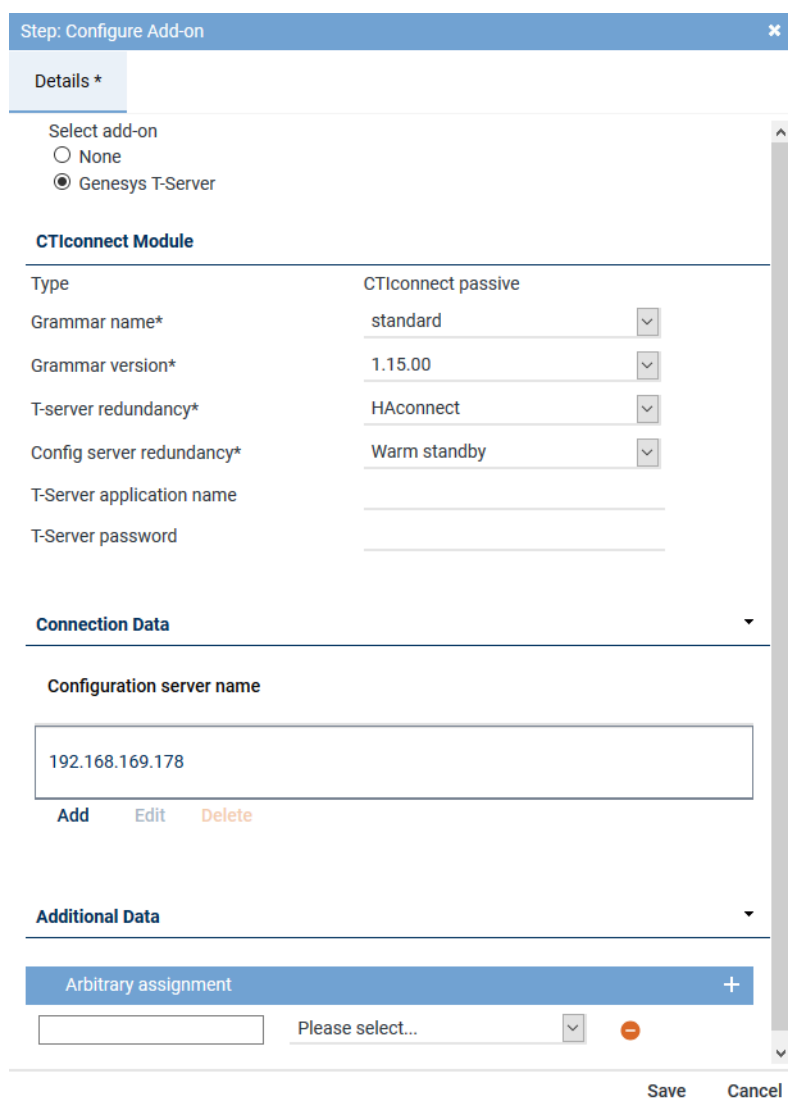


Fig. 330: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

Parameter	Value/Description
<i>Type</i>	Here, the type of the CTI <u>connect</u> module is displayed.
<i>Grammar name</i>	Select the respective grammar.
<i>Grammar version</i>	Select the respective grammar version.
<i>T-server redundancy</i>	Select the redundancy which is used from the drop-down list. <ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.

Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>No redundancy</i> • <i>HAconnect</i> - for High Availability Connection • <i>Warm Standby</i> - for a connectable redundancy
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 73: Configure add-on for Genesys T-Server

Group field Connection Data

In this group field, you can enter one or several sets of connection data.

- In the group field *Connection Data* in the table, click on the button *Add*.
⇒ The following window appears:

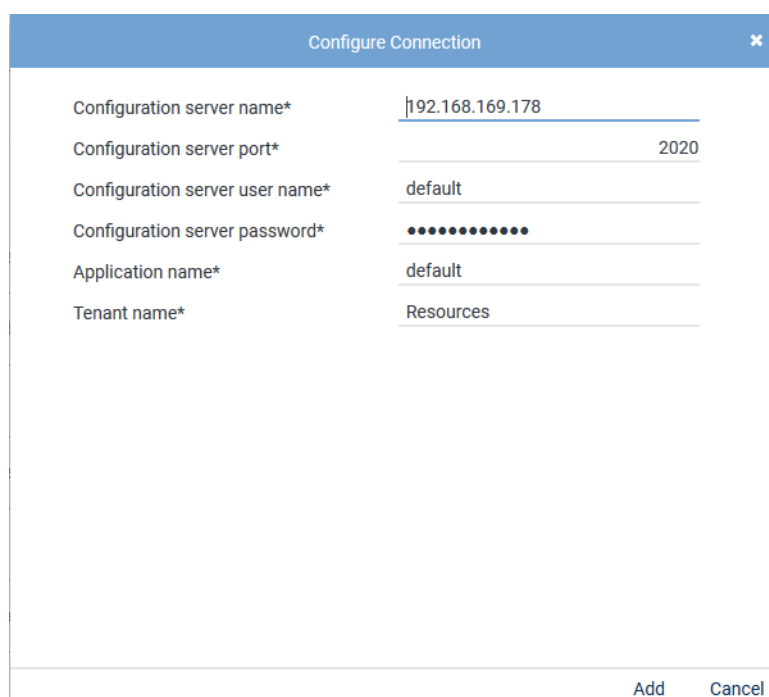


Fig. 331: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<i>Configuration Server: Name</i>	Enter the IP address or the name of the computer that the Genesys Configuration Server runs on.
<i>Configuration Server: Port</i>	Enter the port of the Genesys Configuration Server.

Parameter	Value/Description
<i>Configuration Server: User name</i>	Enter the user name to log in to the Genesys Configuration Server.
<i>Configuration Server: Password</i>	Enter the password to log in to the Genesys Configuration Server.
<i>Application name</i>	Enter the application name that the recording servers uses to log in to the Genesys Configuration Server. Default is <i>default</i> .
<i>Tenant name</i>	Enter the name of the Genesys tenant(s) that are supposed to request the configuration data. Default is <i>Resources</i> . Several tenants can be added separated by commas.

Tab. 74: Configure connection data

Group field Additional Data

The following additional data is delivered by default in the protocol when using Genesys T-Server:

- *CallID*
- *ANI*
- *CallUuid*
- *DNIS*



Further additional data depend on the configuration of the Genesys T-Servers. Check the list *AttributeUserData* in the trace files to find out which further additional data have been delivered by the Genesys T-Servers. Put the addition *UserData* in front of the additional data type when configuring customer-specific additional data, e. g. for *RTargetAgentGroup* you have to configure *UserDataRTargetAgentGroup*.

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure the additional data which is additionally delivered by the PBX or by an add-on but which is not listed yet. Upon assigning the delivered additional data, it appears in the search and replay applications.



The names of the column headlines which are supposed to appear in the players must be configured and made available in the Additional Data module first.

For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.



The drop-down list only contains those additional data that you have configured and made available in the Additional Data module. The display name then appears in the column headlines in the players.

For more information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

1. In the group field headline *Additional Data*, click on the arrow ► to expand the group field and to assign the additional data to the data fields of the search and replay applications.

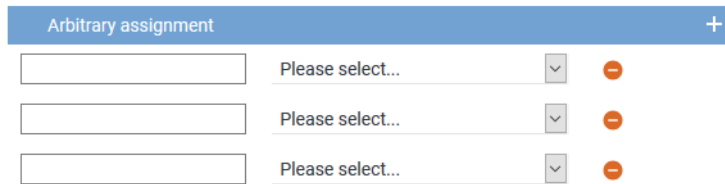



Fig. 332: Arbitrary assignment of the additional data

The following additional data are always available:

- *Start time*
 - *End time*
 - *Duration*
 - *Calling Party Phone Number*
 - *Called Party Phone Number*
 - *Conversation Direction*
2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
 3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
 4. To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.
 - ⇒ An additional row appears to assign another additional data type.
 5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.




To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.



For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

Configure miscellaneous settings

1. Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
 - ⇒ The window *Step: Miscellaneous Settings* appears.

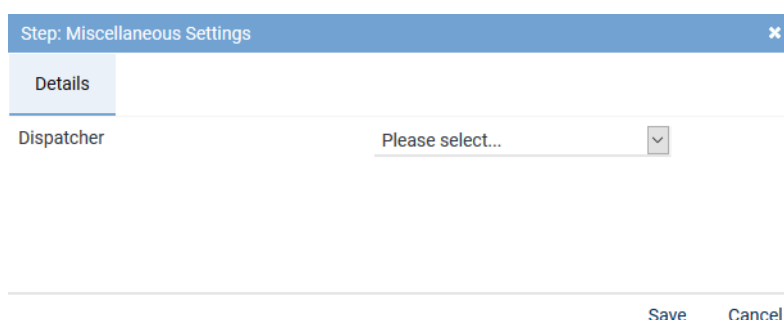


Fig. 333: Configure miscellaneous settings

- Enter the following parameter:


Parameters	Description
<i>Dispatcher</i>	From the drop-down list, select the previously created additional data field that the participant information is supposed to be connected with.





Only those entries appear in the drop-down list which have been configured in the application System Configuration in the Additional Data module. For further information refer to the administration manual *Additional Data module*.

Activate integration

The integration can only be activated after the configuration is complete.

If not all configuration steps have been carried out completely, the icon  (*Incomplete*) will appear in the main view, in the line of the created integration, in the column *Status*.

If the configuration has been carried out completely, the icon  (*Complete*) will appear in the line of the respective step, in the column *Configuration*.

If all settings are complete, the icon  (*OK*) will appear in the main view, in the line of the created integration, in the column *Status*.





















	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		
Step		Configuration		
Configure recording architecture				
Configure CTI connection data				
Configure monitor points				
Global recording settings				
Configure recording servers				
Configure add-on				
Configure miscellaneous settings				

Fig. 334: Activate integration

- Mark the integration in the main view, so that the icon  (*Activate*) becomes active in the toolbar.
- To activate the integration, click on the icon  (*Activate*).
⇒ In the column *Active*, the icon  (*Active*) appears.








    Integration ▾ General			
Name ▾	Type ▾	Active ▾	Status ▾
	Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	 

Fig. 335: 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.



For updates, the integration is stopped and deactivated. Once the update has been completed successfully, you must configure the integration again. Once the configuration has been completed, start the recording architecture again and activate the integration so that the new configuration is applied.

Deactivate/Delete integration

To be able to delete an integration, it has to be deactivated.

- To deactivate the integration, click on the icon  (*Deactivate*) in the toolbar.
 - ⇒ In the column *Active*, the icon  (*Inactive*) appears.
 - ⇒ The icon  (*Delete*) becomes active in the toolbar.







+ ×   Integration ▾ General			
Name ↕	Type ↕	Active ↕	Status ↕
 Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA		

Fig. 336: Deactivate integration

- Click on the icon  (*Delete*) and confirm the security prompt to delete the integration.

7.3.2.5 Synchronization options

There are 2 different types of synchronization:

- Synchronization of the Recording Control service for recording control
- Synchronization of the system storage to compare recording data

7.3.2.5.1 Synchronizing recording control

Recording Control services

In parallel recording servers which have been installed and configured in the same system architecture, you can configure the synchronization of recording control.



DANGER!

Before the configuration, contact your ASC support to ensure that this function is suitable for your recording solution and to avoid a possible loss of recordings!

For information about which recording solutions support this function refer to the file [neo](#) Integration Overview.

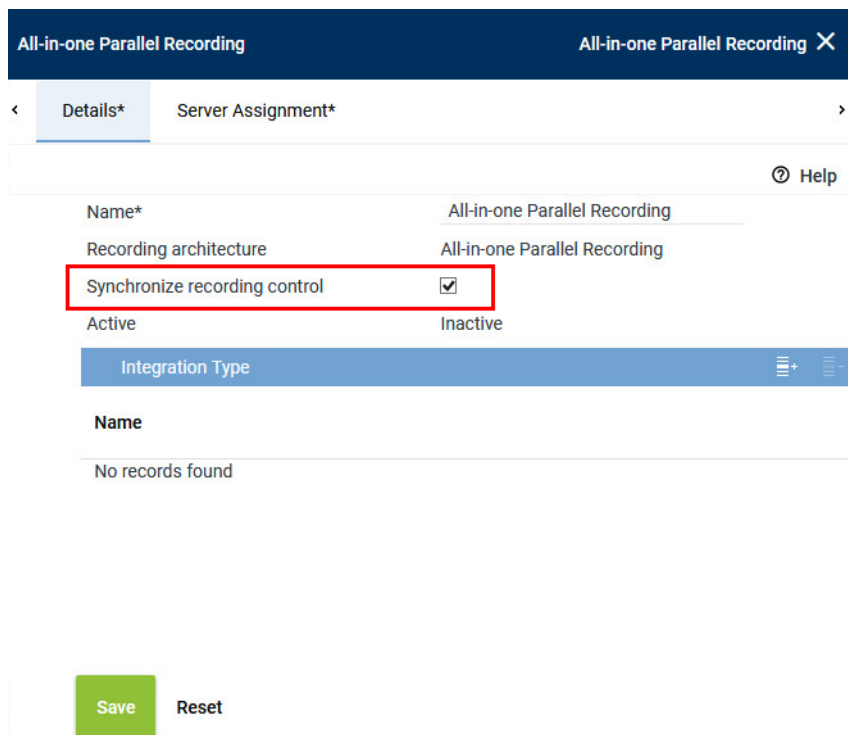
If recording control is supposed to take place by means of external applications such as *CLIENTcommand*, *PHONEapp*, or *SCREENrec* scan Editor, a synchronization of the Recording Control services of the parallel recording servers must be set up.

Primarily, recording control is carried out by the 1st Recording Control service. The Recording Control service guarantees that the conversations are recorded by both recording servers.

If the 1st Recording Control service fails, the 2nd Recording Control service takes over the task of recording control for both recording servers, both of which will record the conversations then.

Synchronization of recording control is configured in the Recording Architectures module. In parallel recording architectures, the check box *Synchronize recording control* appears in the tab *Details*.

1. Activate the check box *Synchronize recording control* so that the Recording Control services can be synchronized and only one service controls recording for the two recording servers.



The screenshot shows a configuration window titled 'All-in-one Parallel Recording'. It has two tabs: 'Details*' and 'Server Assignment*'. The 'Details*' tab is active. Inside, there's a form with fields for 'Name*' (All-in-one Parallel Recording), 'Recording architecture' (All-in-one Parallel Recording), 'Synchronize recording control' (checked), and 'Active' (Inactive). A red rectangle highlights the 'Synchronize recording control' checkbox. Below the form is a section for 'Integration Type' with a table that is currently empty, showing 'No records found'. At the bottom left are 'Save' and 'Reset' buttons.

Fig. 337: Synchronize recording control

2. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

If you subsequently activate or deactivate this synchronization options, you have to carry out the following configuration steps again before the changes take effect:

1. Set the requested state of the recording control:
 - ☒ = *recording control is synchronized*
 - ☐ = *recording control is not synchronized*
2. Deactivate the integration.
3. Deactivate the recording architecture.
4. Check that the following services have been stopped.
 - *ASC RecordingControl*
 - *ASC RecordingModule*
 - *ASC CTIconnect(integration name)*

5. Activate the recording architecture.

WARNING! In this status, all services have received the updated configuration, but may be in a conflict status.

Therefore, you have to carry out the following steps again:

6. Deactivate the recording architecture again.
 7. Check that the following services have been stopped.
 8. Activate the recording architecture again.
 9. Activate the integration.
- ⇒ Now, the changes have been applied.

7.3.2.5.2 Synchronization of system storage

In recording architectures with 2 system storages, you can configure a synchronization for comparing the recordings.

A synchronization configuration is always created for 2 system storages. All recordings which are added to one system storage are copied to the other system storage, too, and vice versa. That way, all recordings of both system storages are available on the 2 system storages simultaneously. If one of the two system storages fails, you can thus access the recordings of the failed system storage via the other system storage.

Synchronization of system storage is configured in the Servers module.

1. To create a synchronization configuration, click on the menu item *Servers > Manage synchronization configuration* in the toolbar of the main view.



