

# EVOIPneo active for Mitel MiVoice MX-ONE (CSTA3)



## Administration manual for system providers

11/8/2021

### Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

EVOflex (country-specific)

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

Copyright © 2021 ASC Technologies AG. All rights reserved.

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



## Contents

<b>1</b>	<b>General information .....</b>	<b>5</b>
<b>2</b>	<b>Introduction .....</b>	<b>6</b>
<b>3</b>	<b>System requirements.....</b>	<b>9</b>
3.1	Hardware components .....	9
3.1.1	Recorder .....	9
3.2	Software components .....	9
3.3	Mitel system components.....	9
3.4	Genesys system components (optional) .....	9
3.4.1	Genesys Framework .....	9
<b>4</b>	<b>Installation requirements .....</b>	<b>10</b>
4.1	Licenses .....	10
4.2	Information .....	11
<b>5</b>	<b>Overview install and configure product.....</b>	<b>12</b>
<b>6</b>	<b>Installation .....</b>	<b>13</b>
<b>7</b>	<b>Configuration.....</b>	<b>14</b>
7.1	Configure Mitel MiVoice MX-ONE CSTA 3 .....	14
7.1.1	Configure CSTA server .....	14
7.1.2	Configure extension monitor points.....	16
7.1.3	Check functionality .....	17
7.2	Configure MiVoice Border Gateway.....	20
7.2.1	Configure MiVoice Border Gateway for SRC .....	20
7.2.2	Confirm certificate on MBG .....	23
7.3	System Configuration.....	25
7.3.1	Start application .....	25
7.3.2	Configure recording solution Mitel MX-ONE CSTA.....	27
7.3.2.1	Configure recording solution All-in-one Basic .....	27
7.3.2.2	Configure recording solution All-in-one Failover .....	90
7.3.2.3	Configure recording solution All-in-one Parallel Recording.....	159
7.3.2.4	Configure recording solution Multi-Server Recording .....	224
7.3.2.5	Configure recording solution Multi-Server Failover .....	289
7.3.2.6	Configure recording solution Multi-Server Parallel Recording .....	356
7.3.3	Configure Recording Content Validation .....	421
7.3.4	Configure PHONEapp for Mitel .....	424
7.3.4.1	Configure Servers module .....	424
7.3.4.2	Configure PHONEapp module .....	426
7.3.4.3	Configure PBX module.....	434
7.3.4.4	Configure Phones module.....	435
7.3.4.5	Configure Recording Planner module .....	438

7.3.4.6	Configure key functions on the Mitel phone .....	439
7.3.5	Synchronization options .....	441
7.3.5.1	Synchronization of recording control .....	442
7.3.5.2	Synchronization of system storage .....	443
7.3.6	Duplicates in parallel recording architectures .....	445
7.3.6.1	Configure duplicate detection.....	446
7.3.6.2	Additional data .....	448
7.3.6.3	Criteria to be ignored.....	449
7.3.7	Standby management for failover architectures.....	450
7.3.7.1	Standby management for All-in-one Failover.....	450
7.3.7.2	Standby management for Multi-Server Failover.....	452
7.3.8	Software update .....	453
7.3.9	Import InAttend conversation to neo .....	454
7.3.9.1	Configure import job .....	454
7.3.9.2	Replaying conversations in POWERplay Web.....	464
7.4	Configure CTIconnect add-on .....	465
7.4.1	Configure Genesys T-Server (optional) .....	465
7.4.1.1	Configure IP address and port of the Genesys T-Server .....	465
7.4.1.2	Configure IP address and port of the Genesys Configuration Server .....	466
7.4.1.3	Configure switch instance in the Genesys Configuration Server .....	467
7.4.1.4	Create users for the Genesys Configuration Server .....	468
<b>8</b>	<b>Troubleshooting.....</b>	<b>469</b>
	<b>List of figures .....</b>	<b>470</b>
	<b>List of tables .....</b>	<b>484</b>
	<b>Glossary .....</b>	<b>487</b>



## General information

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

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

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

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

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

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

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

## 2 Introduction

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



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

The recording solution EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA 3) provides the functionality which is necessary for the 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<sub>neo</sub> Recording Service records the corresponding conversation data and saves them on the recording server.

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

By adding MiContact Center Enterprise, the agents' additional data may be provided in addition to the conversation data.

### Recording solution with Mitel VoIP end devices without MBG (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.

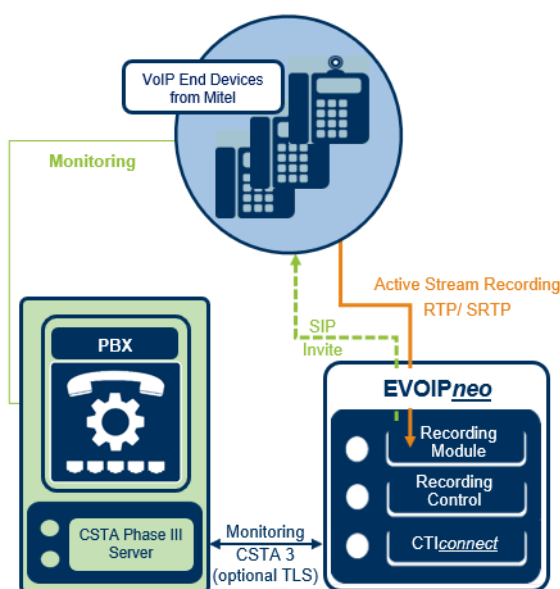


Fig. 1: Recording solution with VoIP end devices without MBG

### Recording solution via Mitel Border Gateway (MBG)

To record softphones and remote end devices (teleworking stations), an additional communication between the recording server and the Mitel Border Gateway (MBG) is required. 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 on the [SRC](#).

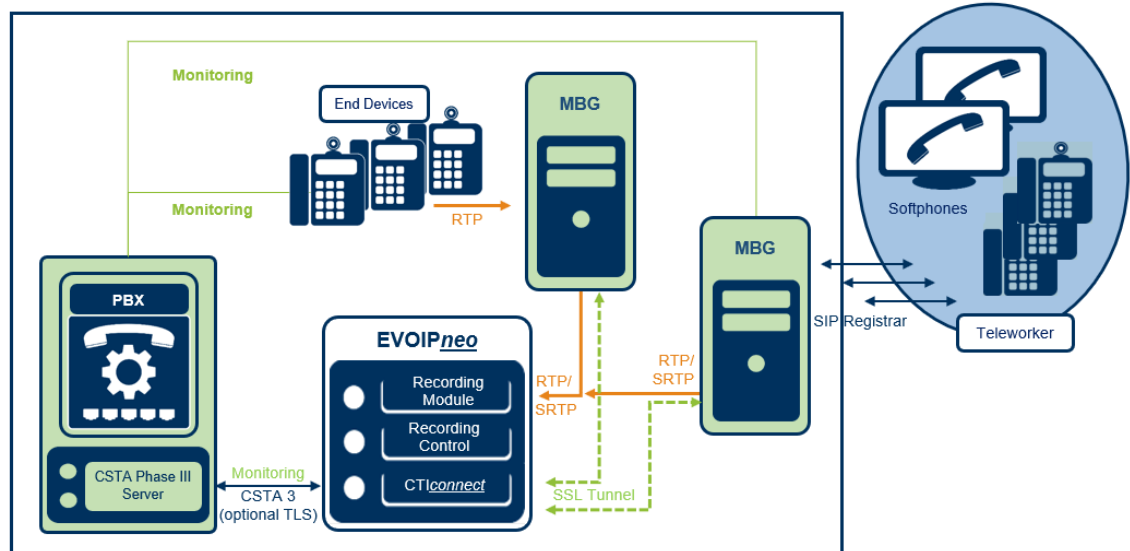


Fig. 2: Recording solution with MBG

### Recording solution with intrusion

For *neo* version 5.3 or higher, the recording solution offers the feature Intrusion which records the recording server by means of silent call intrusion. This allows recording **VoIP** and **TDM** end devices. 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 on the PBX with the configured recording server extension via the **CSTA** connection. Therefore, an extension for the recording server must be available for each concurrent recording.

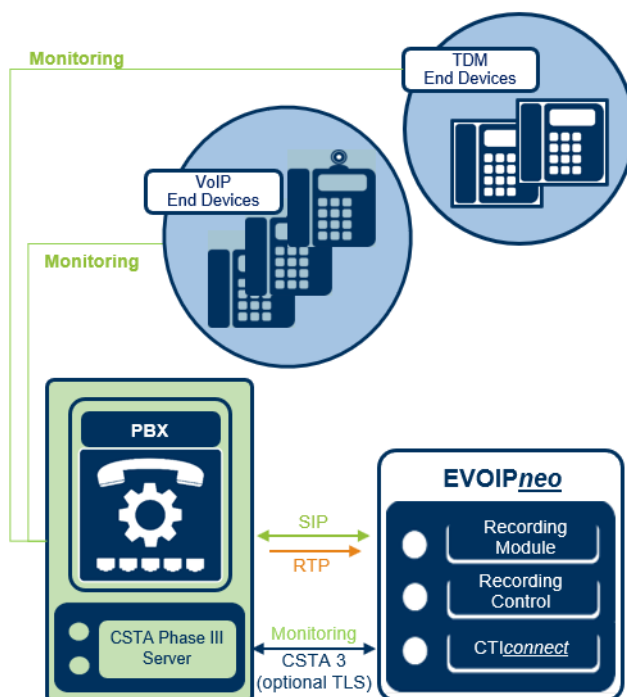


Fig. 3: Recording solution with intrusion



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.



For the description of the passive trunk-side recording solution refer to the separate administration manual for system providers EVOIPneo passive for Mitel MiVoice MX-ONE trunk-side recording.

### 3 System requirements



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



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



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

#### 3.1 Hardware components



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



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

##### 3.1.1 Recorder

For the recording solution you can use the following systems:

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



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

#### 3.2 Software components

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

#### 3.3 Mitel system components



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



MiCollab Softphones can be recorded by means of the MBG like any other SIP client.

#### 3.4 Genesys system components (optional)

##### 3.4.1 Genesys Framework

When using a CTI<sub>connect</sub> 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 <sub>neo</sub> Base license - active	1 license per recording server
EVOIP <sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA 3)	1 license per concurrent recording

Tab. 1: Licenses for recording server

License name	Number
PHONE <sub>app</sub> for Mitel MiVoice Business, MiVoice 5000 and MX-ONE per system	1 license per recording system
PHONE <sub>app</sub> for Mitel MiVoice Business, MiVoice 5000 and MX-ONE per phone	1 license per end device

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

#### MiVoice 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
CTIconnect for Genesys T-Server	1 per recording system
Genesys Recording Connector	1 per monitored recording resource
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 CTIconnect module.

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

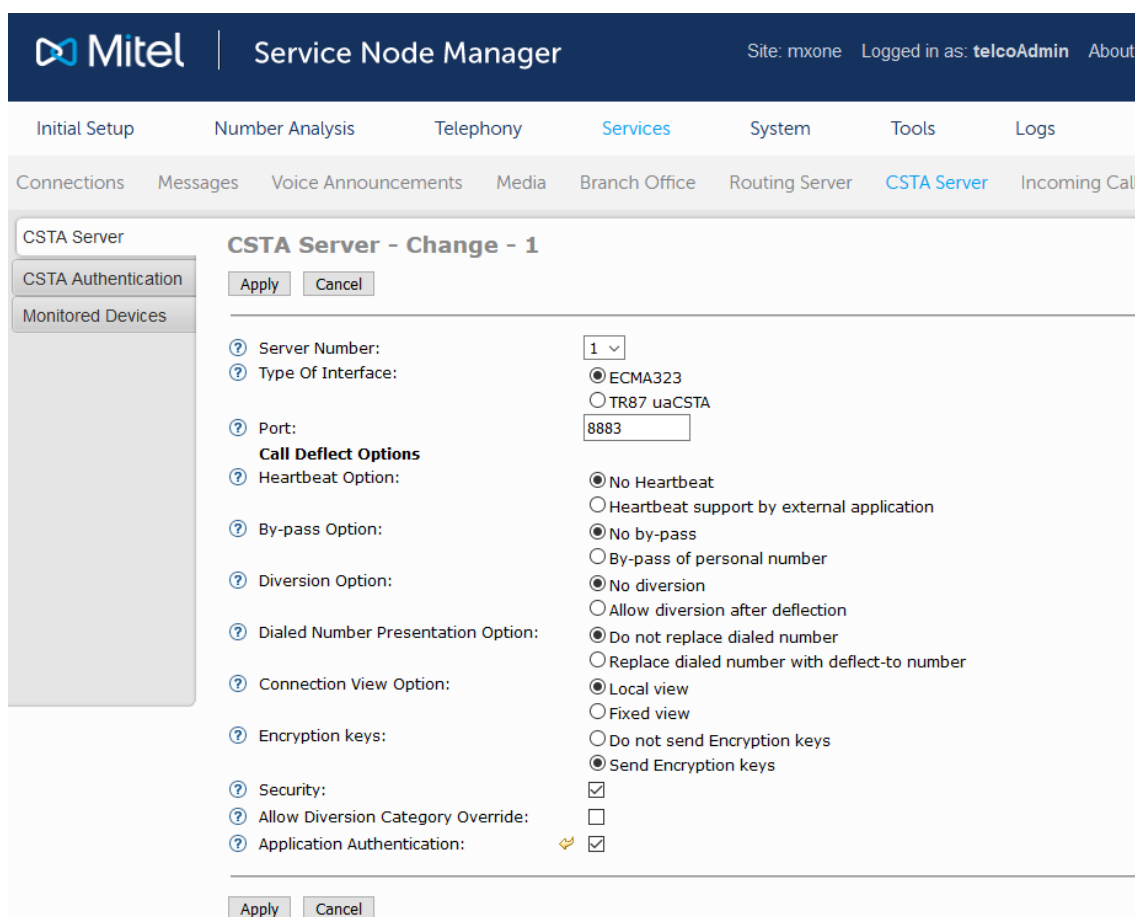
## 7.1 Configure Mitel MiVoice MX-ONE CSTA 3



A Mitel engineer configures the Mitel MiVoice MX-ONE PBX. The IP address of the recording server must be entered in the configuration file of the PBX 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 menu item *Services*.
6. Below, select the menu item *CSTA Server* in the menu bar.
7. Select the menu item *CSTA Server* in the navigation bar.



**Mitel | Service Node Manager** Site: mxone Logged in as: telcoAdmin About

Initial Setup Number Analysis Telephony **Services** System Tools Logs

Connections Messages Voice Announcements Media Branch Office Routing Server **CSTA Server** Incoming Call

**CSTA Server**

**CSTA Authentication**

**Monitored Devices**

**CSTA Server - Change - 1** [Apply] [Cancel]

Server Number: 1

Type Of Interface: ☒ ECMA323 ☐ TR87 uaCSTA

Port: 8883

**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: ☐

Application Authentication: ☒

[Apply] [Cancel]

Fig. 4: Configure CSTA server

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

Type of Interface	ECMA323
-------------------	---------

<i>Port</i>	Enter the port you would like to use for the communication, for TCP 8882, for TLS 8883.
<i>Heartbeat Option</i>	<i>Heartbeat support by external application</i> Not obligatory but recommended.
<i>By-pass Option</i>	<i>No by-pass</i>
<i>Diversion Option</i>	<i>No diversion</i>
<i>Dialed Number Presentation Option</i>	<i>Do not replace dialed number</i>
<i>Connection View Option</i>	<i>Local view</i>
<i>Encryption keys</i>	<i>Send Encryption keys</i>
<i>Security</i>	<p>Activate this option if the connection via TLS is supposed to be used. Unencrypted by default.</p> <p><b>NOTICE!</b> 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>
<i>Application Authentication</i>	<p>Activate this option to use authentication for this application.</p> <p><b>NOTICE!</b> If you would like to use authentication, you must activate it here and in the <u>neo</u> application System Configuration in the CTI connection data.</p>

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



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

11. In the navigation bar, select the menu item *CSTA Authentication*.

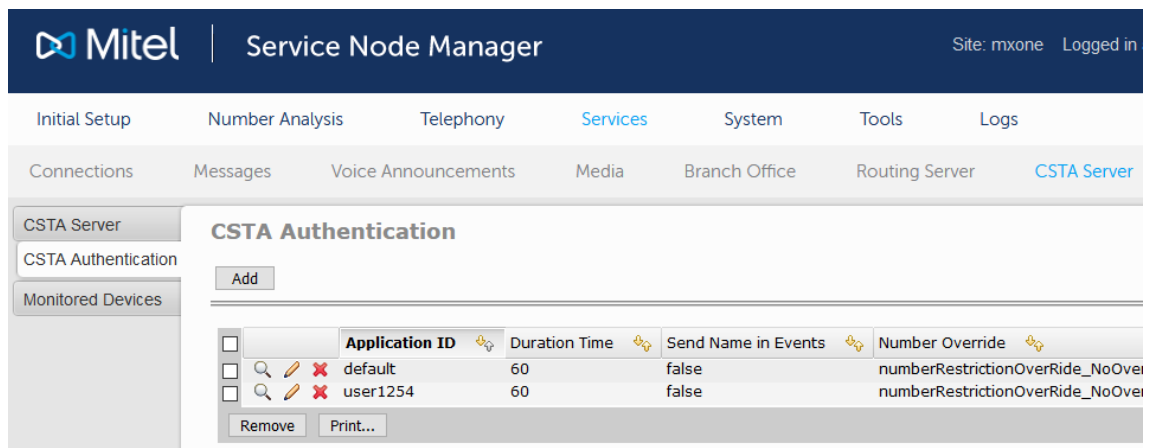
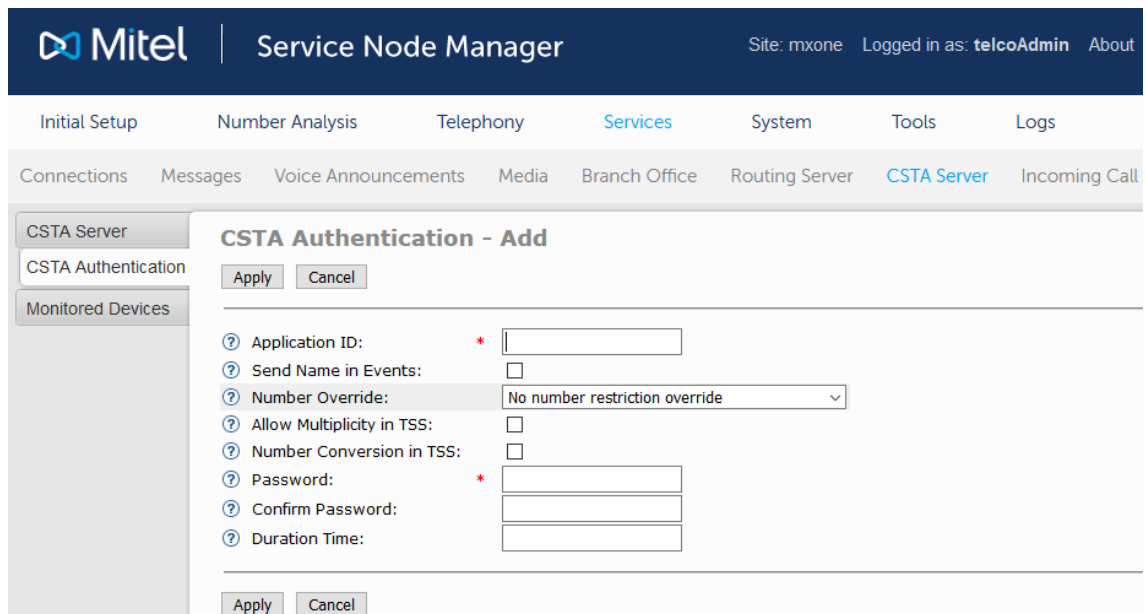


Fig. 5: Configure CSTA server

12. Click on the button *Add* to configure a new authentication.



The screenshot shows the Mitel Service Node Manager interface. The top navigation bar includes 'Initial Setup', 'Number Analysis', 'Telephony', 'Services' (highlighted), 'System', 'Tools', and 'Logs'. Below this, a secondary navigation bar lists 'Connections', 'Messages', 'Voice Announcements', 'Media', 'Branch Office', 'Routing Server', 'CSTA Server' (highlighted), and 'Incoming Call'. On the left, a sidebar menu shows 'CSTA Server', 'CSTA Authentication' (selected), and 'Monitored Devices'. The main content area is titled 'CSTA Authentication - Add' and contains the following fields:

- Application ID:  (required, indicated by a red asterisk)
- Send Name in Events: ☐
- Number Override:  (dropdown menu)
- Allow Multiplicity in TSS: ☐
- Number Conversion in TSS: ☐
- Password:  (required, indicated by a red asterisk)
- Confirm Password:
- Duration Time:

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

Fig. 6: Configure CSTA server


13. Enter an application ID.
14. Enter a password for this application ID.
15. Click on the button *Apply* to save the entries.

### 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).


Provisioning Manager

Users
Services
System
Logs
Own Settings

Extension
Individual Diversion

### Extension Number - Change - MX-ONE, version 7.3

<

**General**

? MiVoice MX-ONE:

? Extension Number:

? Description:

? Server Number:

? Extension Type:

? Customer:

? Common Service Profile:

? Phone Language:

? Backup Answering Position Number:

? Allow Security Exception:

? EDN Extension:

? Boss/Secretary:

? Home Area Code:

? Protocol:

? Free on Second Line:

MX-ONE

22001

1

IP

None ▾

0 - CSP0 (None) ▾

Default ▾

☒

NO

None ▾

☒ SIP

☐ IP

No, can not be changed via terminal menu ▾

**Name Identity**

? First Name:

? Last Name:

**Authorization Code**

Fig. 7: 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.