Fig. 338: Menu item Manage synchronization configuration

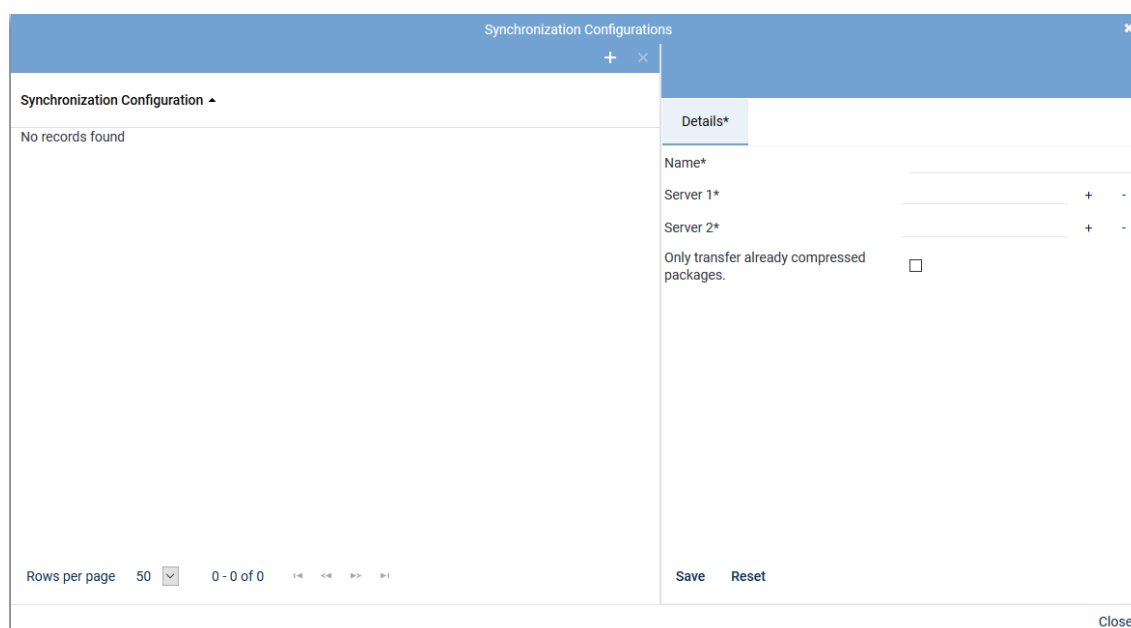



Fig. 339: Configure synchronization configurations

The following options are available:

+	Create	Creates a new synchronization configuration (see chapter "Create synchronization configuration", p. 283).
---	---------------	--


 **Delete** Deletes the selected synchronization configuration (see [chapter "Delete synchronization configuration", p. 284](#)).

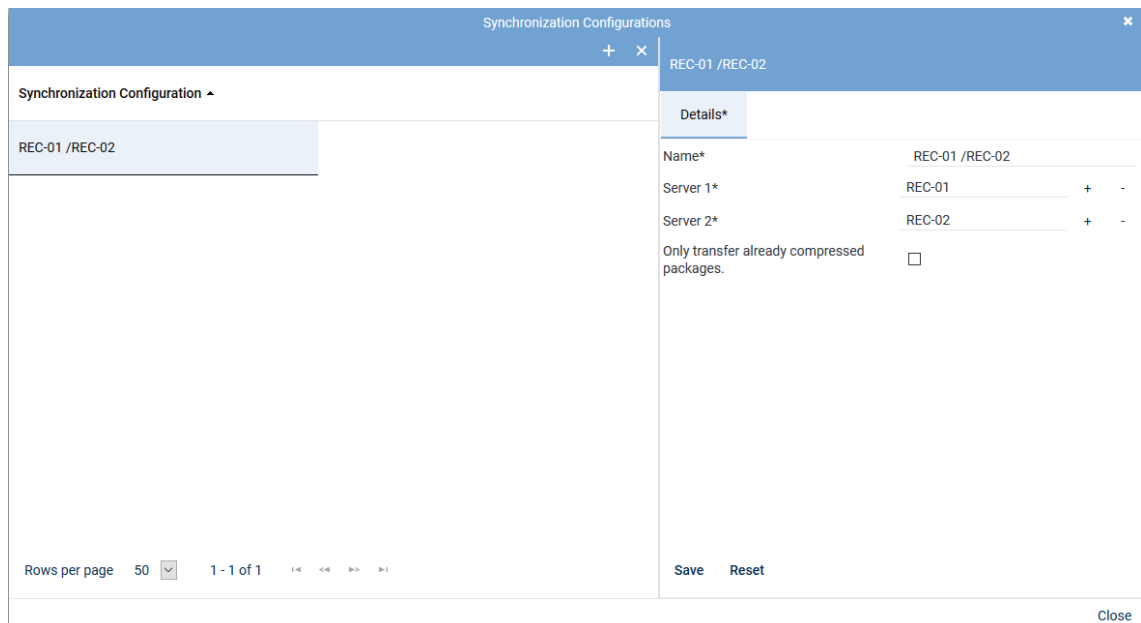
A synchronization configuration becomes active upon saving it and continues running until it is deleted. During this period both system storages are regularly checked for new content and synchronized.



A server which is already used in a synchronization configuration cannot be used in another synchronization configuration.

Create synchronization configuration



- In the window *Administrate Synchronization Configuration*, click on the icon  (*Create*).
⇒ The tab *Details* becomes active.



The screenshot shows a window titled "Synchronization Configurations" with a close button (X) in the top right. Below the title bar is a toolbar with a plus (+) and minus (-) icon. The main area is divided into two panes. The left pane, titled "Synchronization Configuration", shows a list with one entry: "REC-01 / REC-02". The right pane, titled "Details*", shows the configuration details for "REC-01 / REC-02". It includes fields for "Name*" (set to "REC-01 / REC-02"), "Server 1*" (set to "REC-01" with a plus and minus button), and "Server 2*" (set to "REC-02" with a plus and minus button). There is a checkbox for "Only transfer already compressed packages." which is currently unchecked. At the bottom of the right pane are "Save" and "Reset" buttons. At the bottom of the left pane are "Rows per page" (set to 50), "1 - 1 of 1", and navigation icons. A "Close" button is located at the bottom right of the window.


Fig. 340: Create synchronization configuration

- Complete all fields for the new synchronization configuration:

Name	Enter a name for the synchronization configuration.
Server 1 / Server 2	Click on the button  next to the entry field to select the respective server for the synchronization of the system storage from the list of available servers. If you would like to delete an entry in one of the entry fields, click on the button  next to the respective entry field.
Only transfer already compressed packages	Select whether data which has not yet been compressed is supposed to be transferred, too. <input checked="" type="checkbox"/> = Uncompressed data is transferred, too. <input type="checkbox"/> = Only compressed data is transferred. NOTICE! This option is not available until you have entered and saved the two servers.

- Click on the button *Save* to apply the configuration.
- Click on the button *Close* to finish this configuration step and close the window.

Delete synchronization configuration

1. In the window *Administrate synchronization configurations*, select the synchronization configuration you would like to delete.
 2. Click on the icon  (*Delete*) in the toolbar of the window.
- ⇒ The synchronization of the two entered system storages is finished.
- ⇒ The selected synchronization configuration is deleted.

7.3.2.6 Standby management for failover architectures

For architectures with failover concepts, you can go to the standby management to manually select which server with which components is supposed to be active.

For architectures of the type *Parallel Recording*, you can also use the standby management if you have provided for the respective resources.

Using the standby management makes sense in the following cases:

- You would like to switch back to the primary server, e. g. when the standby server has automatically taken over and the primary server is now available again.
- You would like to switch to the standby server manually, e. g. during maintenance of the primary server.



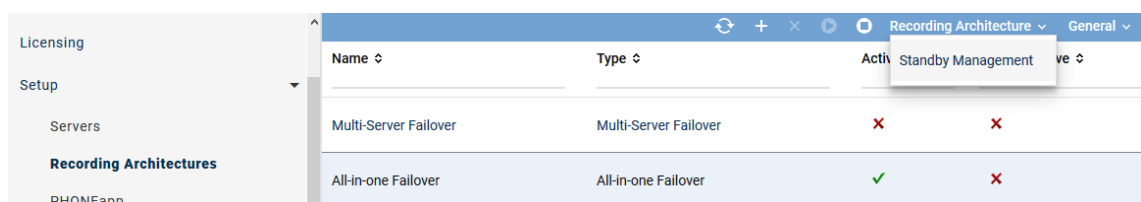
You can only edit the standby management if the corresponding architecture has been activated.

7.3.2.6.1 Standby management for All-in-one Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
 - ⇒ If the selected recording architecture has been activated, the menu item *Standby Management* is active.



Name	Type	Active	Standby Management
Multi-Server Failover	Multi-Server Failover	✗	✗
All-in-one Failover	All-in-one Failover	✓	✗

Fig. 341: Configure standby management


3. Click on the menu item *Standby Management*.
 - ⇒ The window *Standby Management* appears.

Standby Management				
Server Name	Status	Oldest Running Activity	Running Activities	Version
RC - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.01.00
REC-02	In Standby		Activities: 0	
RIA - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.01.00
REC-02	In Standby		Activities: 0	
RM - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.00.00
REC-02	In Standby		Activities: 0	

Fig. 342: Switch server

Here, you see the assignment of the deployed components.

In the column *Status*, you can see which component is currently active.



- To activate a standby server, select the respective server in the list.
 - Click on the icon  (*Activate*) in the toolbar.
- ⇒ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server



This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

- To activate shutdown mode for a server, select the respective server in the list.
 - Click on the icon  (*Activate shutdown mode*) in the toolbar.
- ⇒ The status of the server changes from *Active* to *Shutdown Mode*.
- To deactivate shutdown mode again, click on the icon  in the toolbar again.
- ⇒ The status of the server changes from *Shutdown Mode* to *Active*.




In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

- To activate a standby server, select the respective server in the list.

2. Click on the icon  (*Activate*) in the toolbar.
- ⇒ The status of the standby server changes from *In Standby* to *Active*.
Only now can this server record new conversations.

7.3.2.6.2 Standby management for Multi-Server Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
 - ⇒ If the selected recording architecture has been activated, the menu item *Standby Management* is active.

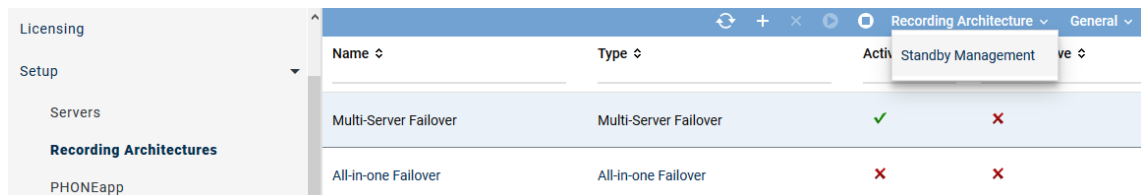


Fig. 343: Menu of the standby management

3. Click on the menu item *Standby Management*.
 - ⇒ The window *Standby Management* appears.

Standby Management				
Server Name	Status	Oldest Running Activity	Running Activities	Version
RC - RC-01 / RC-02				
RC-01	Active		Activities: 0	60.01.00
RC-02	In Standby		Activities: 0	60.00.00
RM - REC-01 / REC-02				
REC-01	Active		Activities: 0	60.00.00
REC-02	In Standby		Activities: 0	
RIA - CTI-01 / CTI-02				
CTI-01	Active		Activities: 0	60.01.00
CTI-02	In Standby		Activities: 0	60.00.00

Fig. 344: Switch server

If you have installed the required redundancy options on different servers, you can use standby management for the following components:

- **RC** (*Recording Control Standby Management*) to secure recording control

- **RM** (*Recorder Standby Management*) to secure recording
- **RIA** (*CTIconnect Standby Management*) to secure the additional data of the recordings

Here, you see the assignment of the deployed components.

In the column *Status*, you can see which component is currently active.

4. To activate a standby server, select the respective server in the list.

5. Click on the icon  (*Activate*) in the toolbar.

⇒ The status of the standby server changes from *In Standby* to *Active*.

Activate shutdown mode for maintenance purposes

If you would like to shut down a server for maintenance purposes, you can activate shutdown mode for this server




This function is not useful for architectures for All-in-one Failover as no additional server can be activated in shutdown mode in this architecture.

1. To activate shutdown mode for a server, select the respective server in the list.

2. Click on the icon  (*Activate shutdown mode*) in the toolbar.

⇒ The status of the server changes from *Active* to *Shutdown Mode*.

3. To deactivate shutdown mode again, click on the icon  in the toolbar again.

⇒ The status of the server changes from *Shutdown Mode* to *Active*.



In shutdown mode, the standby components are not activated automatically. Only those conversations which are already running are continued to be recorded. Once you make manual configurations in the standby management, you must make sure that one of the respective components relevant for recording has been activated. New recordings will not be accepted before another server has been activated manually.

Activate failover components

For another standby server to take over the recording of new conversations, you must activate it manually.

1. To activate a standby server, select the respective server in the list.

2. Click on the icon  (*Activate*) in the toolbar.

⇒ The status of the standby server changes from *In Standby* to *Active*.

Only now can this server record new conversations.

7.3.3 Software update

Due to extensive changes, the configuration of the integration cannot be inherited in updates to version neo 5.2 or higher.

1. Once the update has been completed successfully, you must configure the following settings in the integration again:

- **CTI connection data**
 - Select latest grammar
 - Configure PBX connection data and activate Transport Layer Security
 - Configure failover conditions
- **Global recording settings**
 - Select transport protocol
 - Activate SIP authentication
 - Activate PBX connection

- **Configure recording servers**
 - Activate recording module Active MX-ONE
- 2. Once the integration has been completely configured, change to the Recording Architectures module and restart the recording architecture.
- 3. If the recording architecture is active, change to the Integrations module and activate the integration.

7.3.4 Configure XML PHONEapp

If you would like to use the XML PHONEapp, you have to execute the following configuration:

1. Configure key assignment for the phones.
2. Modules in the application *Configure System Configuration*:
 - Servers module
 - Activate recording control
 - Select recording architecture
 - PHONEapp module
 - Configure phone types
 - Configure basic settings
 - PBX module
 - Activate PHONEapp configuration
 - Configure PBX-specific parameters
 - Phones module
 - Configure the parameters for the assignment of the phone, e. g. extension, PBX phone ID, computer name, address for replay via phone, phone type, and time slot.
 - Recording Planner module
 - Configure operation modes

7.3.4.1 Configure key control

To be able to control the XML PHONEapp via the phone's keys, you have to assign the individual keys the respective commands on the phones. The configuration has to be done in the configuration file of the end devices. The key options must be activated in the PBX. The configuration is usually done by the telecommunication technician.

The assignment of the end devices can be done via the following parameters:

Parameter	Description
deviceIPAddress	IP address of the end device
deviceExtension	Extension of the end device

Tab. 75: Available parameters

Observe the following syntax:

Configuration example for the assignment via the extension:

1. Configure start function
`http://172.16.101.94/PHONEapp/XMLInterface?event=START&deviceExtension=$SIPUSERNAME$$`
2. Configure stop function
`http://172.16.101.94/PHONEapp/XMLInterface?event=STOP&deviceExtension=$SIPUSERNAME$$`

3. Configure mute function
http://172.16.101.94/PHONEapp/XMLInterface?event=MUTE&deviceExtension=\$\$SIPUSERNAME\$\$
4. Configure unmute function
http://172.16.101.94/PHONEapp/XMLInterface?event=UNMUTE&deviceExtension=\$\$SIPUSERNAME\$\$
5. Configure keep function
http://172.16.101.94/PHONEapp/XMLInterface?event=KEEP&deviceExtension=\$\$SIPUSERNAME\$\$
6. Configure delete function
http://172.16.101.94/PHONEapp/XMLInterface?event=DELETE&deviceExtension=\$\$SIPUSERNAME\$\$
7. Configure the display of the current recording status
http://172.16.101.94/PHONEapp/XMLInterface?event=GETSTATE&deviceExtension=\$\$SIPUSERNAME\$\$
8. Configure the display of tagging attributes
http://172.16.101.94/PHONEapp/XMLInterface?event=SET_TAGGING&deviceExtension=\$\$SIPUSERNAME\$\$

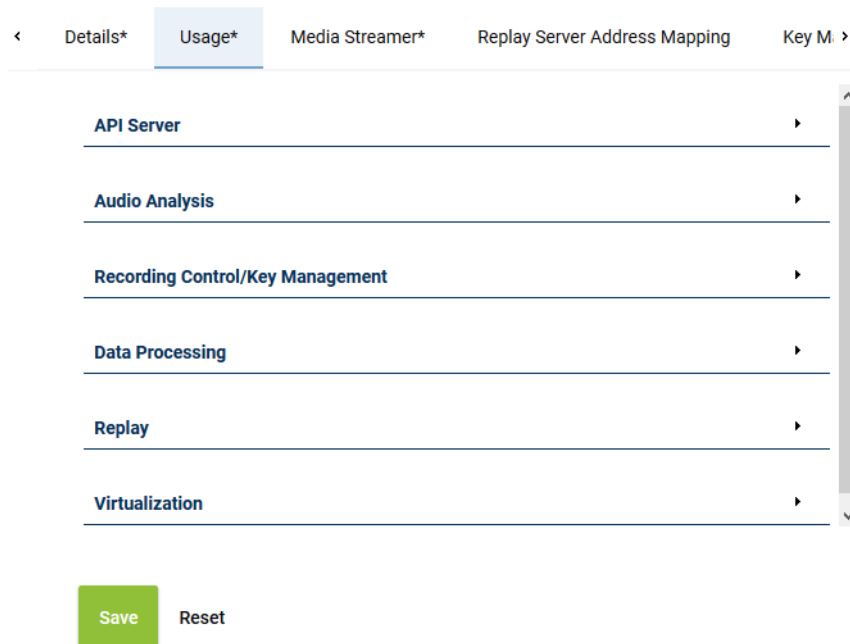


The addition \$\$SIPUSERNAME\$\$ makes sure that the extension of the respectively logged-in users is used.