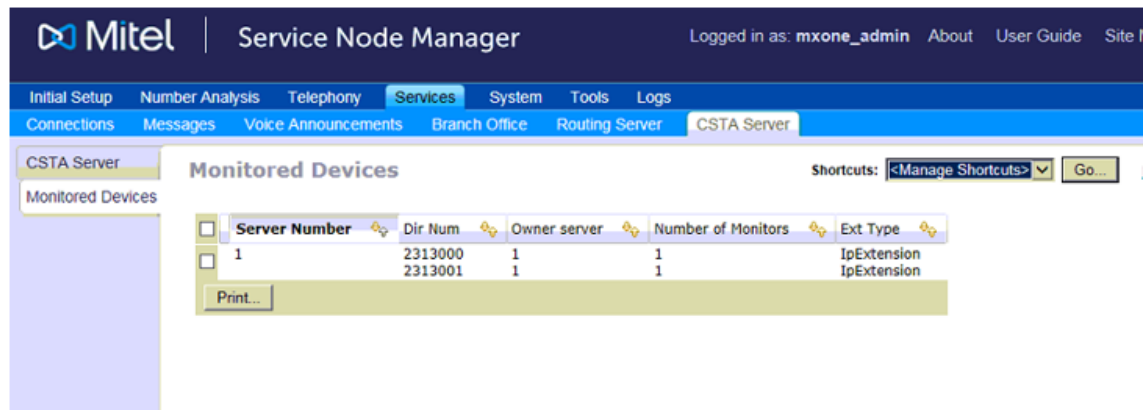


Fig. 8: Check set monitor points

### 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.

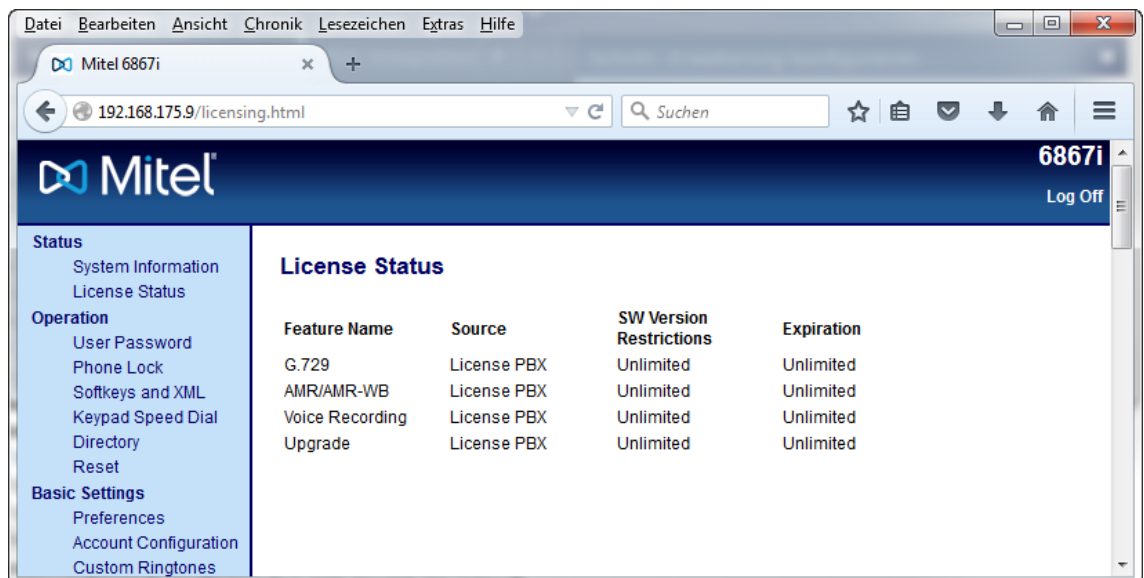


Fig. 9: Check license status

### 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.

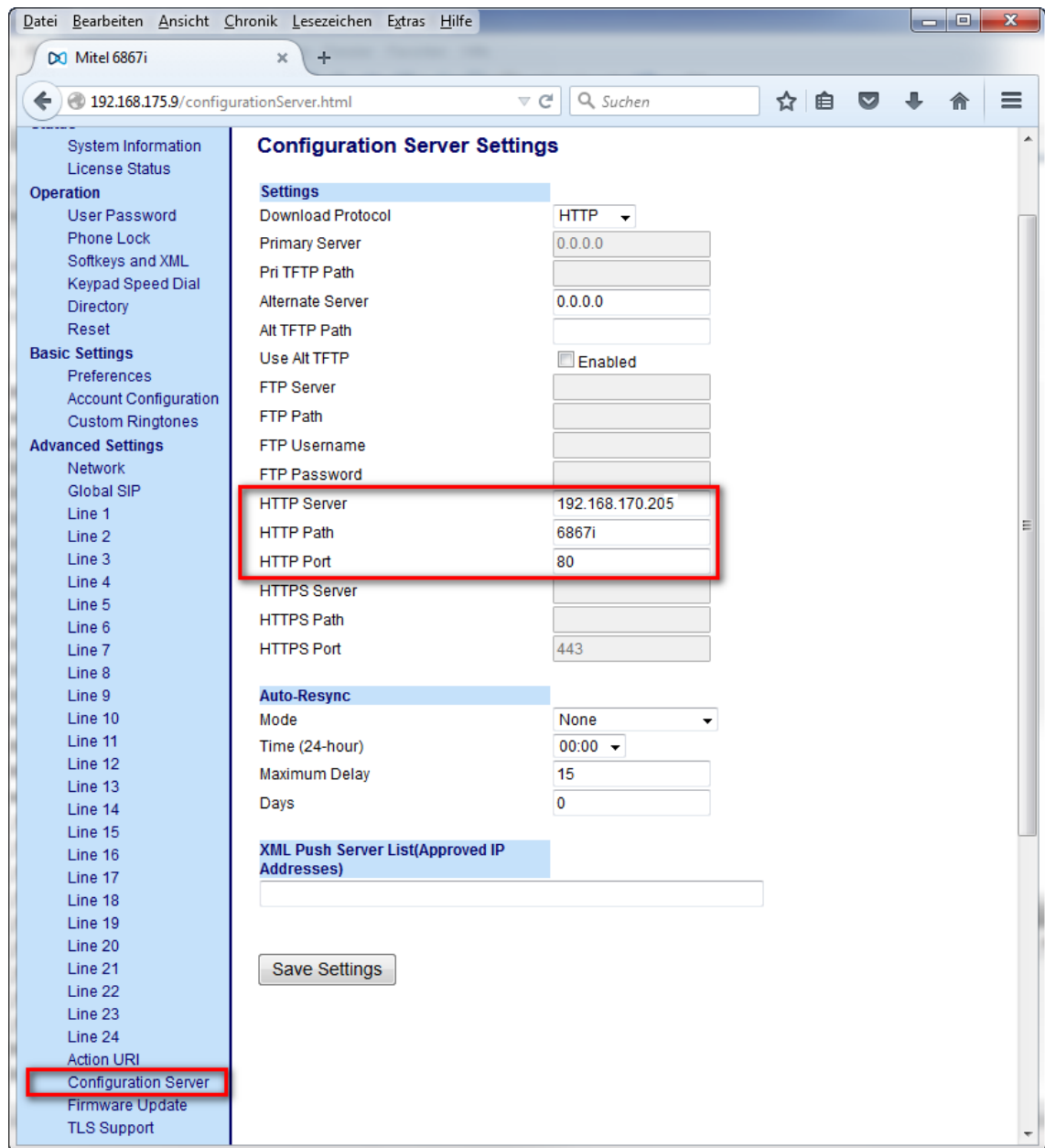


Fig. 10: Check server, path and port

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. 11: Check IP address and transport protocol

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

<i>recorder address1</i>	Enter the IP address of the recording server, e. g. <i>192.168.169.143</i> .
<i>sip services transport protocol:</i>	Enter the respective value for the deployed transport protocol: <i>UDP = 1</i> <i>TCP = 2</i>  The configuration must coincide with the <a href="#">SIP</a> 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 MiVoice Border Gateway

### 7.2.1 Configure MiVoice Border Gateway for SRC

- Log in to the web interface of the Mitel platform for administration purposes.
- In the navigation bar, select the menu item *Application > MiVoice Border Gateway > Service configuration > Application integration*.
- In the group field *Call recording*, activate the check box *Enabled*.



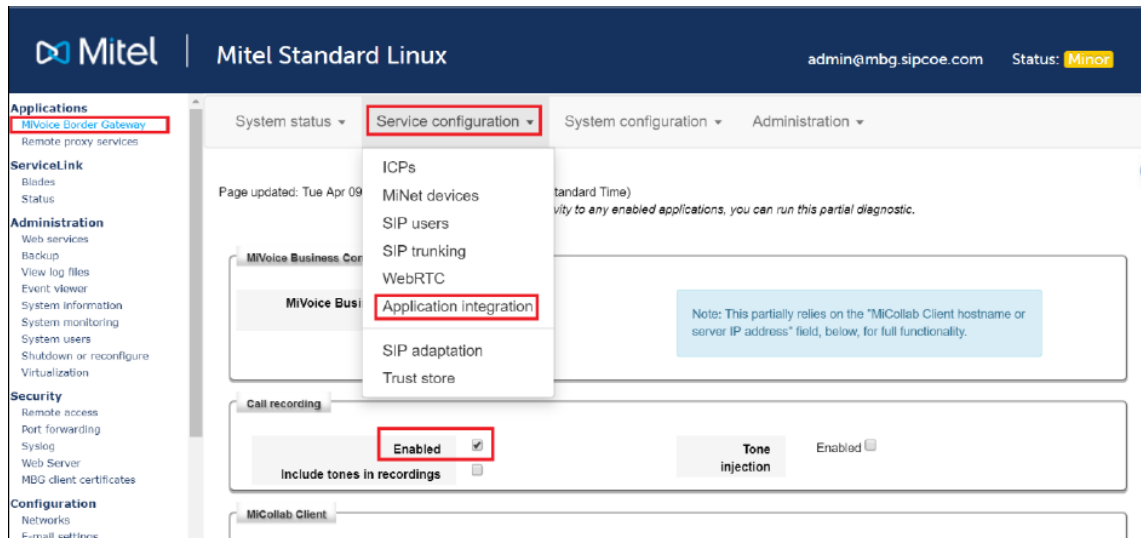


Fig. 12: Activate MBG for Call Recording

For more information about implementing MBGs in VMware environments refer to the following Mitel documents. All documents are available online at Mitel's website and in the info channel.

- Virtual Appliance Deployment Solutions Guide

#### Configure MiVoice Business 9.0 SP3 and 8.0 SP3 PR3 for ASC neo Call Recorder

- VMware Virtual Appliance Quick Reference Guide

#### Add MiVoice Business as an ICP

1. Log in to the MBG and click on MiVoice Border Gateway.
2. In the navigation bar, select the menu item *Applications > MiVoice Border Gateway > Service configuration > ICPs*.

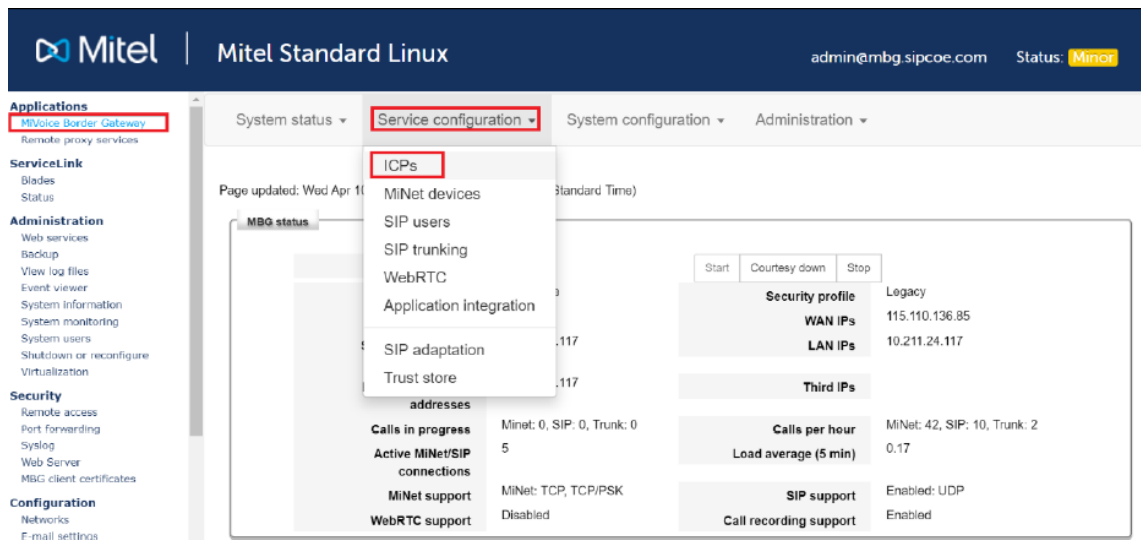


Fig. 13: Add MBG ICPs

3. Add a new ICP with the following parameters:

Name	Enter a respective name.
Hostname or IP address	Enter the IP address of the MiVB.
Type	From the drop-down list, select <i>MiVoice Business</i> .