7.3.4.2 Configure Servers module

To be able to control the recording by means of PHONEapp, you have to activate recording control in the Servers module.

1. Select the menu item *Setup* > *Servers* in the navigation bar.
2. Select the tab *Usage*.



The screenshot shows the 'Usage' tab selected in the 'Servers' module. The tab bar at the top includes 'Details*', 'Usage*' (active), 'Media Streamer*', 'Replay Server Address Mapping', and 'Key M. >'. Below the tab bar, a list of server components is displayed with expandable arrows on the right:

- API Server
- Audio Analysis
- Recording Control/Key Management
- Data Processing
- Replay
- Virtualization

At the bottom of the interface, there are two buttons: a green 'Save' button and a grey 'Reset' button.

Fig. 345: Servers - tab Usage

3. Open the group field *Recording Control/Key Management*.

7.3.4.2.1 Group field Recording Control/Key Management

Recording Control/Key Management ▼

☒ Recording control/Monitoring

Recording architecture ▼

☒ neo key management

Fig. 346: Group field Recording Control/Key Management

Parameters	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <i>CLIENT</i> <u>command</u> or an API recording control or if you would like to use <i>Monitoring</i>. This feature is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> Recording architecture From the drop-down list, select the respective recording architecture you would like to use for the control.
- <i>neo key management</i>	<p>The function allows customer-specific encryption of the recordings. To be able to configure the key management, you have to activate the check box <i>Key management</i>.</p> <p>This function can only be activated if the license <i>ASC_KEY_MANAGEMENT</i> is available.</p> <p>For further information about the configuration of the key management refer to the administration manual <i>Configuration of servers and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 76: Configure Recording Control/Key Management

7.3.4.3 Configure PHONEapp

- In the navigation bar, select the menu item *Setup > PHONEapp*.
⇒ The following window appears:

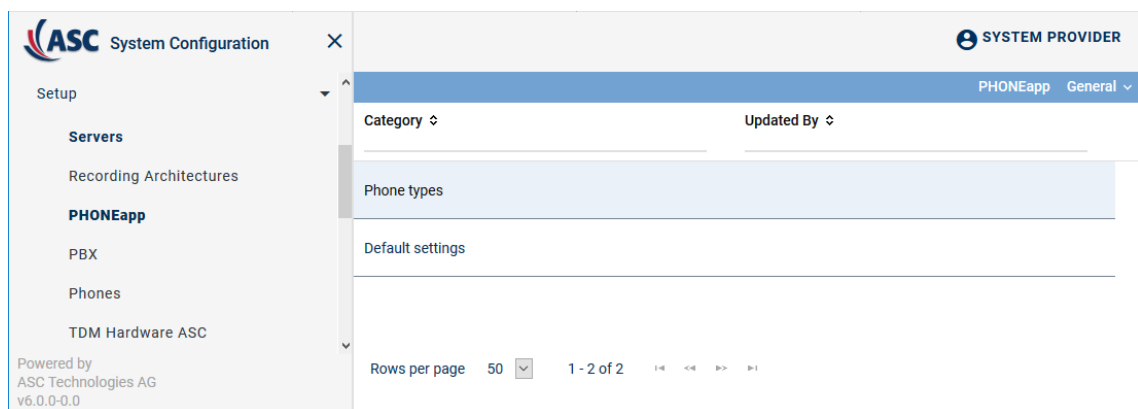


Fig. 347: PHONEapp - main view:

In this module, you can adjust the basic settings for the phone applications and configure phone types.

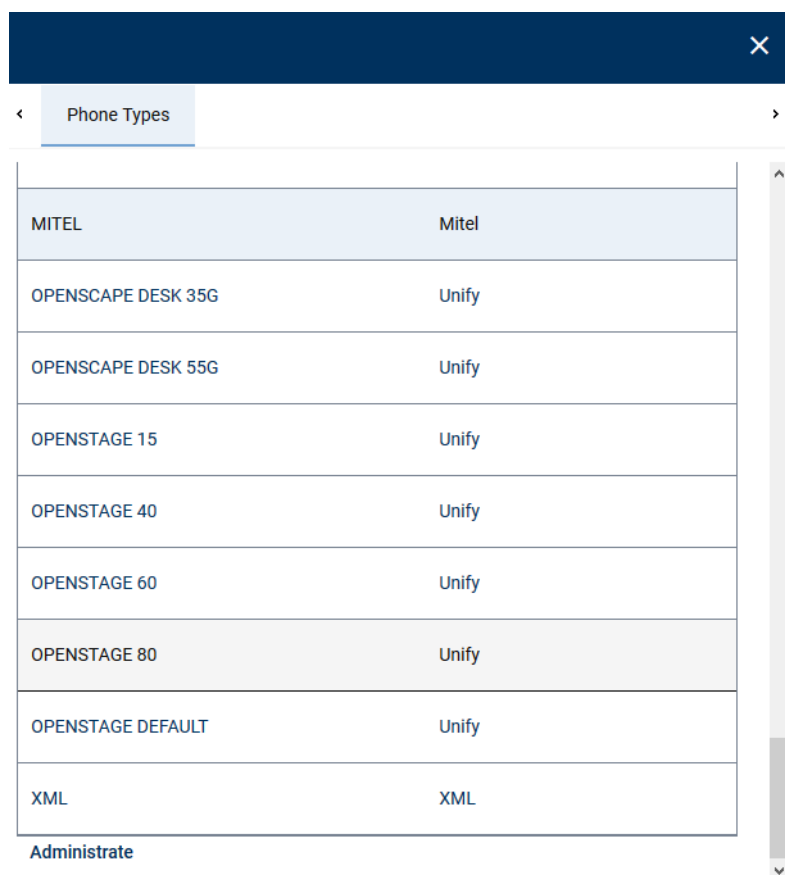
In the category *Phone types*, you can display the properties of the supported end devices and add additional phone types.

To configure the function keys you have to create a new phone type in the category *Phone types*.

7.3.4.3.1 Category Phone Type

The category *Phone Types* displays the properties of the supported end devices.

1. In the main view of *Setup > PHONEapp*, select the category *Phone Types*.
 ⇒ In the detail view, a table is displayed which contains all supported end devices.

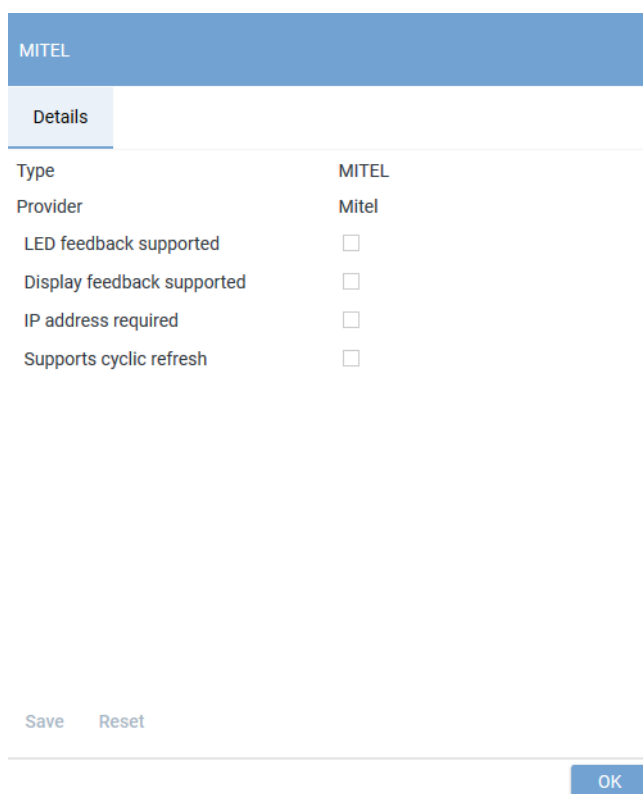


MITEL	Mitel
OPENScape DESK 35G	Unify
OPENScape DESK 55G	Unify
OPENSTAGE 15	Unify
OPENSTAGE 40	Unify
OPENSTAGE 60	Unify
OPENSTAGE 80	Unify
OPENSTAGE DEFAULT	Unify
XML	XML

Administrate

Fig. 348: Detail view phone types

2. To display the properties of the phone type, select the type *Mitel* and click on the button *Administrate*.
 ⇒ In the window *Phone Type*, the properties of the selected end device are displayed.



The screenshot shows a configuration window titled "MITEL". It has a "Details" tab selected. The window displays the following information:

Type	MITEL
Provider	Mitel
LED feedback supported	<input type="checkbox"/>
Display feedback supported	<input type="checkbox"/>
IP address required	<input type="checkbox"/>
Supports cyclic refresh	<input type="checkbox"/>

At the bottom left, there are "Save" and "Reset" buttons. At the bottom right, there is an "OK" button.

Fig. 349: Display of the properties

NOTICE! The properties cannot be configured here but are displayed to inform you which functions are supported by the end device.

- Click on the button *Close* to close the window and to change to the detail view.

7.3.4.3.2 Category Default Settings

Define the values of the general settings for your PBX here. The default settings are divided into different group fields.

- In the main view of *Setup > PHONEapp*, select the category *Default Settings*.
 - ⇒ Different group fields are displayed in the detail view.

<
Default Settings*

General


Activated ☒
PHONEapp URL*
Only certified requests ☐

Language

Time Parameter



Response waiting time* Milliseconds
Error waiting time* Milliseconds
Phone refresh interval* Milliseconds

Tagging Attributes

Request Parameter	Field
tag_field	ASC_COMMENT 

Add
Delete


Register Fields

Field	Recording Control Field	Active
Comment	ASC_COMMENT	 

Add
Delete

Predefined Tagging Fields

☐ Activated



Tagging Field

Save
Reset

Fig. 350: Detail view Default settings

- Adjust the respective settings.
- Click on the button **Save**.

General	Here, you have to enter the address of the PHONEapp and activate it.
<ul style="list-style-type: none"> <i>Activated</i> 	Activates the recording control by means of the PHONEapp.
<ul style="list-style-type: none"> <i>PHONEapp URL</i> 	Enter the URL under which the PHONEapp is supposed to be accessible. Enter the IP address of the application server instead of <host>.

	<p>Enter the additional port, if it differs from default (port 80 for <i>http</i> or port 443 for <i>https</i>), e. g. <i>http://<core_ip>:90</i>.</p> <p>The end device will establish a connection with this URL. The PHONEapp transfers the data provided by the URL to the display of the end device.</p> <p>When using a load balancer, enter the IP address and the port of the load balancer here.</p>
<ul style="list-style-type: none"> • <i>Only certified requests</i> 	<p>If the check box has been activated, certificate-based authentication of the client (end device) on the server is required. To be able to do so, the client certificate must be imported in the certificate key store of the server.</p>
<i>Language</i>	<p>Select the respective default language for the PHONEapp from the drop-down list. The selected language applies to all end devices, unless the display language in the module <i>Setup > Phones</i> is not configured otherwise.</p>
<i>Time Parameter</i>	<p>Define the time parameters in milliseconds here. Do not make any changes without a prior consultation of your local ASC support or the ASC support under +49 700 27278776.</p>
<ul style="list-style-type: none"> • <i>Response waiting time</i> 	<p>Define the period of time during which the PHONEapp is supposed to send a response to the phone. The response waiting time covers the period from the moment of receiving the phone's request via the internal processing of the request to the moment of returning the results to the end device. If the request could not be processed during this period of time, the end device will display a message that the processing is still in progress.</p>
<ul style="list-style-type: none"> • <i>Error waiting time</i> 	<p>Define the maximum period of time available for processing a request. The error waiting time covers the maximum period of time from the moment when the PHONEapp has sent the request to the completion of the internal processing of the request. If the signal of pressing a key could not be processed during the indicated period of time, the process is canceled and an error message is issued.</p>
<ul style="list-style-type: none"> • <i>Phone refresh interval</i> (this setting is only relevant for Alcatel and Cisco) 	<p>Define the interval during which the status is supposed to be refreshed on the phone. If the interval is too short, the display starts blinking repeatedly. If the interval is too long, it may take very long until the current status of the recording is displayed on the end device.</p>
<i>Tagging Attributes</i>	<p>Here, you define which data field is filled when tagging via the PHONEapp. All additional data fields as well as the field <i>ASC_COMMENT</i> are available.</p>
<i>Register Fields</i>	<p>Here, you configure how the tagging value is displayed.</p> <p>All IDs listed under <i>Setup > Additional Data</i> as well as the field <i>ASC-COMMENT</i> can be used.</p>
<i>Predefined Tagging Fields</i>	<p>Define whether a comment field with free text or selectable predefined tagging fields are supposed to be used and saved on the end devices.</p>
<ul style="list-style-type: none"> • <i>Activated</i> 	<p>Activates the list of predefined tagging fields on the end device. If the function has been deactivated, a manual comment field is displayed.</p>

- *Tagging Field*

Define which selectable predefined tagging fields are supposed to be used and saved on the end devices.

Configure tagging attributes



The name of the request parameter *tag_field* must not be changed nor must its assignment be deleted. Otherwise tagging via the PHONEapp does not work anymore. The request parameter *tag_field* can be allocated to another available field, though.




Tagging attributes should only be changed in exceptional justified cases. Incorrect changes can cause a malfunction of the PHONEapp.

Every request parameter may only be used once. The available field may be allocated several times to different request parameters. All additional data which has been marked as available in the Additional Data module of the application System Configuration can be used as field.

Add and edit tagging attributes


1. In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Tagging Attributes*.

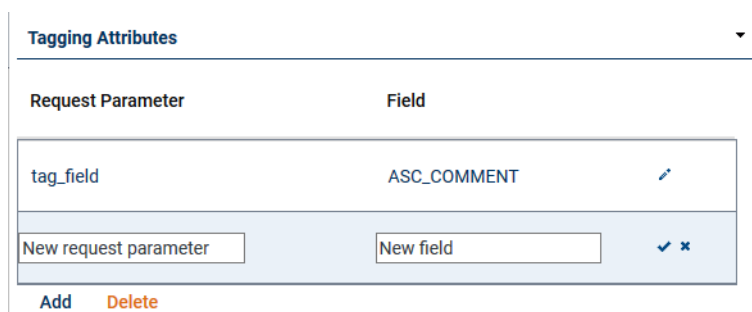


Request Parameter	Field
tag_field	ASC_COMMENT

Add Delete

Fig. 351: Group field Tagging Attributes



2. Click on the button *Add*.
⇒ A new entry is added.
3. To edit the entry, click on the icon .
⇒ The line can be edited.



Request Parameter	Field
tag_field	ASC_COMMENT
New request parameter	New field

Add Delete

Fig. 352: Edit tagging attributes

4. Enter the respective parameters.
5. To save the changes, click on the icon .
To discard the changes, click on the icon .
6. In the detail view, click on the button *Save* to apply the changes in the tab *Default Settings*.

Delete tagging attributes

1. In the detail view, select the attribute you would like to delete.
2. Click on the button *Delete*.
3. Click on the button *Yes*.

⇒ The selected attribute is removed from the list.

4. Click on the button *Save* to apply the change in the tab *Default settings*.

Configure register fields

Add and edit register fields

1. In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Register Fields*.





Register Fields			
Field	Recording Control Field		Active
Comment	ASC_COMMENT	✓	
Add Delete			

Fig. 353: Group field Register Fields

2. Click on the button *Add*.
⇒ A new entry is added.
3. To edit the entry, click on the icon .
⇒ The line can be edited.

Register Fields			
Field	Recording Control Field		Active
Comment	ASC_COMMENT	✓	
<input type="text" value="New field"/>	<input type="text" value="New RC field"/>	<input checked="" type="checkbox"/>	 
Add Delete			

Fig. 354: Edit register fields

4. Enter the respective parameters.
The name in the field *Field* can be selected arbitrarily. In the field *Recording Control Field*, all IDs listed under *Setup > Additional Data* can be used. In addition, the field name *ASC_COMMENT* can be used.
5. Activate or deactivate the register field via the check box.
6. To save the changes, click on the icon .
To discard the changes, click on the icon .
7. In the detail view, click on the button *Save* to apply the changes in the tab *Default Settings*.

Delete register fields

1. In the detail view, select the attribute you would like to delete.
2. Click on the button *Delete*.
3. Click on the button *Yes*.
⇒ The selected attribute is removed from the list.
4. Click on the button *Save* to apply the change in the tab *Default Settings*.

Configure predefined tagging fields

Within the *PHONEapp* you can tag and mark recorded conversations. That way, you can categorize recorded conversations which facilitates filtering and searching for them at a later moment. The *PHONEapp* offers the default possibility to either enter a free text in the comment field or to use predefined tagging fields. The user can see these attributes when pressing a certain key of the end device. That way, the user can tag this conversation during or after the recording.

Activate comment field with free text

1. In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Predefined Tagging Fields*.
 2. Deactivate the check box *Activated*.
- ⇒ The comment with free text is displayed during the tagging process.

Activate tagging fields without free text

Here, you can configure predefined tagging fields which are supposed to be added to the conversation.

1. In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Predefined Tagging Fields*.

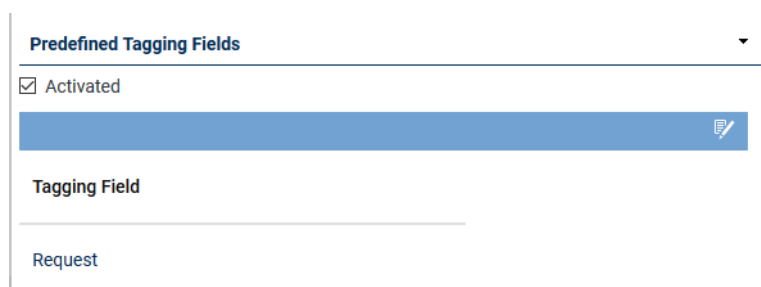

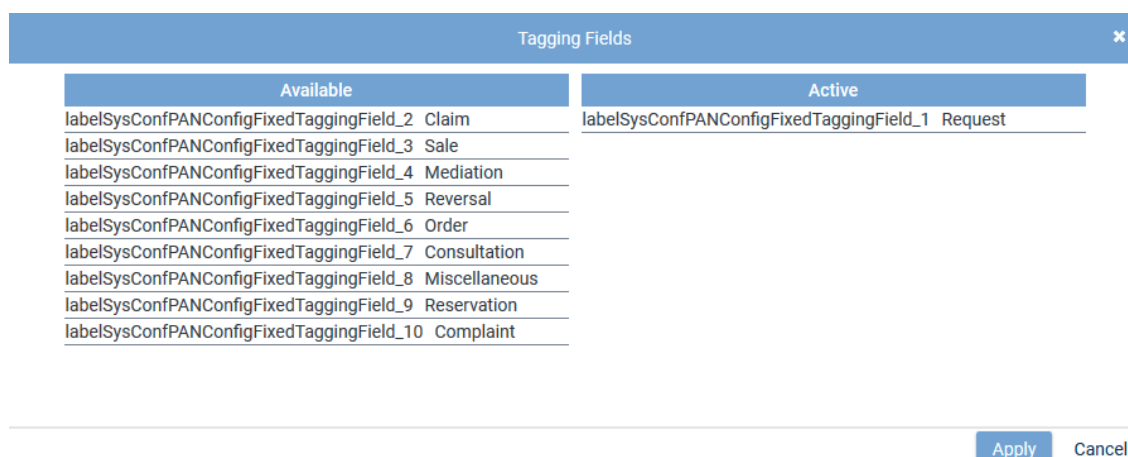



Fig. 355: Configure tagging fields

2. Activate the check box *Activated*.
 3. Click on the icon  (*Edit*).
- ⇒ The window *Tagging Fields* appears.



Available	Active
labelSysConfPANConfigFixedTaggingField_2 Claim	labelSysConfPANConfigFixedTaggingField_1 Request
labelSysConfPANConfigFixedTaggingField_3 Sale	
labelSysConfPANConfigFixedTaggingField_4 Mediation	
labelSysConfPANConfigFixedTaggingField_5 Reversal	
labelSysConfPANConfigFixedTaggingField_6 Order	
labelSysConfPANConfigFixedTaggingField_7 Consultation	
labelSysConfPANConfigFixedTaggingField_8 Miscellaneous	
labelSysConfPANConfigFixedTaggingField_9 Reservation	
labelSysConfPANConfigFixedTaggingField_10 Complaint	

Fig. 356: Edit tagging fields

4. To add a field, select the field and use drag and drop to transfer it from the list of available fields on the left to the list *Active* in the window on the right.
5. To apply the changes, click on the button *Apply*.
To discard the changes, click on the button *Cancel* or on the icon .

6. To activate the fields you have added, click on the check box *Activated*.
 7. In the detail view, click on the button *Save* to apply the changes in the tab *Default Settings*.
- The following fields are available by default in the list *Available*:











<i>Request</i>	Use this attribute to tag conversations which revolve around a request.
<i>Claim</i>	Use this attribute to tag conversations which revolve around a claim.
<i>Mediation</i>	Use this attribute to tag conversations which revolve around a mediation.
<i>Order</i>	Use this attribute to tag conversations which revolve around an order.
<i>Consultation</i>	Use this attribute to tag conversations which revolve around a consultation.
<i>Reservation</i>	Use this attribute to tag conversations which revolve around a reservation.
<i>Complaint</i>	Use this attribute to tag conversations which revolve around a complaint.
<i>Sale</i>	Use this attribute to tag conversations which revolve around a sale.
<i>Reversal</i>	Use this attribute to tag conversations which revolve around a reversal.



The tagging fields are displayed along with their corresponding resource string. You can adjust the tagging fields in the Resource Editor module of the application System Configuration. See administration manual *System Configuration - Resource Editor*.

Changes in the Resource Editor module only apply for future recordings. Existing taggings are not changed.

The following functions are available in the window *Tagging Fields*:

	<i>Add</i>	Adds the selected column.
	<i>Add all</i>	Adds all selected columns.
	<i>Remove</i>	Removes the selected column.
	<i>Remove all</i>	Removes all selected columns.
	<i>Up</i>	Moves the selected column one row up.
	<i>First position</i>	Places the selected column first.
	<i>Down</i>	Moves the selected column one row down.
	<i>Last position</i>	Places the selected column last.
	Saves all changes and closes the window <i>Tagging Fields</i> .	
	Closes the window <i>Tagging Fields</i> without applying the changes.	
	Closes the window <i>Tagging Fields</i> without applying the changes.	



You can change the position of a tagging field by selecting the field with the left mouse key and dragging it to the respective position.

7.3.4.4 Configure PBX module

In the PBX module, you have to activate the PHONE_{app} configuration.

1. In the navigation bar, select the menu item *Setup > PBX*.

2. Select the tab **PHONEapp Configuration**.

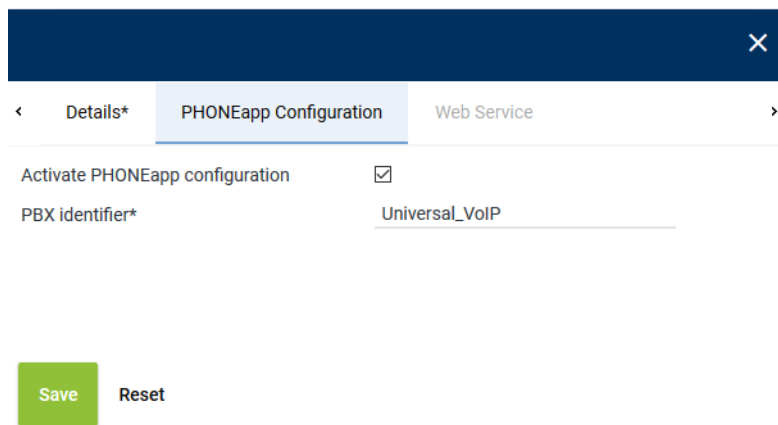


Fig. 357: Activate PHONEapp configuration

3. Enter the following parameters:

Activate PHONEapp configuration	Here, the PHONEapp is activated.
PBX identifier	Enter the identifier of the PBX. The identifier allows the PBX to connect with the PHONEapp. This identifier is specified during the installation of the PBX. Only use letters, numbers, and underscores.

4. In the detail view, click on the button **Save** to apply the changes in the tab **PHONEapp Configuration**.



The fields marked with " * " are mandatory fields. These fields have to be filled out.

7.3.4.5 Configure Phones module

In the Phones module, you can create and configure phones.

1. Select the menu item **Setup > Phones** in the navigation bar.

⇒ The following window appears:

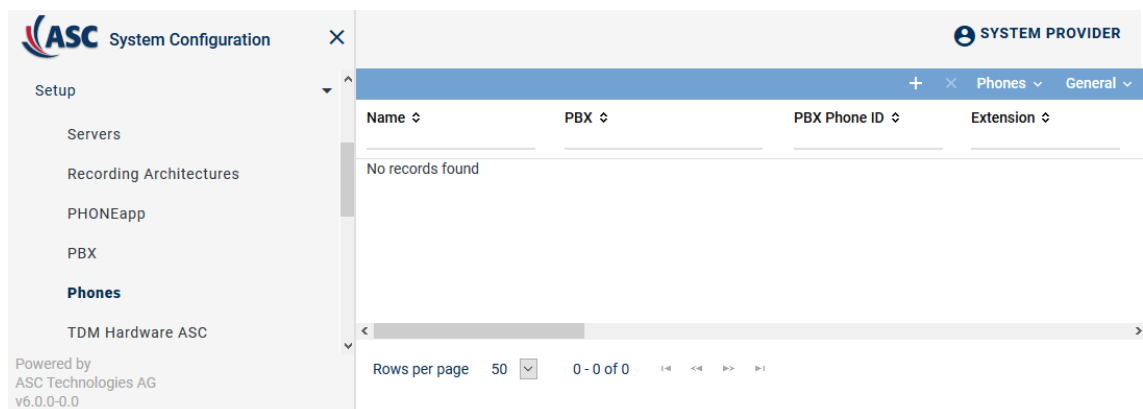



Fig. 358: Phones - main view


Depending on the table configuration, the following information is displayed in the table in the main view:

Name	Shows the name of the phone.
PBX	Shows the name of the PBX.

<i>PBX Phone ID</i>	Shows the identifier which has been configured for the phone in the PBX.
<i>Extension</i>	Shows the assigned extension of the phone.
<i>Computer Name</i>	Shows the computer name if it has been defined in the details.
<i>Phone Type</i>	Shows the selected phone type if the PHONE _{app} configuration has been activated.
<i>Display Language</i>	Shows the selected display language.

NOTICE! You can add hidden columns to the table in the main view via the icon  (*Adjust table*) in the toolbar.

7.3.4.5.1 Create phones

1. Click on the icon  (*Create*) in the toolbar of the window Phones to create new phones. In recording solutions using TDM phones as well as IP phones, a context menu appears in which you can select which phone type you would like to create. The selection depends on the PBX and the installed licenses.

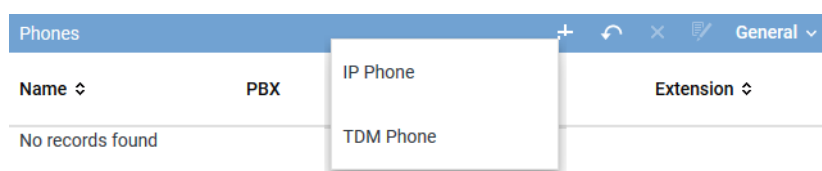



Fig. 359: Create phones Select phone type

The configuration parameters depend on each other. For the unambiguous mapping at least one of the following combinations must be configured for the name of the phone:

- PBX phone ID and SSRC
 - Extension and PBX phone ID
 - Extension and computer name
 - Extension and IP address
 - Extension and MAC address
 - Computer name and PBX phone ID
 - Computer name and IP address
 - Computer name and MAC address
2. In the detail view, click on the button *Save* to apply the changes.
- ⇒ The recently created phone appears in the main view.

7.3.4.5.2 Delete phones

1. In the main view, select the phone you would like to delete.
2. Click on the icon  (*Delete*).
 - ⇒ The security prompt to delete an element appears.
3. To really delete the selected phone, confirm the security prompt.

7.3.4.6 Configure Recording Planner module

The different operation modes for recording calls are configured in the Recording Planner module of the System Configuration.

Information about the creation of profiles can be found in the administration manual *ASC System Configuration - Recording Planner* for Tenants.

7.3.5 Import InAttend conversation to neo

Supported import formats

WAV + CSV

This import format allows you to import recordings which have been created by a third-party system. Audio data must be available in [WAVE](#) format. If the required additional data is contained in the file name, then no separate [CSV](#) file is needed.

A corresponding [CSV](#) file is required, if the data can only be extracted from the content. The file names of associated files have to be identical except for the file extension so that the additional data can be mapped correctly.

WAV + XML

This import format allows you to import recordings which have been created by a third-party system. Audio data must be available in [WAVE](#) format.

If the required additional data is contained in the file name of the [WAVE](#) file, then no separate [XML](#) file is needed.

A corresponding [XML](#) file is required, if the data can only be extracted from the file content. The file names of associated files have to be identical except for the file extension so that the additional data can be mapped correctly.

To import conversations from an InAttend Console of Mitel to the *neo* system, the following pre-conditions must be met:

- Audio data must be available in [WAVE](#) format.
- In the Servers module in the tab *Usage*, the functions *Data storage and import* must have been activated.
- In the PBX module, a [PBX](#) must have been configured.
- In the Additional Data module, respective fields for the additional data must have been configured.
e. g. *customCP01*.
- In the Recording Import module, you must configure an import job.

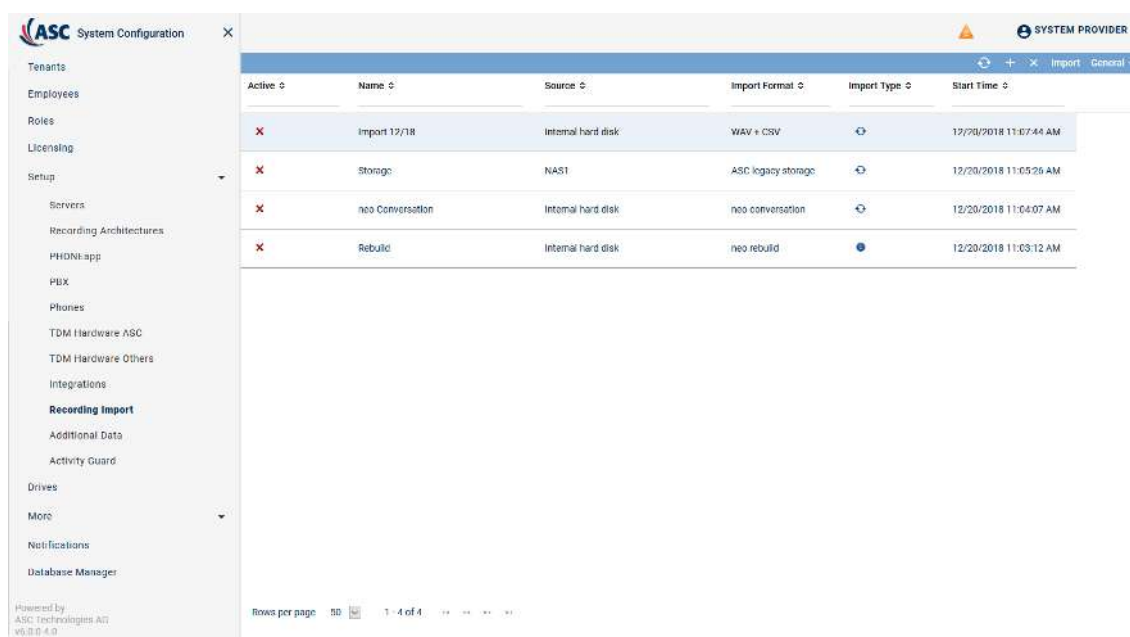
7.3.5.1 Configure import job

To import recordings, you must configure an import job.



The following configuration has to be carried out as system administrator.


1. Open the application *System Configuration*.
2. Log in as system provider.
3. Select the menu item *Setup > Recording Import*.



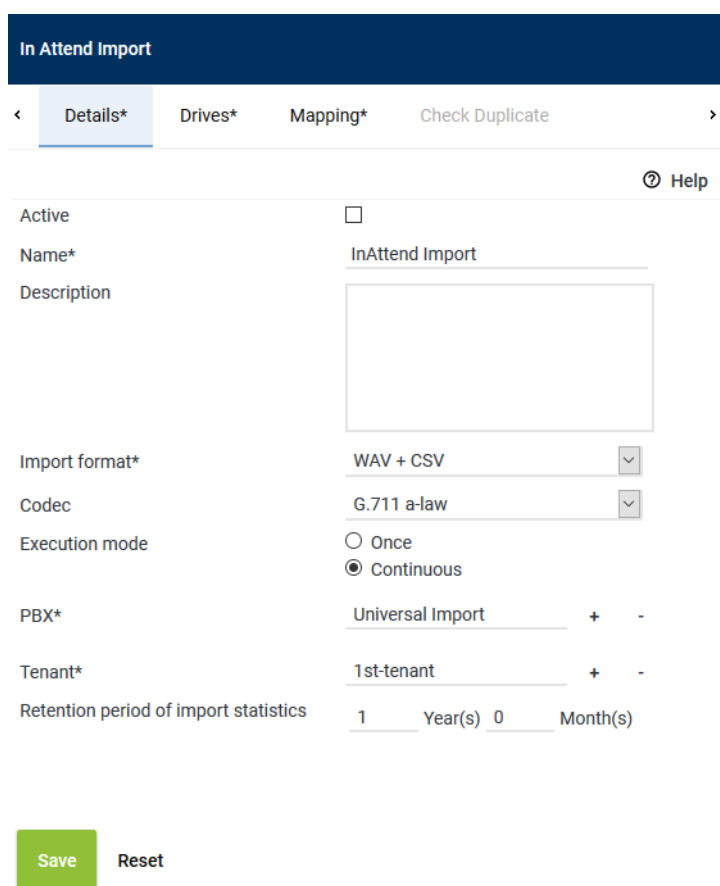
Active	Name	Source	Import Format	Import Type	Start Time
<input checked="" type="checkbox"/>	Import 12/18	Internal hard disk	WAV + CSV		12/20/2018 11:07:44 AM
<input checked="" type="checkbox"/>	Storage	NAS1	ASC legacy storage		12/20/2018 11:05:26 AM
<input checked="" type="checkbox"/>	neo Conversation	Internal hard disk	neo conversation		12/20/2018 11:04:07 AM
<input checked="" type="checkbox"/>	Rebuild	Internal hard disk	neo rebuild		12/20/2018 11:03:12 AM

Rows per page: 50 1 - 4 of 4

Fig. 360: Main view

- Click on the icon  (Create) in the toolbar of the main view.
 - The new import configuration is displayed in the detail view. The configuration options depend on the selected import format.