<i>SIP Capabilities</i>	From the drop-down list, select the entry <i>TCP, UDP, TLS</i> .
<i>Indirect call recording capable</i>	If you use Indirect Call Recording mode, tick the check box.

Tab. 7: Parameters for the ICP

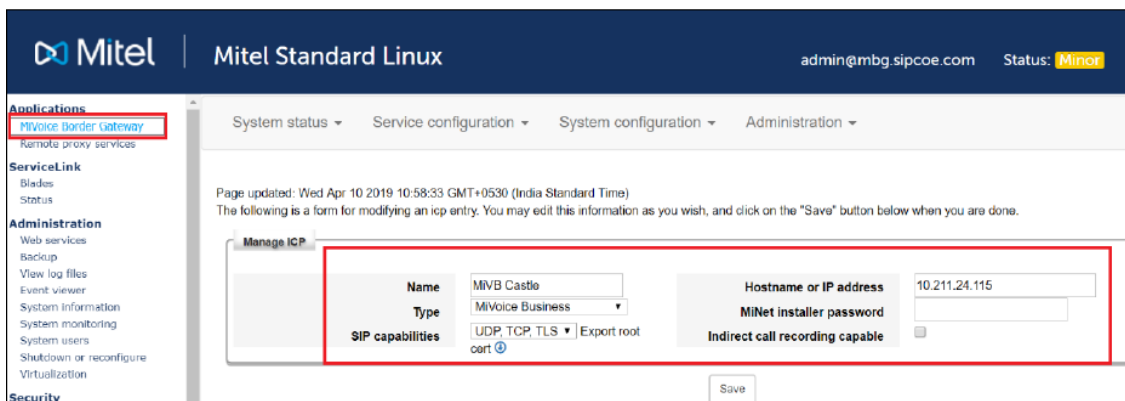


Fig. 14: Configure MBG ICP

### Add Mitel MiNET devices

For each extension which is supposed to be imported, you must add a Mitel MiNET device.

1. Log in to the web interface of the MBG web Admin.
2. In the navigation bar, select the menu item *Applications > MiVoice Border Gateway > Service Configuration*.
3. Add a new device and enter the following parameters:

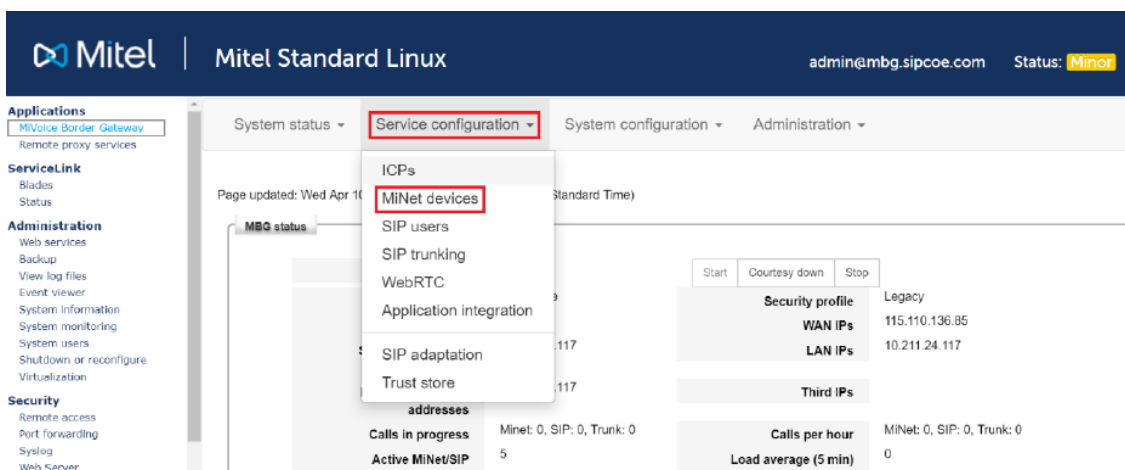


Fig. 15: Add MiNET devices

<i>Enabled</i>	Tick the check box to activate the device.
<i>Configured ICP</i>	Select the previously added ICP for the MiVB.
<i>MAC Address</i>	Enter the IP address of the device which is supposed to be recorded.
<i>Description</i>	Enter a descriptive name.

Tab. 8: Parameters for MiNET device

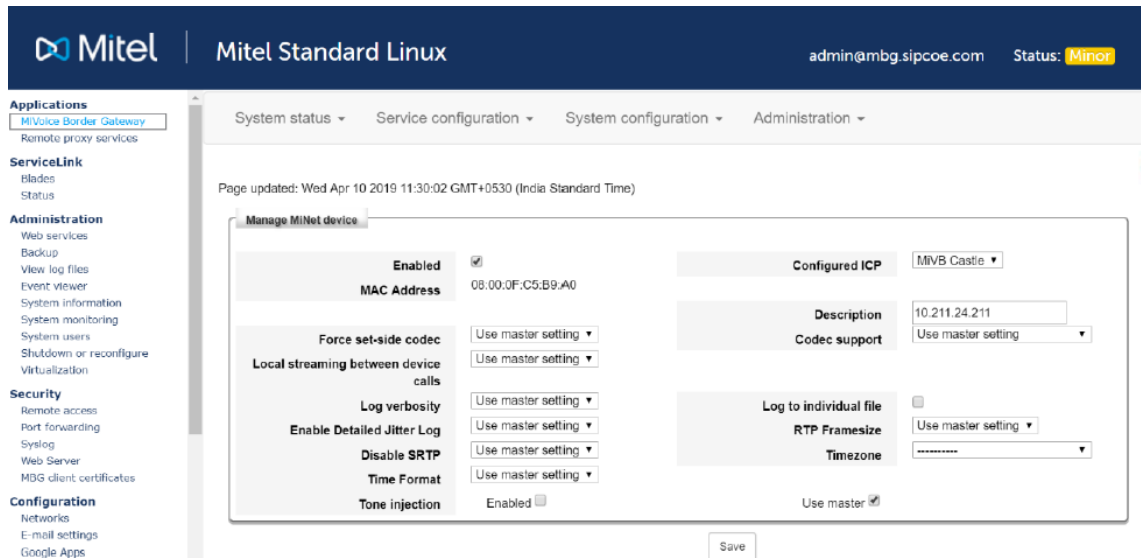


Fig. 16: Add MiNET devices

You can add several devices for recording via the MBG. To facilitate this process, you can switch off the function *Restrict MiNET Device* in the MBG user interface.

This allows several devices to register at the default ICP. The ICP forwards the information to the respective PBX. For more details refer to the MiVoice Border Gateway installation and maintenance manual.



If the default ICP is unavailable while the devices try to establish a connection, the devices cannot be used.

### 7.2.2

#### Confirm certificate on MBG

To be able to establish an [SSL](#) connection to the MiVoice Border Gateway ([MBG](#)), the security certificate on the [MBG](#) must be confirmed.



If you use a pre-shared key, you do not have to confirm the security certificate.

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

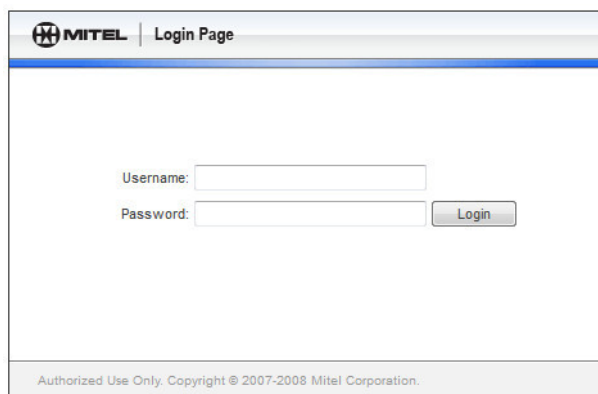
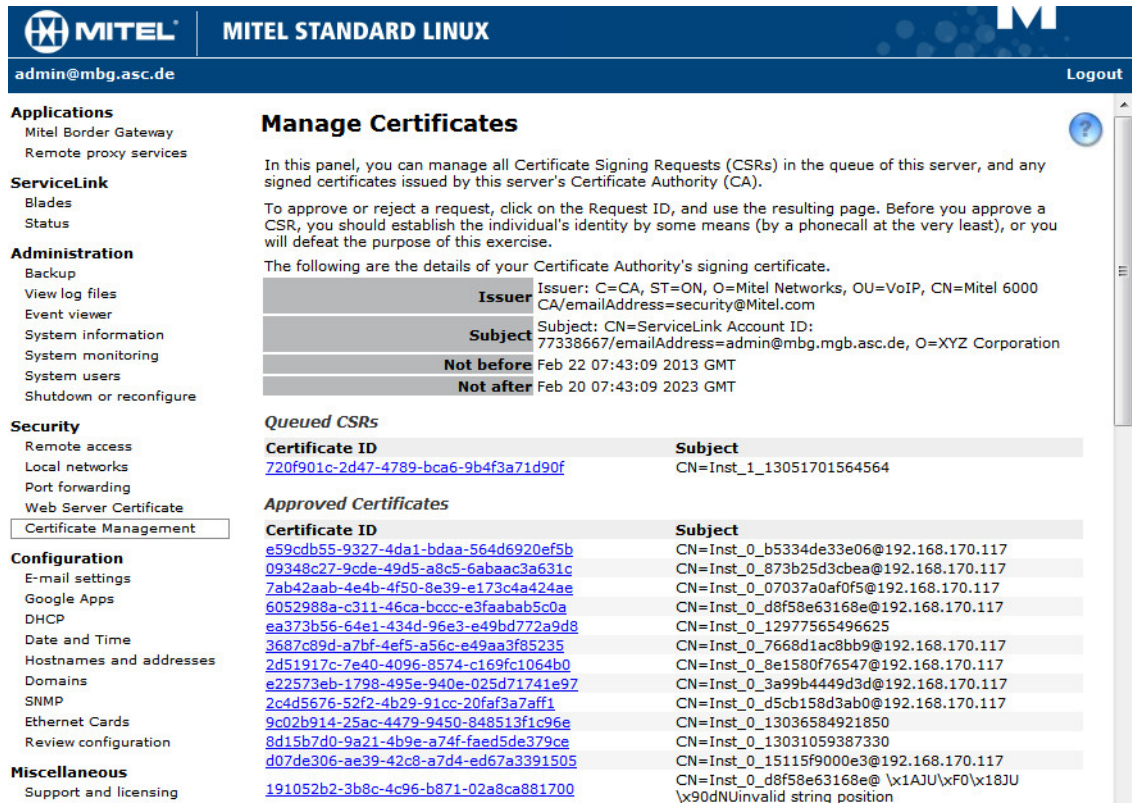


Fig. 17: Login screen MBG

2. Log in to the web interface. The access data for the MiVoice Border Gateway are provided by the Mitel technician.

⇒ The following window appears:



**MITEL STANDARD LINUX**

admin@mbg.asc.de Logout

**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

**Miscellaneous**  
 Support and licensing

### 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.

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

#### Queued CSRs

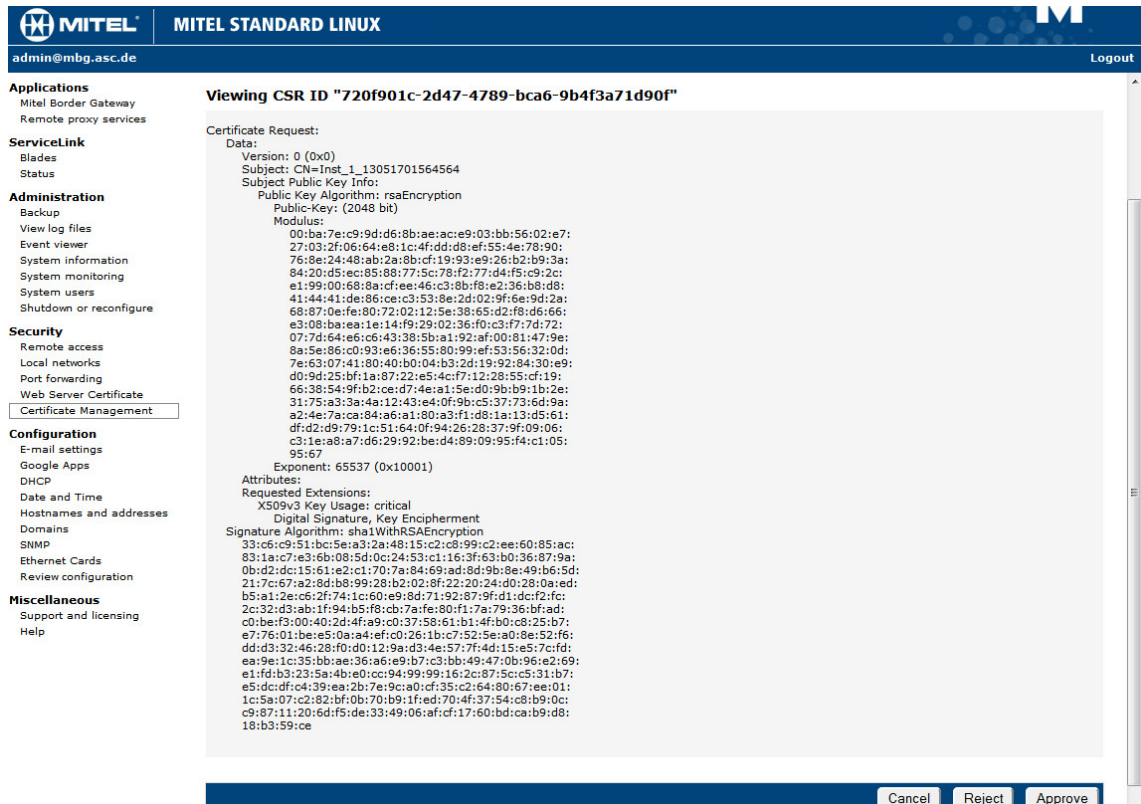
Certificate ID	Subject
<a href="#">720f901c-2d47-4789-bca6-9b4f3a71d90f</a>	CN=Inst_1_13051701564564

#### Approved Certificates

Certificate ID	Subject
<a href="#">e59cdb55-9327-4da1-bdaa-564d6920ef5b</a>	CN=Inst_0_b5334de33e06@192.168.170.117
<a href="#">09348c27-9cde-49d5-a8c5-6abaac3a631c</a>	CN=Inst_0_873b25d3cbea@192.168.170.117
<a href="#">7ab42aab-4e4b-4f50-8e39-e173c4a424ae</a>	CN=Inst_0_07037a0af0f5@192.168.170.117
<a href="#">6052988a-c311-46ca-bccc-e3faabab5c0a</a>	CN=Inst_0_d8f58e63168e@192.168.170.117
<a href="#">ea373b56-64e1-434d-96e3-e49bd772a9d8</a>	CN=Inst_0_12977565496625
<a href="#">3687c89d-a7bf-4ef5-a56c-e49aa3f85235</a>	CN=Inst_0_7668d1ac8bb9@192.168.170.117
<a href="#">2d51917c-7e40-4096-8574-c169fc1064b0</a>	CN=Inst_0_8e1580f76547@192.168.170.117
<a href="#">e22573eb-1798-495e-940e-025d71741e97</a>	CN=Inst_0_3a99b4449d3d@192.168.170.117
<a href="#">2c4d5676-52f2-4b29-91cc-20faf3a7aff1</a>	CN=Inst_0_d5cb158d3ab0@192.168.170.117
<a href="#">9c02b914-25ac-4479-9450-848513f1c96e</a>	CN=Inst_0_13036584921850
<a href="#">8d15b7d0-9a21-4b9e-a74f-faed5de379ce</a>	CN=Inst_0_13031059387330
<a href="#">d07de306-ae39-42c8-a7d4-ed67a3391505</a>	CN=Inst_0_15115f9000e3@192.168.170.117
<a href="#">191052b2-3b8c-4c96-b871-02a8ca881700</a>	CN=Inst_0_d8f58e63168e@192.168.170.117

Fig. 18: Certificate Management

- In the structure view, select the menu item *Security > Certificate Management*.
  - ⇒ In the section *Queued CSRs*, all unconfirmed certificates are listed.
- Click on the certificate of the recording server.
  - ⇒ The certificate is displayed.



**MITEL STANDARD LINUX**

admin@mbg.asc.de Logout

**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

**Miscellaneous**  
 Support and licensing  
 Help

### Viewing CSR ID "720f901c-2d47-4789-bca6-9b4f3a71d90f"

Certificate Request:

Data:

Version: 0 (0x0)

Subject: CN=Inst\_1\_13051701564564

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public Key: (2048 bit)

Modulus:

```
00:ba:7e:c9:9d:d6:8b:ae:ac:e9:03:bb:56:02:e7:
27:03:2f:06:64:e8:1c:4f:dd:d8:ef:55:4e:78:90:
76:8e:24:48:ab:2a:8b:cf:19:93:e9:26:b2:b9:3a:
84:20:d5:ec:85:88:77:5c:78:f2:77:d4:f5:c9:2c:
e1:99:00:68:8a:cf:ee:46:c3:8b:f8:e2:36:b8:d8:
41:44:41:de:86:ce:c3:53:8e:2d:02:9f:6e:9d:2a:
68:87:0e:fe:80:72:02:12:5e:38:65:d2:f8:d6:66:
e3:08:ba:ea:1e:14:f9:29:02:36:f0:c3:f7:7d:72:
07:7d:64:e6:c5:13:38:5b:a1:92:af:00:81:47:9e:
8a:5e:86:c0:93:a6:36:55:80:99:ef:53:56:32:0d:
7e:63:07:41:80:40:b0:04:b3:2d:19:92:84:30:e9:
d0:9d:25:bf:1a:87:22:e5:4c:f7:12:28:55:cf:19:
66:38:54:9f:b2:ce:d7:4e:a1:5e:d0:9b:b9:1b:2e:
31:75:a3:3e:4a:12:43:e4:0f:9b:c5:37:73:6d:9a:
a2:4e:7a:ca:84:a6:a1:80:a3:f1:d8:1a:13:65:61:
df:d2:d9:79:1c:51:64:0f:94:26:28:37:9f:09:06:
c3:1e:a8:a7:d6:29:92:be:d4:89:09:95:f4:c1:05:
95:67
```

Exponent: 65537 (0x10001)

Attributes:

Requested Extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

Signature Algorithm: sha1WithRSAEncryption

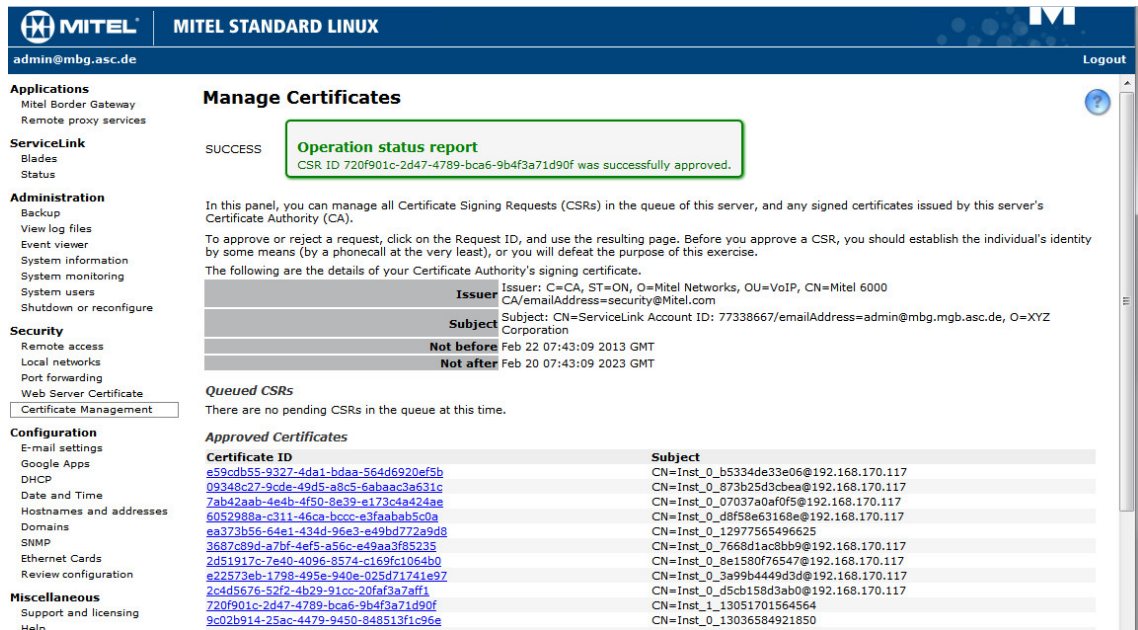
```
33:c6:c9:51:bc:5e:a3:2a:48:15:c2:c8:99:c2:ee:60:85:ac:
83:1a:c7:e3:6b:08:5d:0c:24:53:c1:16:3f:63:b0:36:87:9a:
0b:d2:dc:15:61:e2:c1:70:7a:84:69:ad:8b:9b:8e:49:b6:5d:
21:7c:67:a2:8d:b8:99:28:b2:02:8f:22:20:24:d0:28:0a:ed:
b5:a1:2e:c6:2f:74:1c:60:e9:8d:71:92:87:9f:d1:dc:f2:fc:
2c:32:d3:ab:1f:94:b5:f8:cb:7a:fe:80:f1:7a:79:36:bf:ad:
c0:be:f3:00:40:2d:4f:a9:c0:37:58:61:b1:4f:b0:c8:25:b7:
e7:76:01:be:e5:0a:a4:ef:c0:26:1b:c7:52:e5:a0:8e:52:f6:
dd:d3:32:46:28:f0:d0:12:9a:d3:4e:57:7f:4d:15:e5:7c:fd:
ea:9e:1c:35:bb:ae:36:a6:e9:b7:c3:bb:49:47:0b:96:e2:69:
e1:fd:b3:23:5a:4b:e0:cc:94:99:99:16:2c:87:5c:c5:31:b7:
e5:dc:df:c4:39:ea:2b:7e:9c:a0:cf:35:c2:64:80:67:ee:01:
1c:5a:07:c2:82:bf:0b:70:b9:1f:ed:70:4f:37:54:c8:b9:0c:
c9:87:11:20:6d:f5:de:33:49:06:af:cf:17:60:bd:ca:b9:d8:
18:b3:59:ce
```

Cancel Reject Approve

Fig. 19: Confirm selected certificate

5. Click on the button *Approve*.

⇒ Once the certificate has been shared, the following success notification appears:



The screenshot shows the MITEL STANDARD LINUX web interface. The left sidebar contains a navigation menu with categories: Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled 'Manage Certificates' and displays a 'SUCCESS' message in a green box: 'Operation status report: CSR ID 720f901c-2d47-4789-bca6-9b4f3a71d90f was successfully approved.' Below this, there is a detailed explanation of the process and a table showing the details of the Certificate Authority's signing certificate. The table has columns for Issuer, Subject, Not before, and Not after. Below the table, there are sections for 'Queued CSRs' (showing no pending CSRs) and 'Approved Certificates' (showing a list of certificates with their IDs and subjects).