7.3.5.1.1 Tab Details



In Attend Import

<

Details*

Drives*

Mapping*

Check Duplicate

>

Active

☐

Name*

InAttend Import

Description

Import format*

WAV + CSV

Codec

G.711 a-law

Execution mode

☐ Once
 ☒ Continuous

PBX*

Universal Import

+

-

Tenant*

1st-tenant

+

-



Retention period of import statistics

1 Year(s) 0 Month(s)


Save

Reset

Fig. 361: Tab Details (example)

<i>Active</i>	<p>Once the configuration has been completed, you can activate the import job by means of the check box.</p> <p><input checked="" type="checkbox"/> = Job is active.</p> <p><input type="checkbox"/> = Job is not active.</p> <p>As long as an import job is active, the recording system checks whether new files are available in the source directory. If new data is available, it is imported.</p>
<i>Name</i>	Enter the name for the import job.
<i>Description</i>	Here, you can enter a description of the import job.
<i>Import format</i>	<p>Select the import format from the drop-down list. The following formats have been tested by ASC and are supported:</p> <ul style="list-style-type: none"> • WAV + CSV • WAV + XML
<i>Codec</i>	<p>Select the codec from the drop-down list in which the recordings are supposed to be saved.</p> <p>The following codecs are supported:</p> <ul style="list-style-type: none"> • G.711 A-law • G.711 μ-law • G.729a • Linear PCM 8 bit
<i>Execution mode</i>	<p>Select whether the import is supposed to be executed once or continuously.</p> <ul style="list-style-type: none"> • <i>Once</i> <p>The import is started upon activating the import configuration. The source directory is checked for data only once.</p> <ul style="list-style-type: none"> • <i>Continuous</i> <p>The import is started permanently upon activating the import configuration and does not end before the import configuration is deactivated manually. The source directory is constantly checked for new data as long as the import configuration is active.</p> <p>NOTICE! For some import formats only continuous execution is available. In this case, the present setting is automatic.</p>
<i>PBX</i>	<p>By clicking on the button , select for which PBX the data is supposed to be imported, see chapter "Assign PBX", p. 303.</p> <p>It is necessary to map the imported data to a PBX so that the extensions can be mapped. For a mere import, you can either select a configured Mitel PBX or a PBX of the type <i>Universal Import</i>. The PBX must have been configured in the PBX module previously.</p>
<i>Tenant</i>	<p>By clicking on the button , select which tenant the imported data is supposed to be mapped to, see chapter "Assign tenant", p. 304.</p> <p>NOTICE! In a 1-tenant system, the tenant is entered here automatically. The setting cannot be changed.</p>

Assign PBX

1. Click on the button  on the right of the entry field.
2. Select a [PBX](#) from the list.



Dialog titled "PBX" with a close button (X) in the top right corner. It contains a table with two columns: "Name" and "Type". The table lists various PBX systems. At the bottom, there are "Add" and "Cancel" buttons.

Name	Type
SIP	Universal VoIP
Cisco ...	Cisco UCM
Avaya_1	Avaya CM
Cisco Jabber	Cisco Jabber
Universal import	Universal import
Universal analog CM	Universal analog CM
OpenScape Xpert	OpenScape Xpert

Rows per page: 20 (dropdown) | 1 - 20 of 21 | Navigation icons: first, previous, next, last

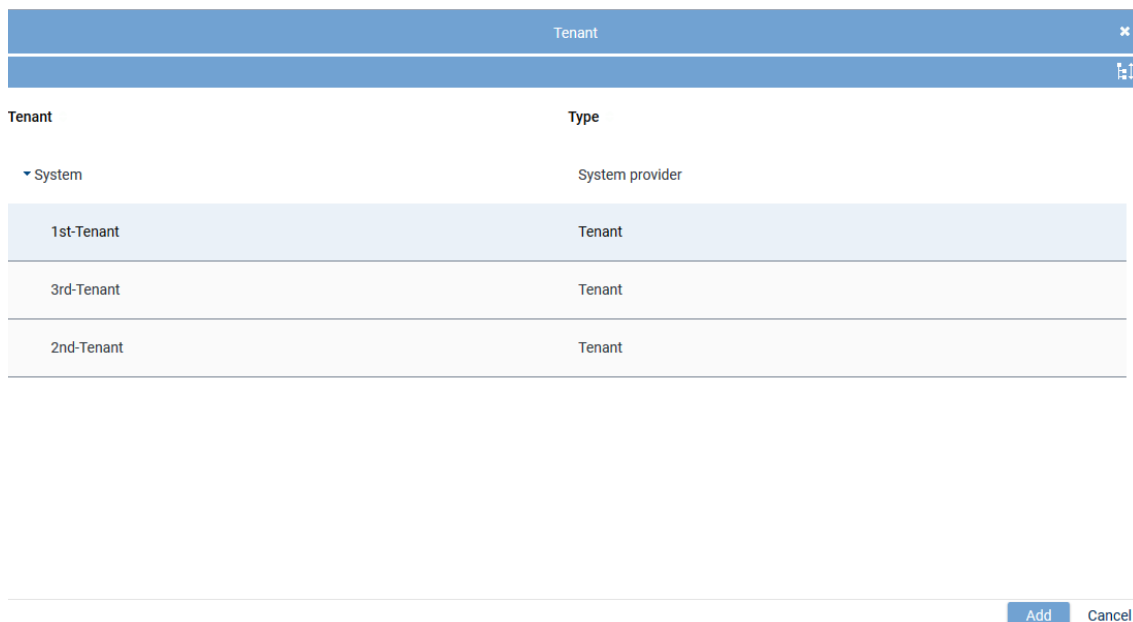
Buttons: Add, Cancel

Fig. 362: Add PBX

- To apply the selection, click on the button *Add*.
To discard the selection and close the window, click on the button *Cancel*.

Assign tenant

- Click on the button **+** on the right of the entry field.
- Select a tenant from the list.



Dialog titled "Tenant" with a close button (X) in the top right corner. It contains a table with two columns: "Tenant" and "Type". The table lists various tenants. At the bottom, there are "Add" and "Cancel" buttons.

Tenant	Type
System	System provider
1st-Tenant	Tenant
3rd-Tenant	Tenant
2nd-Tenant	Tenant

Buttons: Add, Cancel

Fig. 363: Add tenant

- To apply the selection, click on the button *Add*.
To discard the selection and close the window, click on the button *Cancel*.

7.3.5.1.2 Tab Drives

- Select the tab *Drives* to configure the source.



A drive can be used in several job configurations as long as the drive is not used actively by a configuration.

If a drive is currently used actively by a job, no additional job which uses the same drive can be released or activated. This behavior includes all modules, i. e. regardless of the module that the configuration belongs to.

Settings depend on the selected import format.

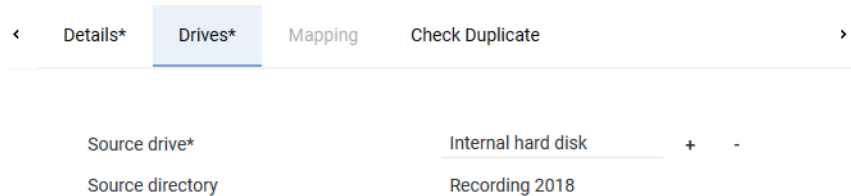


Fig. 364: Tab Drives - WAVE formats

Source drive	Select the drive from which the data is supposed to be imported, see chapter "Assign drive", p. 305 .
Source directory	Enter the directory from which the data is supposed to be imported.

Assign drive

1. Click on the button **+** on the right of the entry field.
2. Select a drive from the list.

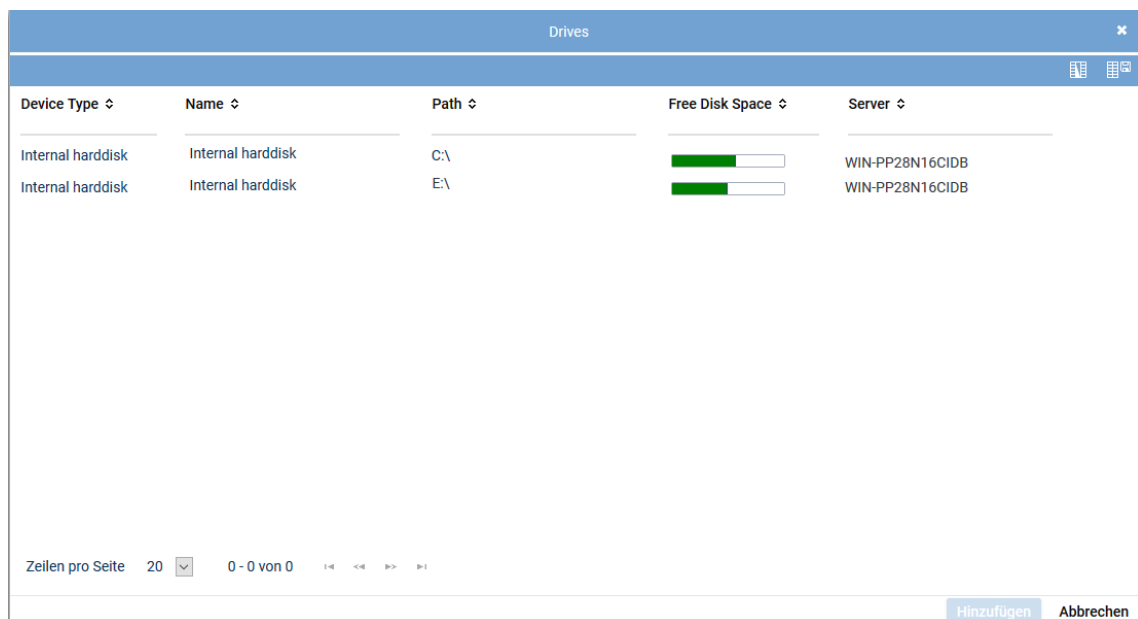


Fig. 365: Add drive

3. To apply the selection, click on the button **Add**.
To discard the selection and close the window, click on the button **Cancel**.

7.3.5.1.3 Tab Mapping

1. Select the tab *Mapping*.

Here, you can configure the rules that have to be observed when mapping the additional data from the sets of data which are supposed to be imported to the data structure in the neo recording system.

The following group fields are available to be configured:

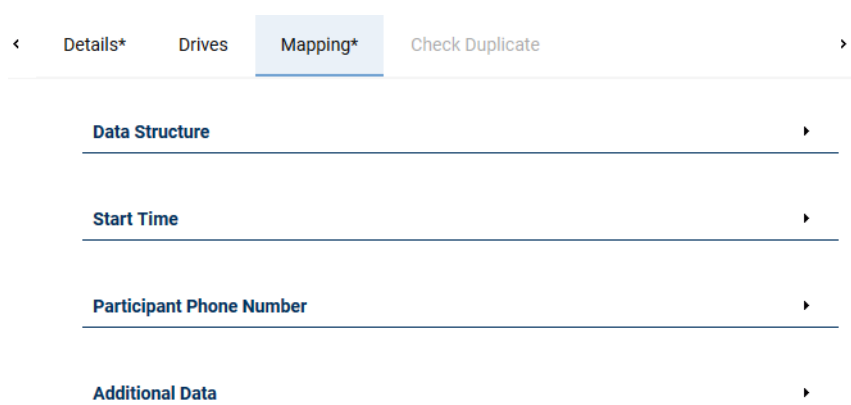


Fig. 366: Tab Mapping for **WAVE** import format

The additional data can either be extracted from the file name of the **WAVE** file or from the file content of the delivered **CSV** or **XML** file.

The file names of associated files (**WAVE** and XML file or **WAVE** and CSV file) have to be identical except for the file extension so that the additional data can be mapped correctly.

If no separate file with additional data is available, the additional data is extracted from the file name of the **WAVE** file.

Example for a file name of a **WAVE** file:

%y-%m-%d_%H-%M-%S_%ATT_ID_%A_NUM_%B_NUM.wav

e. g. 2019-11-06_10-44-46_Shruthiv_9002_61.wav

Group field Data Structure

If the information from the file name is supposed to be used, enter the format of the file name.

If you use the import format **WAV + CSV**, additionally enter the delimiter which separates the columns in the file content.



Fig. 367: Group field Data Structure

There are 2 options for data formats:

1. The file name consists of information sections which are separated by a certain delimiter. A new section always starts at the beginning of a file name and behind a delimiter. Every section ends in front of a delimiter and in front of the period preceding the file extension.

Example: The file name "MyRecordings_2013-10-01_0681-123456.wav" consists of 3 sections which are separated by understrikes.

In this case, select the option *separated by delimiter* and enter the delimiter in the entry field.

NOTICE! Numbers and letters cannot be used as delimiters.

- The file name consists of information sections which are **not** separated by a certain delimiter.

In this case, you have to define a regular expression which marks the sections as groups.

In this case, select the option *defined by regular expression* and enter the regular expression in the entry field.

Group field Start Time

Here, you can define how the start time of the recordings is supposed to be read out of the file name or the file content.

Import format WAV + CSV

Start Time	Start Time
Source <input type="text" value="File name"/>	Source <input type="text" value="File content"/>
<input type="radio"/> Date and time in same section Section no.* <input type="text" value="1"/> Format* <input type="text"/>	<input checked="" type="radio"/> Date and time in the same column Column* <input type="text" value="Starttime"/> Format* <input type="text" value="yy-MM-dd-hh-mm-ss"/>
<input checked="" type="radio"/> Date and time in separate sections Section no. for date* <input type="text" value="1"/> Format* <input type="text" value="yyyy-MM-dd"/> Section no. for time* <input type="text" value="2"/> Format* <input type="text" value="hh-mm-ss"/>	<input type="radio"/> Date and time in separate columns Column for date* <input type="text"/> Format* <input type="text"/> Column for time* <input type="text"/> Format* <input type="text"/>

Fig. 368: Group field Start Time - import format WAV + CSV

- Select the source from which the information is supposed to be read out.
- Select whether one and the same information section contains date and time.
- Enter at which location of the structure the relevant information can be found.
 - For *Source = File name*:
Enter the number of the section which contains the information.
You have to enter the delimiter which separates the sections in the file name in the group field *Data Structure*, see [chapter "Group field Data Structure", p. 306](#).
 - For *Source = File content*:
Enter the name of the column which contains the information.
- Enter the format which contains date and time in the different information sections, see Format definitions.

Import format WAV + XML

Start Time	Start Time
Source <input type="text" value="File content"/>	Source <input type="text" value="File name"/>
<input checked="" type="radio"/> Date and time in the same XML tag XML tag* <input type="text" value="Recording/Starttime"/> Format* <input type="text" value="yy-MM-dd-hh-mm-ss"/>	<input type="radio"/> Date and time in same section Section no.* <input type="text" value="1"/> Format* <input type="text"/>
<input type="radio"/> Date and time in separate XML tags XML tag for date* <input type="text"/> Format* <input type="text"/> XML tag for time* <input type="text"/> Format* <input type="text"/>	<input checked="" type="radio"/> Date and time in separate sections Section no. for date* <input type="text" value="1"/> Format* <input type="text" value="yyyy-MM-dd"/> Section no. for time* <input type="text" value="2"/> Format* <input type="text" value="hh-mm-ss"/>

Fig. 369: Group field Start Time - import format WAV + XML

1. Select the source from which the information is supposed to be read out.
2. Select whether one and the same information section contains date and time.
3. Enter at which location of the structure the relevant information can be found.
 - For *Source = File name*:
Enter the number of the section which contains the information.
You have to enter the delimiter which separates the sections in the file name in the group field *Data Structure*, see [chapter "Group field Data Structure", p. 306](#).
 - For *Source = File content*:
Enter the hierarchical order of the XML tags from the root element to the XML tag which contains the information. The XML tag sequence has to be entered without blanks and the individual XML tags separated by a slash (e. g. Recording/Starttime). If the relevant information is contained in an attribute, then the attribute name has to be entered in square brackets preceded by an @ sign (e. g. Recording/Starttime[@date]).
4. Enter the format which contains date and time in the different information sections, see Format definitions.

Group field Participant Phone Number

Here, you can define from which sections the information of the conversation participants is supposed to be read out from the file name.

Participant Phone Number		
Handling of stereo recordings		<input type="checkbox"/> Mix stereo to mono
Several phone numbers in a column separated by <input type="text"/>		
<small>(max. 1 characters)</small>		
Source	Section No./Column	Track
File name	4	left
File name	5	left
New	Edit	Delete

Fig. 370: Group field Participant phone number (example)

Handling stereo recordings	This option is not relevant for InAttend conversation, as WAVE files are available in mono only.
-----------------------------------	--

Several phone numbers in a column separated by This option is not relevant, as the information is read out from the **WAVE** files name.