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

Fig. 20: Success notification for shared certificate

The recording server can now connect to 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.`



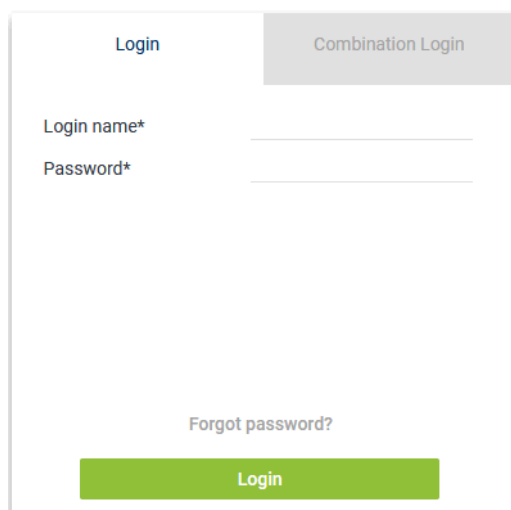


Fig. 21: System Configuration - web interface

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

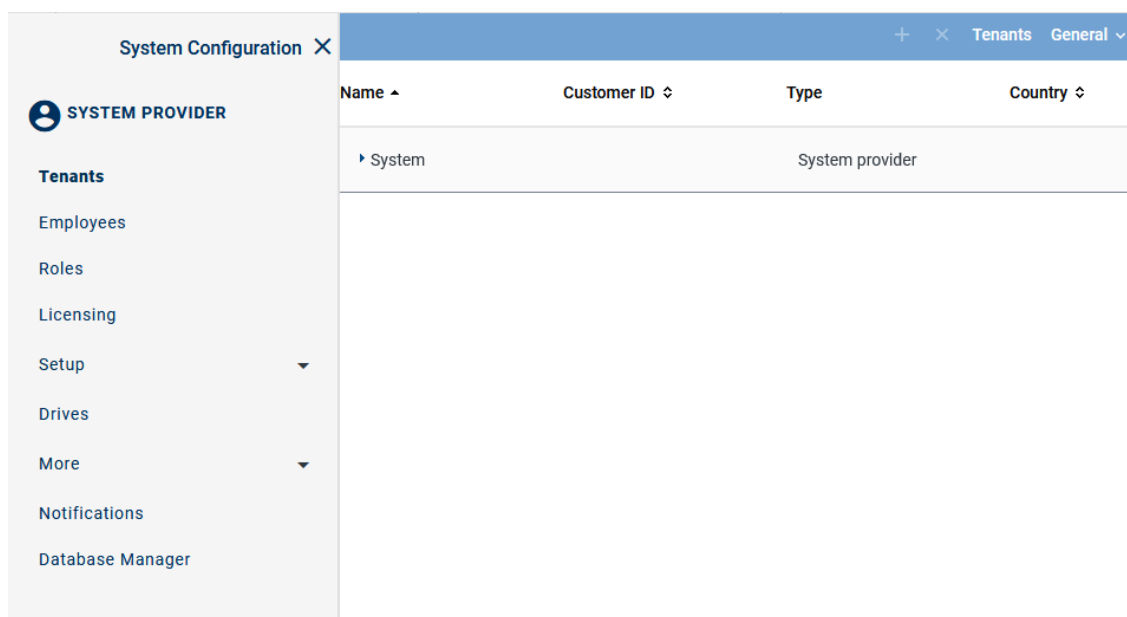
Login data for the administrator of the system provider:

User name:	<i>system-admin</i>
<u>neo</u> version < 6.3	
Default password:	1
	If the default password 1 has never been changed before a software update to a <u>neo</u> 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 <u>neo</u> version ≥ 6.3, the changed password remains.
<u>neo</u> version ≥ 6.3	
Default password:	A\$c123

Tab. 9: Login data - system provider

## 2. Log in to the web interface.

⇒ The main window System Configuration appears.



Name	Customer ID	Type	Country
System		System provider	

Fig. 22: System Configuration - main view:

### 7.3.2 Configure recording solution Mitel MX-ONE CSTA

#### Supported recording architectures

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

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

#### 7.3.2.1 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:

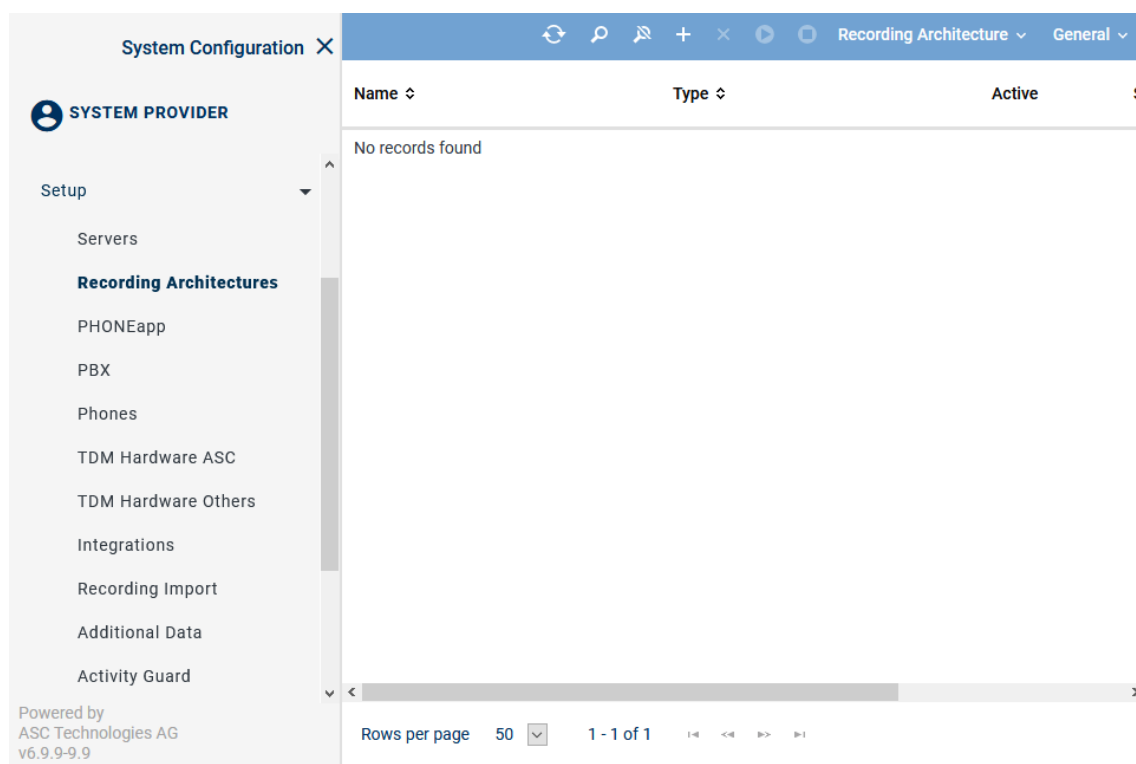



Fig. 23: Recording architectures - main view

<b>Name</b>	Name of the recording architecture
<b>Type</b>	Type of the recording architecture
<b>Active</b>	Shows whether the recording architecture has been activated and is ready to be used for the recording.  <div> <span>✓</span> = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon <span>⏏</span> (Deactivate) in the toolbar. </div>

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









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

### Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 24: Toolbar Recording Architectures module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	<p>Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.</p> <p>The icon  is displayed whenever the search has been adjusted by means of a filter.</p>
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	<p>Deletes the selected recording architecture. The recording architecture is removed from the list of the main view.</p> <p><b>NOTICE!</b> You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.</p>
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	<p>Deactivates the selected recording architecture.</p> <p><b>NOTICE!</b> You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.</p>
<i>Recording Architecture</i>	<i>Standby Management</i>	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	<p>Opens a window in which you can adjust the following settings for the main view:</p> <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>




<i>General Help</i>	Opens the online help.
<i>Module Help</i>	Opens the module-specific online help.



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

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

Create a recording architecture of the type *All-in-one Basic Recording*.

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

⇒ The window *New Recording Architecture* appears.

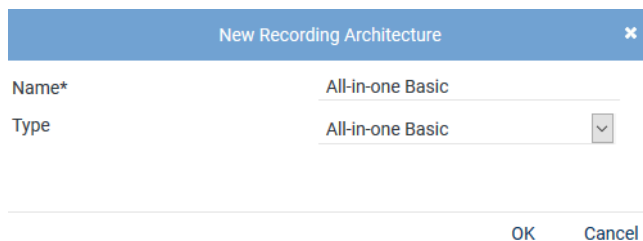


Fig. 25: Create recording architecture - All-in-one Basic Recording

- 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.

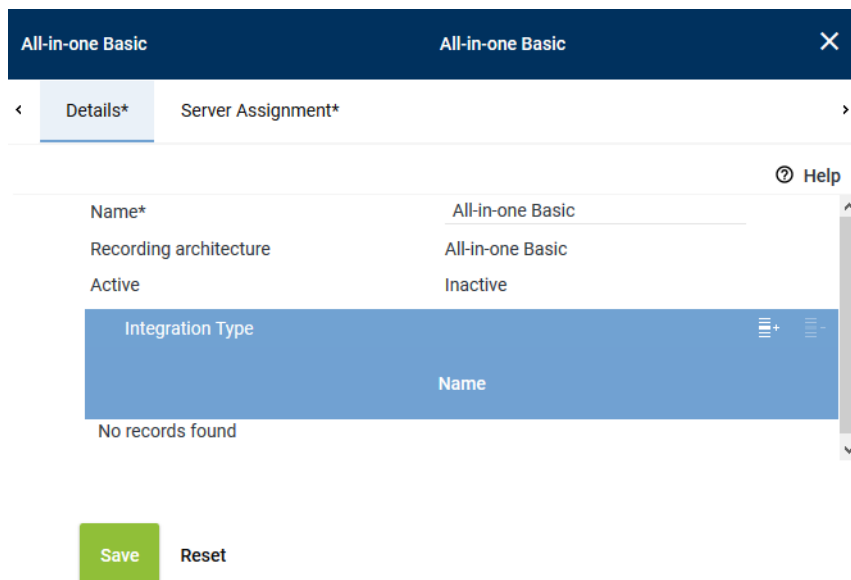
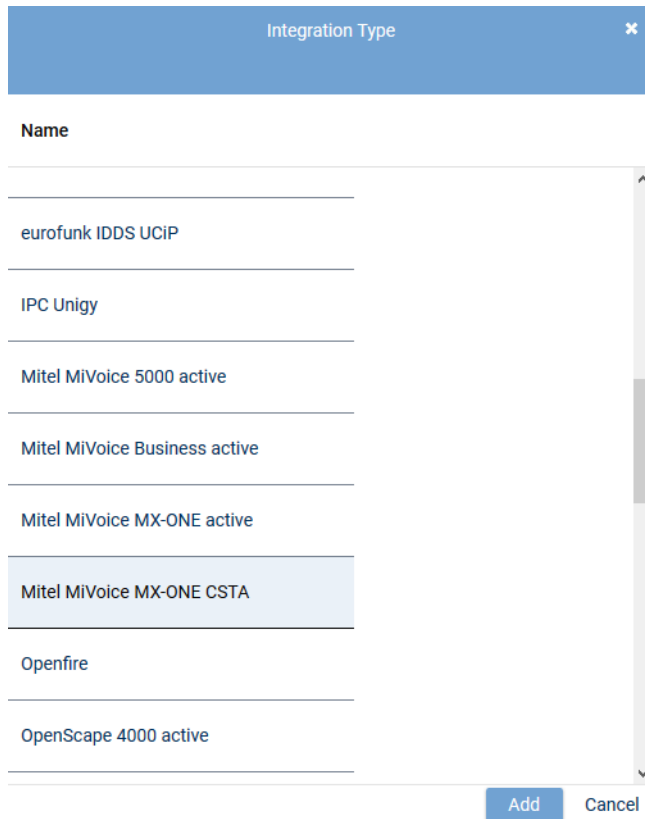