List

The list shows all import configuration rules that have been saved to be able to map the participant phone numbers.

Source	Shows whether the information is read out of the file name or out of the file content.
Section No./XML Tag or Section no./Column	Shows from which information section the information is read out. NOTICE! The column title depends on the import format.
Track	Selecting a track is not relevant for InAttend conversations, as the import files are available in mono.

Tab. 77: Mapping rules for participant phone numbers

New	The button opens a window in which you can create a new entry. See chapter "Configure source for participant phone numbers", p. 309 .
Edit	The button opens a window in which you can edit a selected entry. See chapter "Configure source for participant phone numbers", p. 309 .
Delete	The button deletes the selected entry from the list.

Tab. 78: Buttons

Configure source for participant phone numbers

1. Click on the button *New* to configure a new source.

In the window *Source for Participant Phone Numbers*, you can define how additional data is supposed to be read out from the file name or the file content.

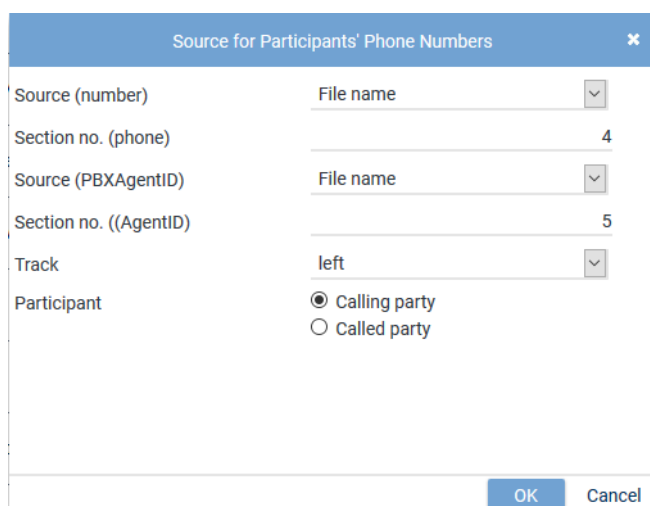


Fig. 371: Edit source for participant phone number (example)

Source	From the drop-down list, select the file name as the source for the additional data.
XML Tag or	Enter the number of the file name section that contains the information.

<i>Column Name</i> or <i>Section No.</i>	NOTICE! The name of the entry field depends on the source and the import format.
<i>Track</i>	Selecting a track is not relevant for InAttend conversations, as the import files are available in mono.
<i>Participant</i>	Select whether the phone numbers come from calling parties or from called parties.

- Click on the button *OK* to apply the configuration and close the window.

Configure source for additional data

- Click on the button *New* to configure a new source.

In the window *Source for Additional Data*, you can define how additional data is supposed to be read out from the file name and which additional data type they are supposed to be mapped to.

- In the group field *Additional Data*, click on the button *New* or *Edit*.

⇒ The following window appears:

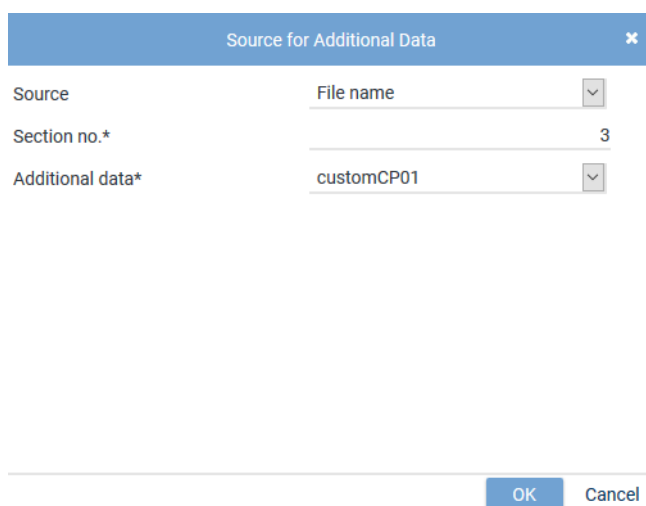


Fig. 372: Edit source for additional data (example for WAVE import format)

<i>Source</i>	From the drop-down list, select the <i>file name</i> as the source for the additional data.
<i>XML Tag</i> or <i>Column Name</i> or <i>Section No.</i>	Enter the number of the file name section that contains the information. NOTICE! The name of the entry field depends on the source and the import format.
<i>Additional data</i>	From the drop-down list, select the additional data type that the information is supposed to be mapped to. For further information about the configuration of the additional data refer to the administration manual System Configuration <i>Additional Data module</i> .

- Click on the button *OK* to apply the configuration and close the window.

See also

📄 Group field Data Structure [► 306]

7.3.5.2 Replaying conversations in POWERplay Web

1. Log in to the application *POWERplay* Web as administrator of the tenant to replay conversations.
2. Select the menu item *Recording View* in the navigation bar.

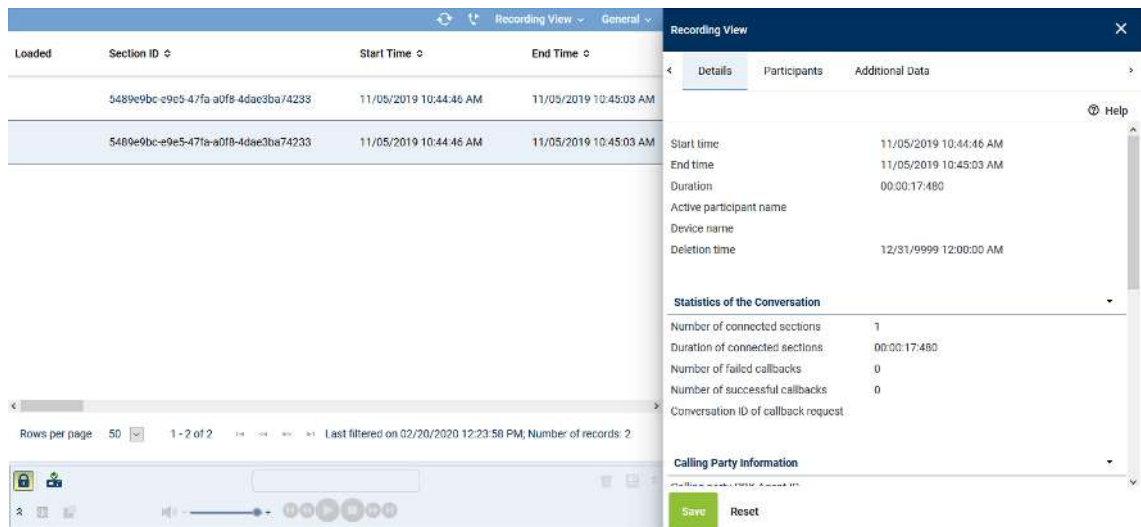


Fig. 373: POWERplay Web - Recording View

3. Use the search function to search for the start time of the conversation to select the conversation you have imported.
4. Select a conversation to check the additional data.
5. Change to the tab *Additional Data*.

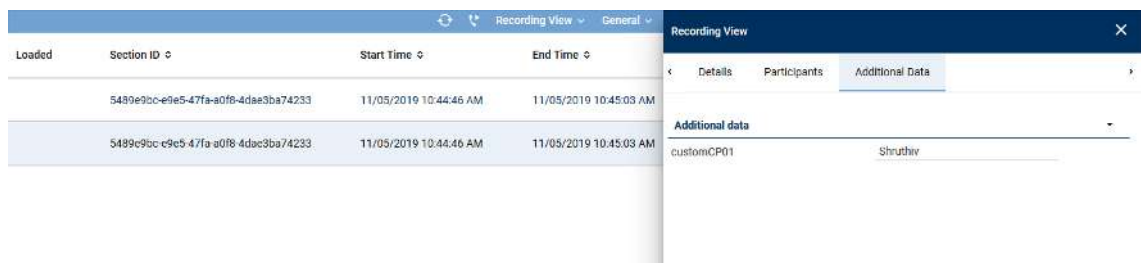


Fig. 374: Recording View - tab Additional Data

⇒ In the field *customCP01*, the name of the participant appears.

7.4 Configure CTIconnect add-on

7.4.1 Configure Genesys T-Server (optional)

7.4.1.1 Configure IP address and port of the Genesys T-Server

1. Log in to the Genesys Administrator.
2. Click on the menu item *Environment > Applications* in the navigation bar.

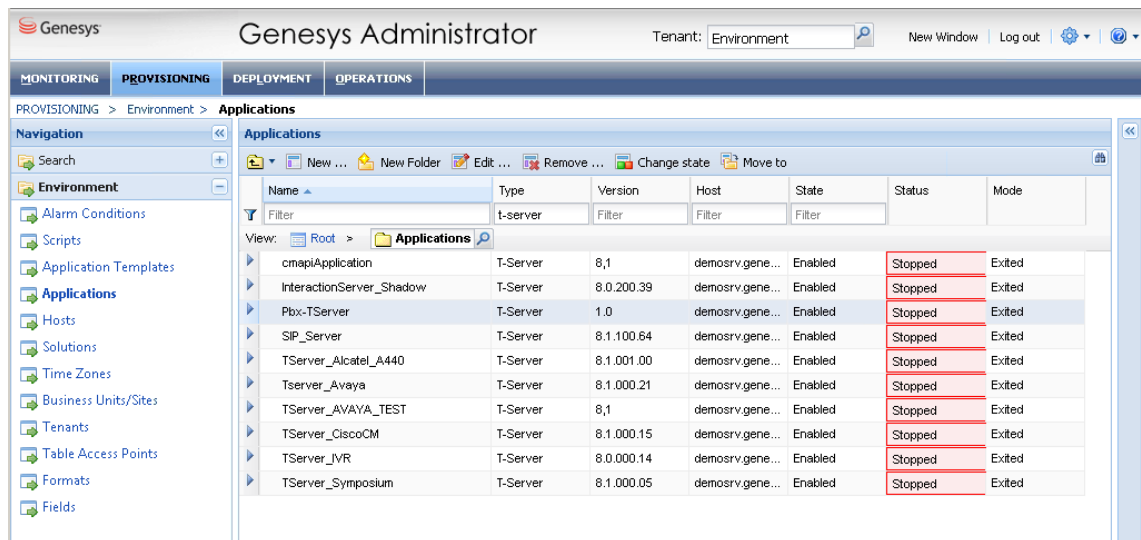


Fig. 375: Genesys Administrator - select T-Server

- Double-click on the entry T-Server which has been connected to the switch instance to be monitored.
⇒ The window *Configuration* appears.
- Expand the area *Server Info*.

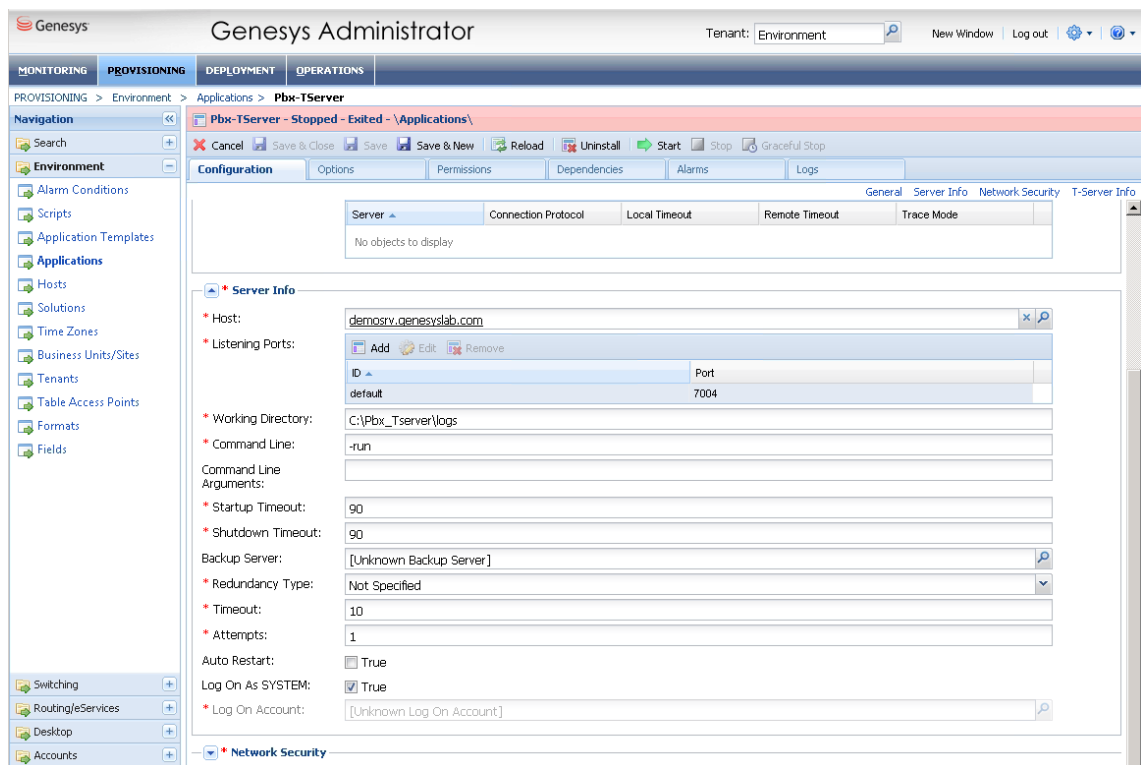


Fig. 376: Genesys Administrator - configure T-Server

- In the field *Host*, enter the IP address or the computer name of the T-Server, e. g. *demosrv8.genesyslab.com*.
- In the field *Listening Port*, enter the port of the T-Server, e. g.

7.4.1.2 Configure IP address and port of the Genesys Configuration Server

- Click on the menu item *Environment > Applications* in the navigation bar.

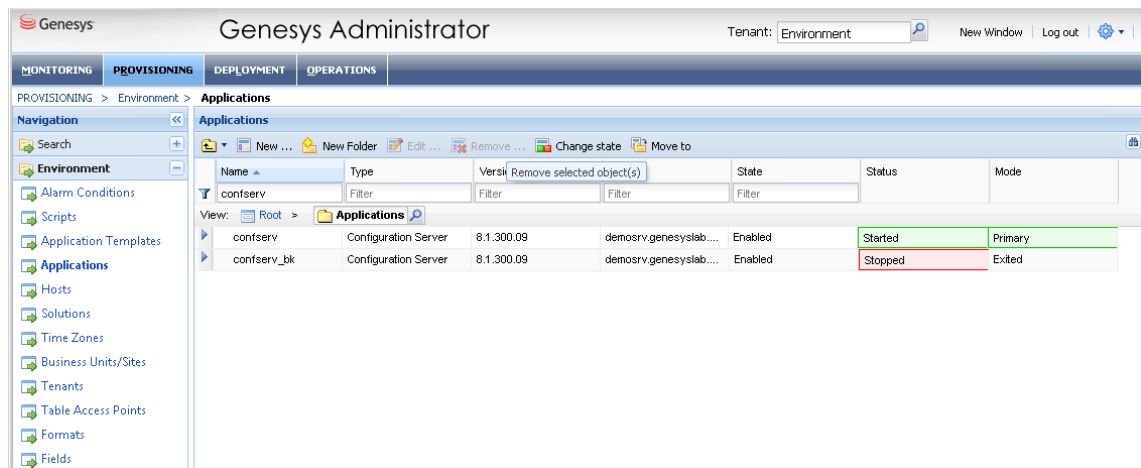


Fig. 377: Genesys Administrator - select configuration server

- Double-click on the entry Configuration Server, e. g. *confserv*.
⇒ The window *Configuration* appears.
- Expand the area *Server Info*.

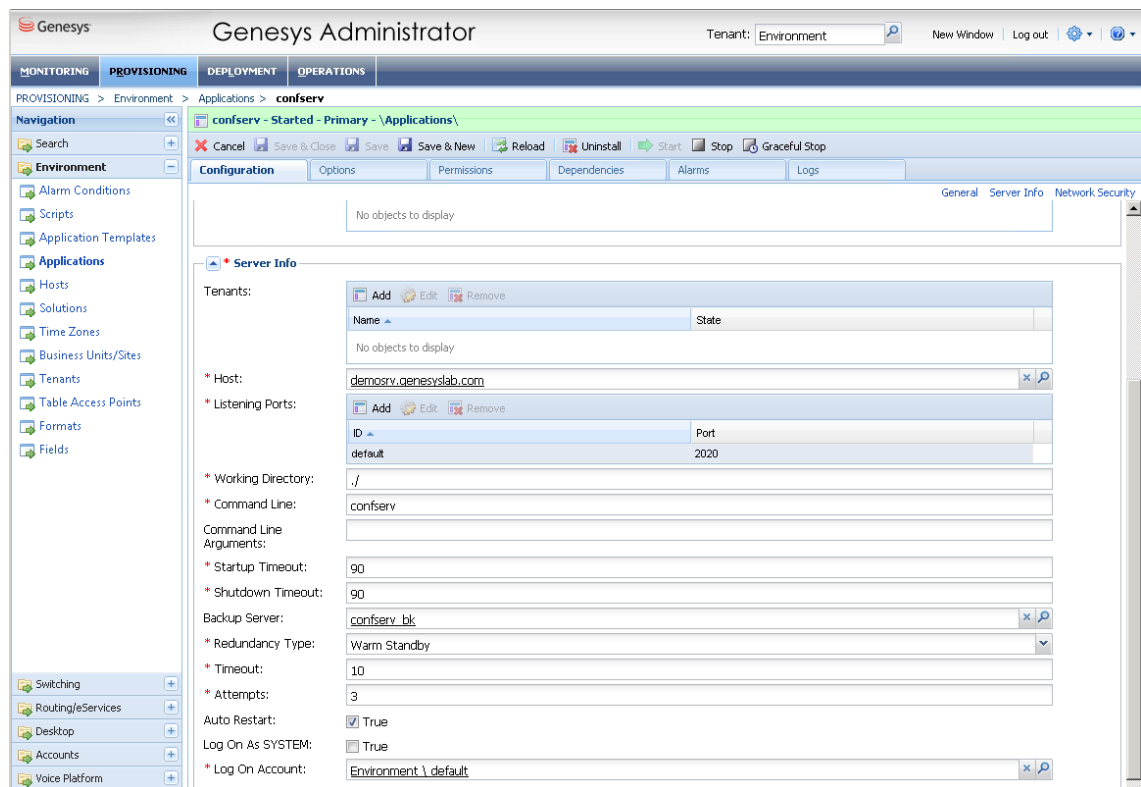


Fig. 378: Genesys Administrator - configure configuration server

- In the field *Host*, enter the IP address or the computer name of the configuration server, e. g. *demosrv8.genesyslab.com*.
- In the field *Listening Port*, enter the port of the configuration server, e. g. *2020*.

7.4.1.3 Configure switch instance in the Genesys Configuration Server

- Click on the menu item *Switching > Switches* in the navigation bar.

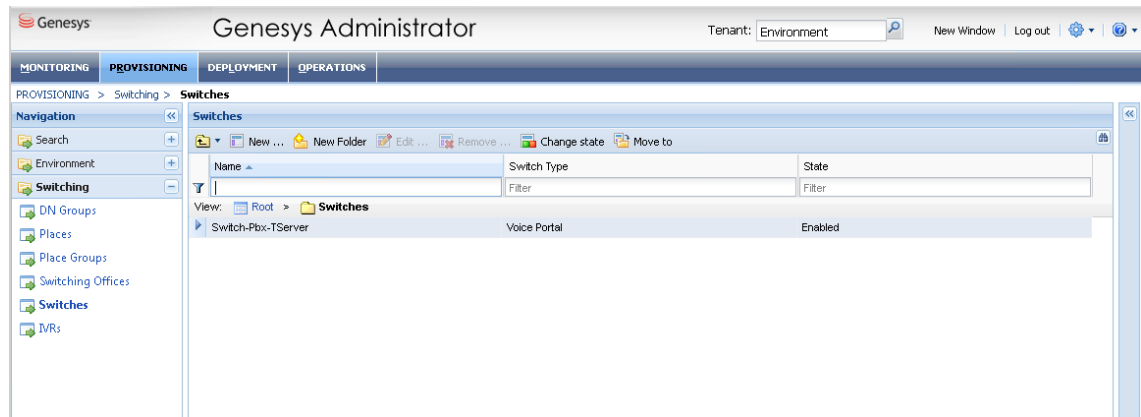


Fig. 379: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.
⇒ The window *Configuration > General* appears.

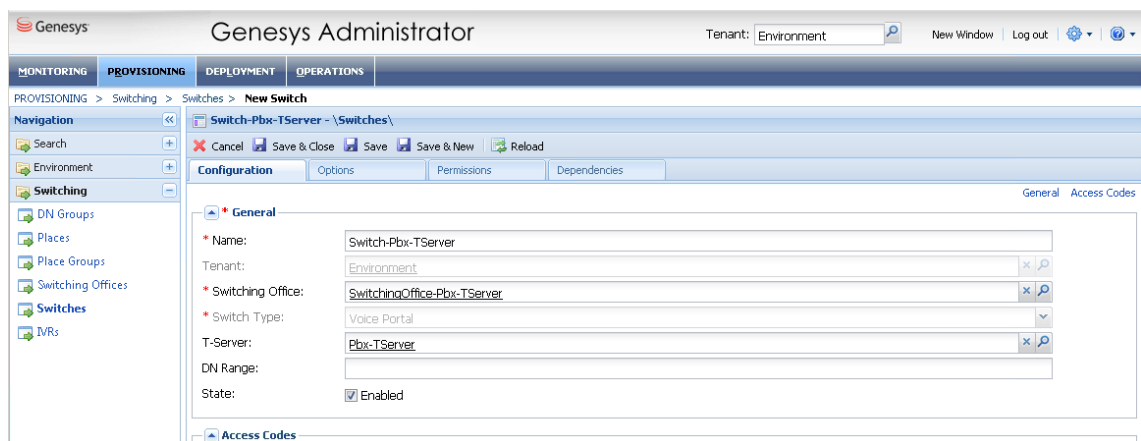


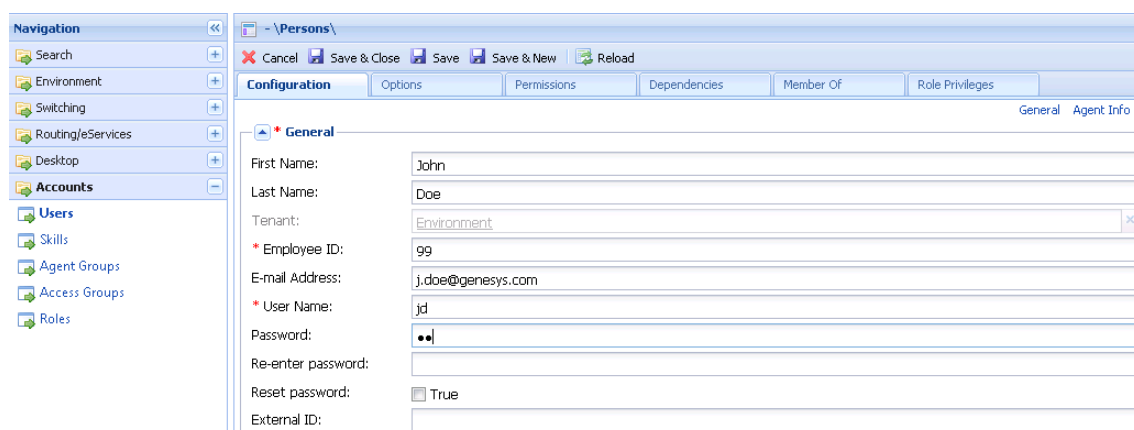
Fig. 380: Genesys Administrator - configure switch instance

3. Enter the same name in the configuration as in the Genesys T-Server.
4. Check whether the T-Server is identical to the T-Server configured in the Genesys T-Server.
5. Click on the button *Save* to save the entries.

7.4.1.4 Create users for the Genesys Configuration Server

To access the Genesys Configuration Server, you have to create a user.

1. Click on the menu item *Account > Users* in the navigation bar.
2. Click on the button *New*.
⇒ The window *Configuration > General* appears.



Navigation: Search, Environment, Switching, Routing/Services, Desktop, Accounts, Users, Skills, Agent Groups, Access Groups, Roles

Configuration: Options, Permissions, Dependencies, Member Of, Role Privileges

General Agent Info

* General

First Name: John

Last Name: Doe

Tenant: Environment

* Employee ID: 99

E-mail Address: j.doe@genesys.com

* User Name: jd

Password: [masked]

Re-enter password: [empty]

Reset password: ☐ True

External ID: [empty]

Fig. 381: Genesys administrator - create user

3. Complete the mandatory fields *Employee ID*, *User Name*, and *Password*.
4. Assign the user the rights to the created switch instance.
5. Click on the button *Save* to save the entries.

8 Troubleshooting



Before initiating any troubleshooting measures, verify that the recording solution has been configured according to the description in the manual and check whether an up-to-date hotfix version with bug fixes is available.

When opening a ticket, include the following information:

- Wireshark traces of the recording server
- server configuration of the end devices
- software version of the PBX
- software version of the Application Link Server
- type of the end devices

Log level settings

Module	Log level
RIA	DEBUG
RECORDING_CONTROL	DEBUG
RECORDING_MODULE_MANAGER	DEBUG
API_SERVER	DEBUG

When opening a ticket for the Genesys T-Server, include the following information:

- Log files with test calls
NOTICE! Before creating any log files, adjust the settings of the log levels in the Log Level module in the System Monitoring as described below, see user manual *System Monitoring*.
- detailed description of the issue and of the scenarios of the test calls which have been made
- extension of the affected device
- employed recording solution
- Wireshark traces of the recording network interface
- software version of the Genesys T-Server

Log level settings

Module	Log level
RIA	DEBUG
RIA_ASSISTANT_FOR_GENESYS	DEBUG
RECORDING_CONTROL	DEBUG
RECORDING_MODULE_MANAGER	DEBUG
API_SERVER	DEBUG
FILE_MANAGER	DEBUG

List of figures

Fig. 1	Recording solution with Mitel MiVoice CSTA 3	6
Fig. 2	Recording solution with VoIP end devices without MBG	7
Fig. 3	Recording solution with MBG	7
Fig. 4	Recording solution with intrusion	8
Fig. 5	Configure CSTA server	14
Fig. 6	Configure free-line signal for extension	16
Fig. 7	Check set monitor points	17
Fig. 8	Check license status	17
Fig. 9	Check server, path and port	18
Fig. 10	Check IP address and transport protocol	19
Fig. 11	Login screen MBG	19
Fig. 12	Certificate Management	20
Fig. 13	Confirm selected certificate	21
Fig. 14	Success message for a released certificate	21
Fig. 15	System Configuration - web interface	22
Fig. 16	System Configuration - main view:	23
Fig. 17	Recording architectures - main view	24
Fig. 18	Create recording architecture - All-in-one Basic Recording	25
Fig. 19	Recording architecture - tab Details	25
Fig. 20	Select integration type	26
Fig. 21	Recording Architecture - tab Server Assignment	27
Fig. 22	Recording Architecture - assign server	27
Fig. 23	Recording Architecture - activate recording type	28
Fig. 24	Recording architecture - activate recording architecture	28
Fig. 25	Servers - main view	29
Fig. 26	Toolbar Servers module	29
Fig. 27	Add server locations	30
Fig. 28	Delete server location	31
Fig. 29	Servers - tab Details	32
Fig. 30	Servers - tab Usage	32
Fig. 31	Group field API Server	33
Fig. 32	Select storage expansion	34
Fig. 33	Group field Audio Analysis	35
Fig. 34	Group field Recording Control/Key Management	35
Fig. 35	Group field Data Processing	36
Fig. 36	Select server	38
Fig. 37	Group field Replay	38
Fig. 38	Select server	40
Fig. 39	Group field Virtualization	40
Fig. 40	Servers module - tab Media Streamer	41
Fig. 41	Servers Module - tab Replay Server Address Mapping	43

Fig. 42	Servers module - tab Key Management.....	44
Fig. 43	Servers module - tab Keystore/Virtualization	45
Fig. 44	Add NTP server.....	46
Fig. 45	Edit IP address.....	47
Fig. 46	Remove NTP server.....	47
Fig. 47	Create new PBX.....	48
Fig. 48	Toolbar PBX module	48
Fig. 49	Create new PBX - tab Details	49
Fig. 50	Tenants - main view - tab Extensions	50
Fig. 51	Assign extensions to tenants	51
Fig. 52	Remove extensions.....	52
Fig. 53	Select extensions	53
Fig. 54	Tenants - main view - tab PBX Agent ID.....	54
Fig. 55	Assign PBX Agent IDs to tenants.....	54
Fig. 56	Select PBX Agent IDs	56
Fig. 57	Additional Data module main view	56
Fig. 58	Configure additional data	57
Fig. 59	Additional data - configure availability	57
Fig. 60	Integrations - main view	58
Fig. 61	Toolbar Integrations module	58
Fig. 62	Choose file	59
Fig. 63	Upload grammar	59
Fig. 64	Create integration type.....	60
Fig. 65	Integrations - select PBX.....	60
Fig. 66	Assign recording architecture - All-in-one Basic	61
Fig. 67	Configuration steps of the integration	61
Fig. 68	Configuration step - Configure Recording Architecture.....	62
Fig. 69	Configure CTIconnect module	62
Fig. 70	Configure connection data	63
Fig. 71	Configure connection data	63
Fig. 72	Arbitrary assignment of the additional data.....	64
Fig. 73	Configure switching conditions.....	65
Fig. 74	Configure regular expression for phone type identification	66
Fig. 75	Activate CTIconnect module 2	67
Fig. 76	Configure CTIconnect module	67
Fig. 77	Configure connection data	68
Fig. 78	Configure connection	68
Fig. 79	Arbitrary assignment of the additional data.....	69
Fig. 80	Configuration step - configure monitor points	70
Fig. 81	Add extension monitor points.....	71
Fig. 82	Configured extension monitor points.....	72
Fig. 83	Configuration step - Global Recording Settings	73

Fig. 84	Configure add-on for MiContact Center Enterprise	75
Fig. 85	Arbitrary assignment of the additional data	76
Fig. 86	Overview of the add on of Genesys T-Server	78
Fig. 87	Configure add-on for Genesys T-Server	79
Fig. 88	Configure connection data	80
Fig. 89	Arbitrary assignment of the additional data	82
Fig. 90	Configure miscellaneous settings	82
Fig. 91	Activate integration.....	83
Fig. 92	Activated integration.....	83
Fig. 93	Deactivate integration	84
Fig. 94	Recording architectures - main view	85
Fig. 95	Create recording architecture - All-in-one Failover	85
Fig. 96	Recording architecture - tab Details - All-in-one Failover.....	86
Fig. 97	Select integration type.....	87
Fig. 98	Recording Architecture - tab Server Assignment	88
Fig. 99	Recording Architecture - assign server - example	88
Fig. 100	Recording Architecture - activate recording type	89
Fig. 101	Recording architecture - activate recording architecture.....	89
Fig. 102	Servers - main view.....	90
Fig. 103	Toolbar Servers module	90
Fig. 104	Add server locations.....	92
Fig. 105	Delete server location	93
Fig. 106	Servers - tab Details.....	93
Fig. 107	Servers - tab Usage	94
Fig. 108	Group field API Server	94
Fig. 109	Select storage expansion.....	96
Fig. 110	Group field Audio Analysis	96
Fig. 111	Group field Recording Control/Key Management	97
Fig. 112	Group field Data Processing	98
Fig. 113	Select server	100
Fig. 114	Group field Replay	100
Fig. 115	Select server	102
Fig. 116	Group field Virtualization	102
Fig. 117	Servers module - tab Media Streamer	103
Fig. 118	Servers Module - tab Replay Server Address Mapping.....	105
Fig. 119	Servers module - tab Key Management.....	106
Fig. 120	Servers module - tab Keystore/Virtualization	107
Fig. 121	Add NTP server.....	108
Fig. 122	Edit IP address.....	109
Fig. 123	Remove NTP server.....	109
Fig. 124	Create new PBX.....	110
Fig. 125	Toolbar PBX module	110

Fig. 126 Create new PBX - tab Details	111
Fig. 127 Tenants - main view - tab Extensions	112
Fig. 128 Assign extensions to tenants	113
Fig. 129 Remove extensions.....	114
Fig. 130 Select extensions	115
Fig. 131 Tenants - main view - tab PBX Agent ID.....	116
Fig. 132 Assign PBX Agent IDs to tenants.....	116
Fig. 133 Select PBX Agent IDs	118
Fig. 134 Additional Data module main view	118
Fig. 135 Configure additional data	119
Fig. 136 Additional data - configure availability	119
Fig. 137 Integrations - main view	120
Fig. 138 Toolbar Integrations module	120
Fig. 139 Choose file	121
Fig. 140 Upload grammar	121
Fig. 141 Create integration type.....	122
Fig. 142 Integrations - select PBX.....	122
Fig. 143 Assign recording architecture - All-in-one Failover	123
Fig. 144 Configuration steps of the integration	123
Fig. 145 Configuration step - Configure Recording Architecture.....	124
Fig. 146 Configure CTIconnect module	124
Fig. 147 Configure connection data	125
Fig. 148 Configure connection data	125
Fig. 149 Arbitrary assignment of the additional data.....	126
Fig. 150 Configure switching conditions.....	127
Fig. 151 Configure regular expression for phone type identification	128
Fig. 152 Activate CTIconnect module 2	129
Fig. 153 Configure CTIconnect module	129
Fig. 154 Configure connection data	130
Fig. 155 Configure connection	130
Fig. 156 Arbitrary assignment of the additional data.....	131
Fig. 157 Configuration step - configure monitor points	132
Fig. 158 Add extension monitor points.....	133
Fig. 159 Configured extension monitor points.....	134
Fig. 160 Configuration step - Global Recording Settings	135
Fig. 161 Configuration step - Configure recording servers	137
Fig. 162 Tab Extensions	138
Fig. 163 Add extensions.....	138
Fig. 164 Added extensions.....	139
Fig. 165 Configure add-on for MiContact Center Enterprise.....	140
Fig. 166 Arbitrary assignment of the additional data.....	141
Fig. 167 Overview of the add on of Genesys T-Server	143