Fig. 26: Recording architecture - tab Details

### 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. 27: 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..

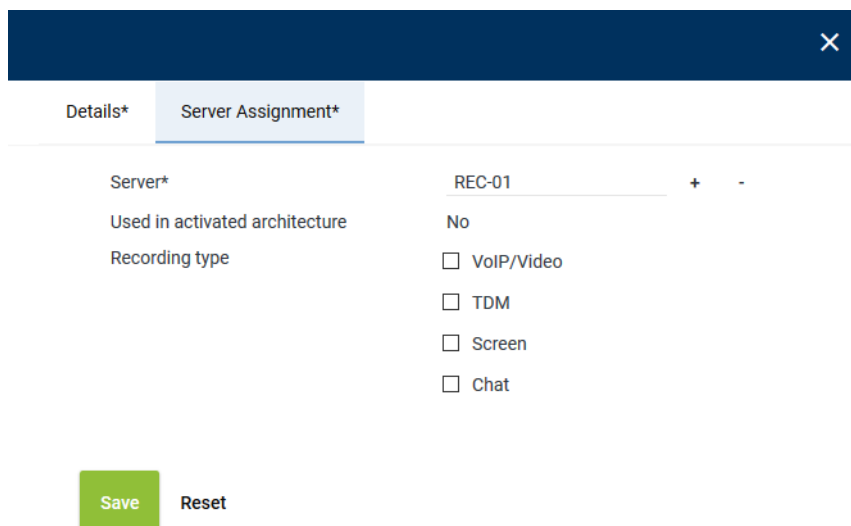


Fig. 28: Recording architecture - tab Server Assignment

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



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

Fig. 29: Recording architecture - assign server

3. Select the respective server.



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

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

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen

☐ Chat




**Save** Reset

Fig. 30: Recording architecture - activate recording variant



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

### Activate recording architecture

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





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

Fig. 31: Recording architecture - activate recording architecture

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



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



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

#### 7.3.2.1.2 Configure server

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

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

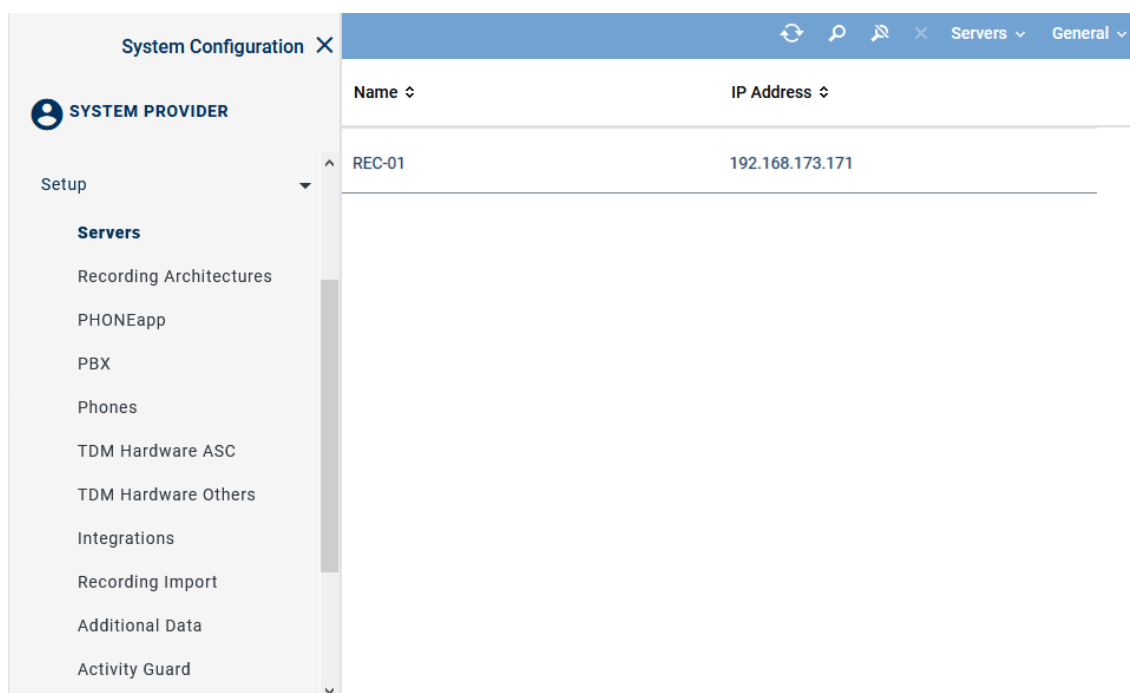


Fig. 32: Servers - main view

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

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






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

### Toolbar of the Servers module

The toolbar offers the following functions.



Fig. 33: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.  The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <u>neo</u> system.

<b>Servers</b>	<b>Administrate Server Locations</b>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 34.</a>
	<b>Administrate NTP Server</b>	Opens a window in which you can administrate the servers for the time synchronization, see <a href="#">Administrate NTP server.</a>
	<b>Manage Synchronization Configurations</b>	Opens a window in which you can manage the synchronization configurations.
<b>General</b>	<b>Adjust Table</b>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<b>General Help</b>	Opens the online help.
	<b>Module Help</b>	Opens the module-specific online help.



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

### Administrate server locations

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

#### Add server locations

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

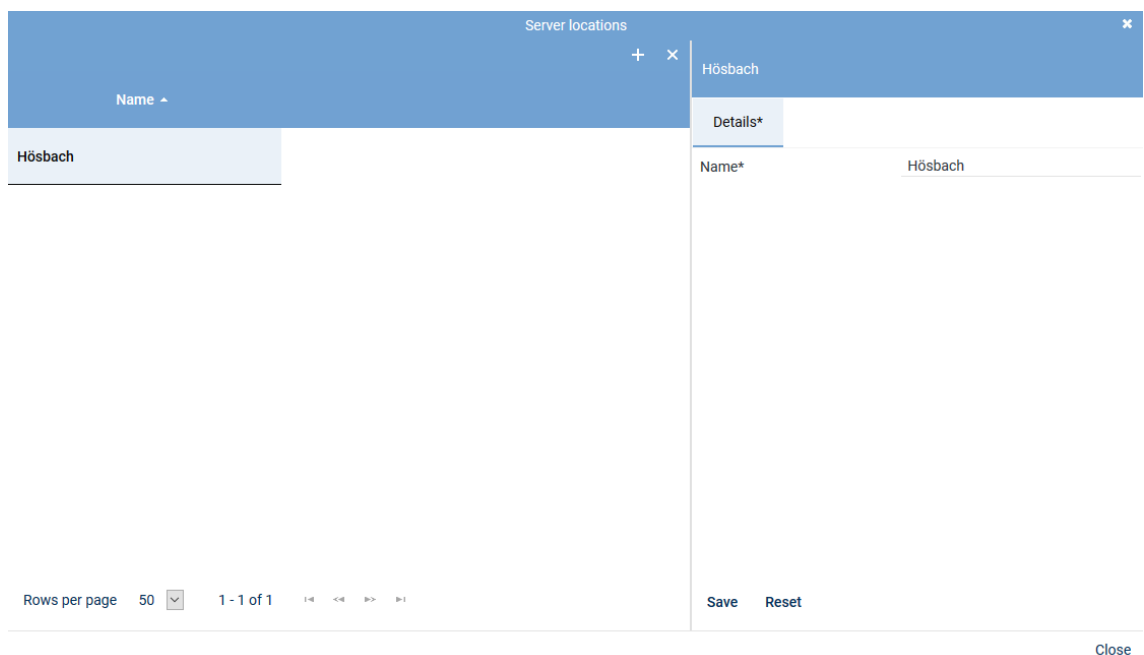



Fig. 34: Add server locations

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

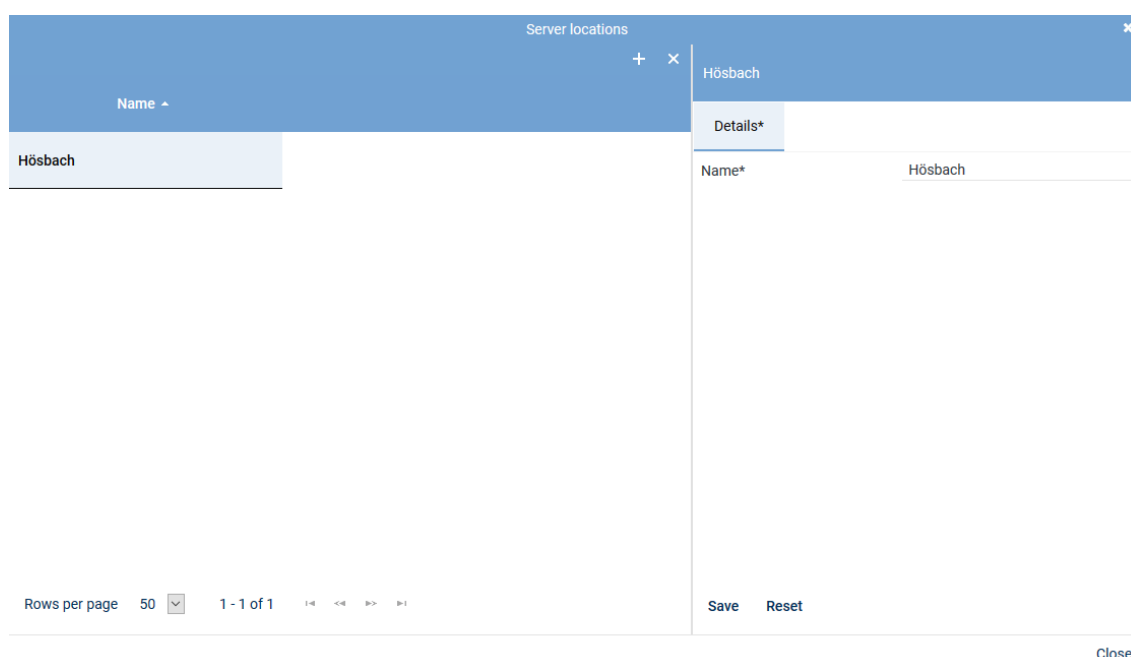
4. To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

### Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Inside the window, there is a table with a header "Name" and a single row containing "Hösbach". To the right of the table is a "Details\*" panel. The "Details\*" panel has a tab labeled "Details\*" and a form field labeled "Name\*" with the value "Hösbach". At the bottom of the window, there are buttons for "Save" and "Reset", and a "Close" button in the bottom right corner. The bottom of the window also displays "Rows per page 50" and "1 - 1 of 1".