Fig. 168	Configure add-on for Genesys T-Server	144
Fig. 169	Configure connection data	145
Fig. 170	Arbitrary assignment of the additional data	147
Fig. 171	Configure miscellaneous settings	147
Fig. 172	Activate integration.....	148
Fig. 173	Activated integration.....	148
Fig. 174	Deactivate integration	149
Fig. 175	Recording architectures - main view	150
Fig. 176	Create recording architecture - Multi-Server Recording.....	150
Fig. 177	Recording architecture - tab Details - Multi-Server Recording.....	151
Fig. 178	Select integration type.....	152
Fig. 179	Recording Architecture - tab Server Assignment.....	153
Fig. 180	Recording Architecture - assign server - example	153
Fig. 181	Add Recording Server.....	154
Fig. 182	Recording architecture - activate recording architecture.....	155
Fig. 183	Servers - main view.....	156
Fig. 184	Toolbar Servers module.....	156
Fig. 185	Add server locations.....	157
Fig. 186	Delete server location	158
Fig. 187	Servers - tab Details.....	159
Fig. 188	Servers - tab Usage	159
Fig. 189	Group field API Server	160
Fig. 190	Select storage expansion.....	161
Fig. 191	Group field Audio Analysis	162
Fig. 192	Group field Recording Control/Key Management	162
Fig. 193	Group field Data Processing	163
Fig. 194	Select server	165
Fig. 195	Group field Replay	165
Fig. 196	Select server	167
Fig. 197	Group field Virtualization	167
Fig. 198	Servers module - tab Media Streamer	168
Fig. 199	Servers Module - tab Replay Server Address Mapping	170
Fig. 200	Servers module - tab Key Management.....	171
Fig. 201	Servers module - tab Keystore/Virtualization	172
Fig. 202	Add NTP server.....	173
Fig. 203	Edit IP address.....	174
Fig. 204	Remove NTP server.....	174
Fig. 205	Create new PBX.....	175
Fig. 206	Toolbar PBX module	175
Fig. 207	Create new PBX - tab Details	176
Fig. 208	Tenants - main view - tab Extensions	177
Fig. 209	Assign extensions to tenants	178

Fig. 210 Remove extensions.....	179
Fig. 211 Select extensions	180
Fig. 212 Tenants - main view - tab PBX Agent ID.....	181
Fig. 213 Assign PBX Agent IDs to tenants.....	181
Fig. 214 Select PBX Agent IDs	183
Fig. 215 Additional Data module main view	183
Fig. 216 Configure additional data	184
Fig. 217 Additional data - configure availability	184
Fig. 218 Integrations - main view	185
Fig. 219 Toolbar Integrations module	185
Fig. 220 Choose file	186
Fig. 221 Upload grammar	186
Fig. 222 Create integration type	187
Fig. 223 Integrations - select PBX.....	187
Fig. 224 Assign recording architecture - Multi-Server Recording.....	188
Fig. 225 Configuration steps of the integration	188
Fig. 226 Configuration step - Configure Recording Architecture.....	189
Fig. 227 Configure CTIconnect module	190
Fig. 228 Configure connection data	190
Fig. 229 Configure connection data	191
Fig. 230 Arbitrary assignment of the additional data.....	192
Fig. 231 Configure switching conditions.....	193
Fig. 232 Configure regular expression for phone type identification	194
Fig. 233 Activate CTIconnect module 2	194
Fig. 234 Configure CTIconnect module	195
Fig. 235 Configure connection data	195
Fig. 236 Configure connection	196
Fig. 237 Arbitrary assignment of the additional data.....	197
Fig. 238 Configuration step - configure monitor points	198
Fig. 239 Add extension monitor points.....	198
Fig. 240 Configured extension monitor points.....	200
Fig. 241 Configuration step - Global Recording Settings	201
Fig. 242 Configuration step - Configure recording servers	202
Fig. 243 Tab Extensions	203
Fig. 244 Add extensions.....	204
Fig. 245 Added extensions.....	204
Fig. 246 Configure add-on for MiContact Center Enterprise.....	205
Fig. 247 Arbitrary assignment of the additional data.....	207
Fig. 248 Overview of the add on of Genesys T-Server	208
Fig. 249 Configure add-on for Genesys T-Server	209
Fig. 250 Configure connection data	210
Fig. 251 Arbitrary assignment of the additional data.....	212

Fig. 252	Configure miscellaneous settings	212
Fig. 253	Activate integration.....	213
Fig. 254	Activated integration.....	213
Fig. 255	Deactivate integration	214
Fig. 256	Recording architectures - main view	215
Fig. 257	Create recording architecture - Multi-Server Failover	215
Fig. 258	Recording architecture - tab Details - Multi-Server Failover	216
Fig. 259	Select integration type.....	217
Fig. 260	Recording Architecture - tab Server Assignment	218
Fig. 261	Recording Architecture - assign server - example	219
Fig. 262	Add Recording Server	220
Fig. 263	Recording architecture - activate recording architecture.....	221
Fig. 264	Servers - main view	221
Fig. 265	Toolbar Servers module	222
Fig. 266	Add server locations.....	223
Fig. 267	Delete server location	224
Fig. 268	Servers - tab Details.....	224
Fig. 269	Servers - tab Usage	225
Fig. 270	Group field API Server	225
Fig. 271	Select storage expansion.....	227
Fig. 272	Group field Audio Analysis	227
Fig. 273	Group field Recording Control/Key Management	228
Fig. 274	Group field Data Processing	229
Fig. 275	Select server	231
Fig. 276	Group field Replay	231
Fig. 277	Select server	233
Fig. 278	Group field Virtualization	233
Fig. 279	Servers module - tab Media Streamer	234
Fig. 280	Servers Module - tab Replay Server Address Mapping	236
Fig. 281	Servers module - tab Key Management.....	237
Fig. 282	Servers module - tab Keystore/Virtualization	238
Fig. 283	Add NTP server.....	239
Fig. 284	Edit IP address.....	240
Fig. 285	Remove NTP server.....	240
Fig. 286	Create new PBX.....	241
Fig. 287	Toolbar PBX module	241
Fig. 288	Create new PBX - tab Details	242
Fig. 289	Tenants - main view - tab Extensions	243
Fig. 290	Assign extensions to tenants	244
Fig. 291	Remove extensions.....	245
Fig. 292	Select extensions	246
Fig. 293	Tenants - main view - tab PBX Agent ID.....	247

Fig. 294	Assign PBX Agent IDs to tenants.....	247
Fig. 295	Select PBX Agent IDs	249
Fig. 296	Additional Data module main view	249
Fig. 297	Configure additional data	250
Fig. 298	Additional data - configure availability	250
Fig. 299	Integrations - main view	251
Fig. 300	Toolbar Integrations module	251
Fig. 301	Choose file	252
Fig. 302	Upload grammar	252
Fig. 303	Create integration type	253
Fig. 304	Integrations - select PBX.....	253
Fig. 305	Assign recording architecture - Multi-Server Failover	254
Fig. 306	Configuration steps of the integration	254
Fig. 307	Configuration step - Configure Recording Architecture.....	255
Fig. 308	Configure CTIconnect module	255
Fig. 309	Configure connection data	256
Fig. 310	Configure connection data	256
Fig. 311	Arbitrary assignment of the additional data	257
Fig. 312	Configure switching conditions.....	258
Fig. 313	Configure regular expression for phone type identification	259
Fig. 314	Activate CTIconnect module 2	260
Fig. 315	Configure CTIconnect module	260
Fig. 316	Configure connection data	261
Fig. 317	Configure connection	261
Fig. 318	Arbitrary assignment of the additional data	262
Fig. 319	Configuration step - configure monitor points	263
Fig. 320	Add extension monitor points.....	264
Fig. 321	Configured extension monitor points.....	265
Fig. 322	Configuration step - Global Recording Settings	266
Fig. 323	Configuration step - Configure recording servers	268
Fig. 324	Tab Extensions	269
Fig. 325	Add extensions.....	269
Fig. 326	Added extensions.....	270
Fig. 327	Configure add-on for MiContact Center Enterprise	271
Fig. 328	Arbitrary assignment of the additional data	272
Fig. 329	Overview of the add on of Genesys T-Server	274
Fig. 330	Configure add-on for Genesys T-Server	275
Fig. 331	Configure connection data	276
Fig. 332	Arbitrary assignment of the additional data	278
Fig. 333	Configure miscellaneous settings	278
Fig. 334	Activate integration.....	279
Fig. 335	Activated integration.....	279

Fig. 336 Deactivate integration	280
Fig. 337 Synchronize recording control.....	281
Fig. 338 Menu item Manage synchronization configuration	282
Fig. 339 Configure synchronization configurations	282
Fig. 340 Create synchronization configuration.....	283
Fig. 341 Configure standby management.....	284
Fig. 342 Switch server.....	285
Fig. 343 Menu of the standby management.....	286
Fig. 344 Switch server.....	286
Fig. 345 Servers - tab Usage	289
Fig. 346 Group field Recording Control/Key Management	290
Fig. 347 PHONEapp - main view:	290
Fig. 348 Detail view phone types	291
Fig. 349 Display of the properties	292
Fig. 350 Detail view Default settings.....	293
Fig. 351 Group field Tagging Attributes	295
Fig. 352 Edit tagging attributes	295
Fig. 353 Group field Register Fields.....	296
Fig. 354 Edit register fields.....	296
Fig. 355 Configure tagging fields	297
Fig. 356 Edit tagging fields.....	297
Fig. 357 Activate PHONEapp configuration	299
Fig. 358 Phones - main view	299
Fig. 359 Create phones Select phone type.....	300
Fig. 360 Main view	302
Fig. 361 Tab Details (example).....	302
Fig. 362 Add PBX	304
Fig. 363 Add tenant.....	304
Fig. 364 Tab Drives - WAVE formats	305
Fig. 365 Add drive	305
Fig. 366 Tab Mapping for WAVE import format	306
Fig. 367 Group field Data Structure	306
Fig. 368 Group field Start Time - import format WAV + CSV	307
Fig. 369 Group field Start Time - import format WAV + XML	308
Fig. 370 Group field Participant phone number (example)	308
Fig. 371 Edit source for participant phone number (example)	309
Fig. 372 Edit source for additional data (example for WAVE import format).....	310
Fig. 373 POWERplay Web - Recording View	311
Fig. 374 Recording View - tab Additional Data	311
Fig. 375 Genesys Administrator - select T-Server	312
Fig. 376 Genesys Administrator - configure T-Server.....	312
Fig. 377 Genesys Administrator - select configuration server.....	313

Fig. 378 Genesys Administrator - configure configuration server	313
Fig. 379 Genesys Administrator - switch instances	314
Fig. 380 Genesys Administrator - configure switch instance	314
Fig. 381 Genesys administrator - create user	315

List of tables

Tab. 1	Licenses for recording server	10
Tab. 2	Licenses for the phone application (optional).....	10
Tab. 3	Licenses	10
Tab. 4	Licenses	10
Tab. 5	Licenses for MiContact Center Enterprise optional	10
Tab. 6	Licenses for Genesys.....	10
Tab. 7	Login data - system provider	22
Tab. 8	Configure audio analysis.....	35
Tab. 9	Configure Recording Control/Key Management	35
Tab. 10	Configure data storage.....	36
Tab. 11	Configure replay.....	38
Tab. 12	Configure virtualization.....	40
Tab. 13	Create PBX	49
Tab. 14	Create integration type	60
Tab. 15	Configure CTIconnect module	63
Tab. 16	Configure connection data	63
Tab. 17	Configure CTIconnect module	67
Tab. 18	Configure connection data	68
Tab. 19	Global recording settings	73
Tab. 20	Configure CTIconnect module	75
Tab. 21	Configure connection data	76
Tab. 22	Configure add-on for Genesys T-Server	79
Tab. 23	Configure connection data	80
Tab. 24	Configure audio analysis.....	96
Tab. 25	Configure Recording Control/Key Management	97
Tab. 26	Configure data storage.....	98
Tab. 27	Configure replay.....	100
Tab. 28	Configure virtualization.....	102
Tab. 29	Create PBX	111
Tab. 30	Create integration type	122
Tab. 31	Configure CTIconnect module	124
Tab. 32	Configure connection data	125
Tab. 33	Configure CTIconnect module	129
Tab. 34	Configure connection data	130
Tab. 35	Global recording settings	135
Tab. 36	Configure recording servers.....	137
Tab. 37	Configure CTIconnect module	140
Tab. 38	Configure connection data	141
Tab. 39	Configure add-on for Genesys T-Server	144
Tab. 40	Configure connection data	145
Tab. 41	Configure audio analysis.....	162

Tab. 42	Configure Recording Control/Key Management	162
Tab. 43	Configure data storage.....	163
Tab. 44	Configure replay.....	165
Tab. 45	Configure virtualization.....	167
Tab. 46	Create PBX	176
Tab. 47	Create integration type.....	187
Tab. 48	Configure CTIconnect module	190
Tab. 49	Configure connection data	191
Tab. 50	Configure CTIconnect module	195
Tab. 51	Configure connection data	196
Tab. 52	Global recording settings	201
Tab. 53	Configure recording servers.....	202
Tab. 54	Configure CTIconnect module	206
Tab. 55	Configure connection data	206
Tab. 56	Configure add-on for Genesys T-Server	209
Tab. 57	Configure connection data	210
Tab. 58	Configure audio analysis.....	227
Tab. 59	Configure Recording Control/Key Management	228
Tab. 60	Configure data storage.....	229
Tab. 61	Configure replay.....	231
Tab. 62	Configure virtualization.....	233
Tab. 63	Create PBX	242
Tab. 64	Create integration type.....	253
Tab. 65	Configure CTIconnect module	256
Tab. 66	Configure connection data	256
Tab. 67	Configure CTIconnect module	260
Tab. 68	Configure connection data	261
Tab. 69	Global recording settings	266
Tab. 70	Configure recording servers.....	268
Tab. 71	Configure CTIconnect module	271
Tab. 72	Configure connection data	272
Tab. 73	Configure add-on for Genesys T-Server	275
Tab. 74	Configure connection data	276
Tab. 75	Available parameters	288
Tab. 76	Configure Recording Control/Key Management	290
Tab. 77	Mapping rules for participant phone numbers.....	309
Tab. 78	Buttons	309

Glossary

μ-law

PCM digitization method for analog audio signals according to ITU G.711. In the process, analog voice signals are converted into digital signals by means of a logarithmic quantization characteristic. The μ-law algorithm is used in the US while the A-law algorithm is the standard in Europe.

A-law

PCM digitization method for analog audio signals according to ITU G.711. In the process, analog voice signals are converted into digital signals by means of a logarithmic quantization characteristic. The A-law algorithm is used in Europe while the μ-law algorithm is the standard in the US.

API

Application Programming Interface

API server

Server on which the API service runs. (API=Application Programming Interface)

Codec

Code/Decode implementation of a method for transforming from coded/decoded data to de-coded or coded data

CSTA

Computer Supported Telecommunications Applications (CSTA) Standard which defines how data is transferred between PBX and all external computer programs connected to the device.

CSV

Comma-separated values is a file format which stores tabular data in plain text form.

CTI

Computer Telephony Integration

IP

Internet Protocol, basic protocol for Internet communication

LCR

Last Conversation Repeat

MBG

Mitel Border Gateway

NTP

Network Time Protocol NTP is a standard for the synchronization of clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP. It has been developed with the objective to guarantee reliable time verification across networks with variable packet runtime. (Source: Wikipedia 12th June 2018)

PBX

Private Branch Exchange

PCM

Pulse Code Modulation is an uncompressed pulse modulation method which transforms a time- and value-continuous analog signal into a time- and value-discrete digital signal. It is used in audio technology, for example in the context of the G.711 standard and in video technology for digital video signals in compliance with the ITU-R BT 601 standard. (Source: Wikipedia 12th June 2018)

RTP

Real-time Transport Protocol is a protocol to continuously transmit audio and video files via the IP protocol within the network.

SIP

Session Initiation Protocol

SRC

Secure Recording Connector, the recording session is delivered to the recording server via the Secure Recording Connector.

SSL

Secure Socket Layer

TCP

Transmission Control Protocol, controlled connection establishment, secure data transmission, controlled connection termination

TDM

Time Division Multiplexing is an umbrella term for time-slot-oriented interfaces, ITU G.703 defined. The term is used ASC-wide representative for conventional telephony.

TLS

Transport Layer Security; 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)

VM

Virtual machine

VoIP

Voice over IP

WAVE

The WAVE file format is a container format to digitally save audio files. It is based on the Resource Interchange File Format (RIFF) which is defined by Microsoft for Windows. A WAVE file already contains information about the format of the audio data before the audio data are actually stored.

XML

Extensible Markup Language is a human-readable and machine-readable language which defines a set of rules for encoding documents.