Fig. 35: Delete server location

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

### Tab Details

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

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

? Help

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

Save
Reset

Fig. 36: Servers - tab Details

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

### Tab Usage

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



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

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

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

Save
Reset

Fig. 37: Servers - tab usage



### Group field API Server

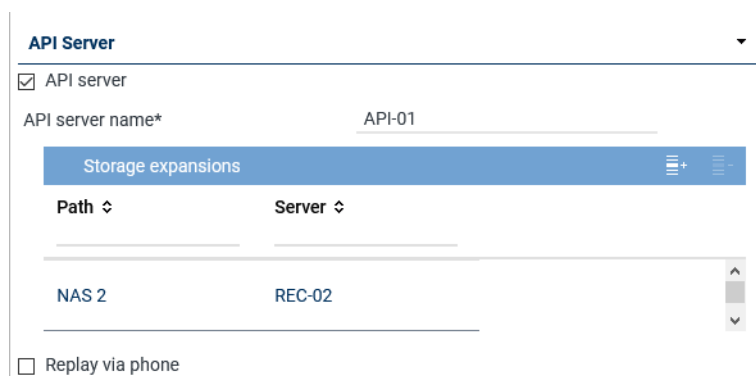




Fig. 38: Group field API Server

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


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

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

Parameter	Value/Description
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping", p. 47</a>.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List</i> <i>Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay", p. 38</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul>

Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.  <input type="checkbox"/> = Function has not been activated.</p> <p><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWERplay Pro</li> <li>• Application POWERplay Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see <a href="#">chapter "Tab Media Streamer", p. 45</a>. To be able to do so, at least 1 PBX must have been configured in the system.</p>

### Add storage expansion for replay

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

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

Rows per page: 20 1 - 1 of 1

Add Cancel

Fig. 39: Select storage expansion

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

### Group field Audio analysis

**Audio Analysis**

☒ Emotion detection

Stream audio data from\* REC-01 + -

Fig. 40: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> <li>Click on the button <b>+</b> to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 10: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

Rows per page 20 ▼ 1 - 8 of 8 ⏪ ⏩ ⏴ ⏵

Add Cancel

Fig. 41: Select server for emotion detection

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

### Group field Recording Control/Key Management

**Recording Control/Key Management** ▼

☒ Recording control/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 42: Group field Recording Control/Key Management

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

Tab. 11: Configure recording control/key management

### Group field Data Processing

**Data Processing**

☒ Data storage

☐ Transfer data for replay

Target Server

Name

IP Address ↕

No records found

☒ Transfer data for data storage

Target Server

Name

IP Address ↕

No records found

Activate period of time

☒

Start

0:00

▼

End

4:00

▼

Receives data from

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 43: Group field Data Processing

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34


40 / 489

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 42</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list", p. 42</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b></p> <p>For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>

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

Tab. 12: Data storage

### Add target server to a list

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

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

Rows per page 20 1 - 6 of 6

Add Cancel

Fig. 44: 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*

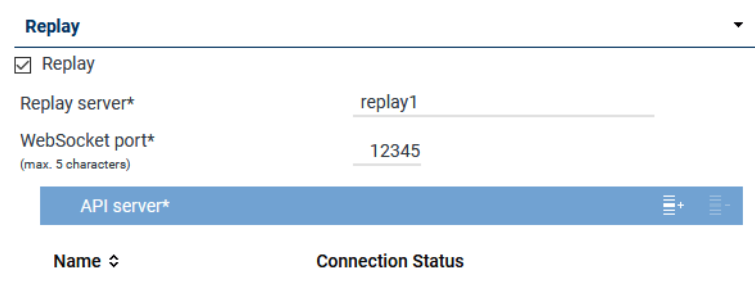




Fig. 45: Group field *Replay*

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API server</a> must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in <a href="#">POWERplay Web</a> are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 44.</li> <li>By clicking on the icon  (Remove), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 13: 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. 46: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 37.

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



### Group field Virtualization

#### Virtualization

☐ VM without Trusted License

Fig. 47: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> <li>• <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 14: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

### Tab Media Streamer

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

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



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

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

PBX +

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

Save
Reset

Fig. 48: Servers module - tab Media Streamer

2. Enter the following parameters:

<b>PBX</b>	<p><b>PBX</b> that the Media Streamer is supposed to be mapped to.</p> <p>Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.</p> <p>If no <b>PBX</b> has been created in the system yet, you can create a <b>PBX</b> via the blue bar <b>PBX</b>, see <a href="#">chapter "Create PBX"</a>, p. 52.</p>
<b>Extension</b>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <b>8000</b>.</p>
<b>Media streamer IP address</b>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <b>SIP</b> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <b>169.254.254.100</b> in the drop-down list.</p>
<b>Minimum port</b>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<b>Maximum port</b>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p>

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

### Tab Replay Server Address Mapping

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

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




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

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

---

**Replay Server Addresses**

 Remove Replay Server Addresses

Internal IP address/ port of the replay server:  :

Internal download URL:

External address/ port of the replay server:  :

External download URL:

Fig. 49: Servers Module - tab Replay Server Address Mapping

### Group field Replay Server Addresses

1. Enter the following parameters

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

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



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

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



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



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

### Tab Key Management

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

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

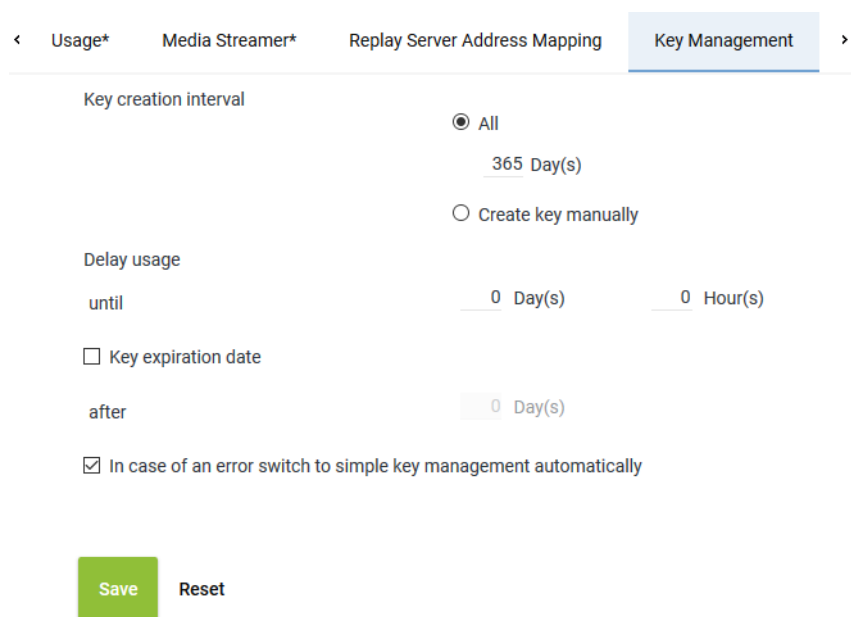


Fig. 50: Servers module - tab Key Management

<b>Key creation interval</b>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</li> </ul>
<b>Delay usage</b>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<b>Key expiration date</b>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p>

	<p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

#### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.  
In this case, no separate configuration is required.  
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*  
In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*  
**NOTICE! License Management does not support encryption.**

#### For licensing, there are the following options:

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on. In this case, no separate configuration is required.

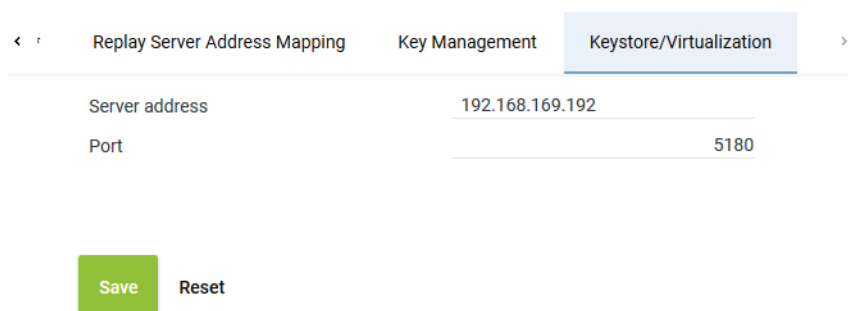
- *Trusted Virtualization License*

Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this. In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



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

Fig. 51: Servers module - tab Keystore/Virtualization

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



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

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

### 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:

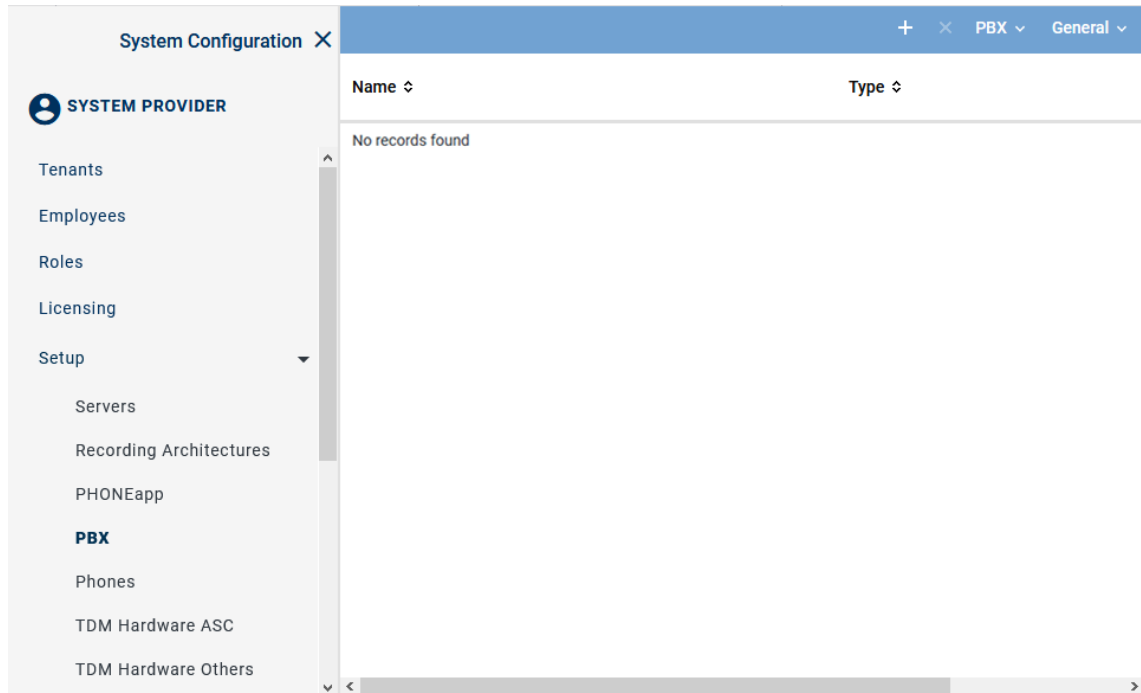


Fig. 52: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

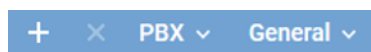




Fig. 53: Toolbar PBX module

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




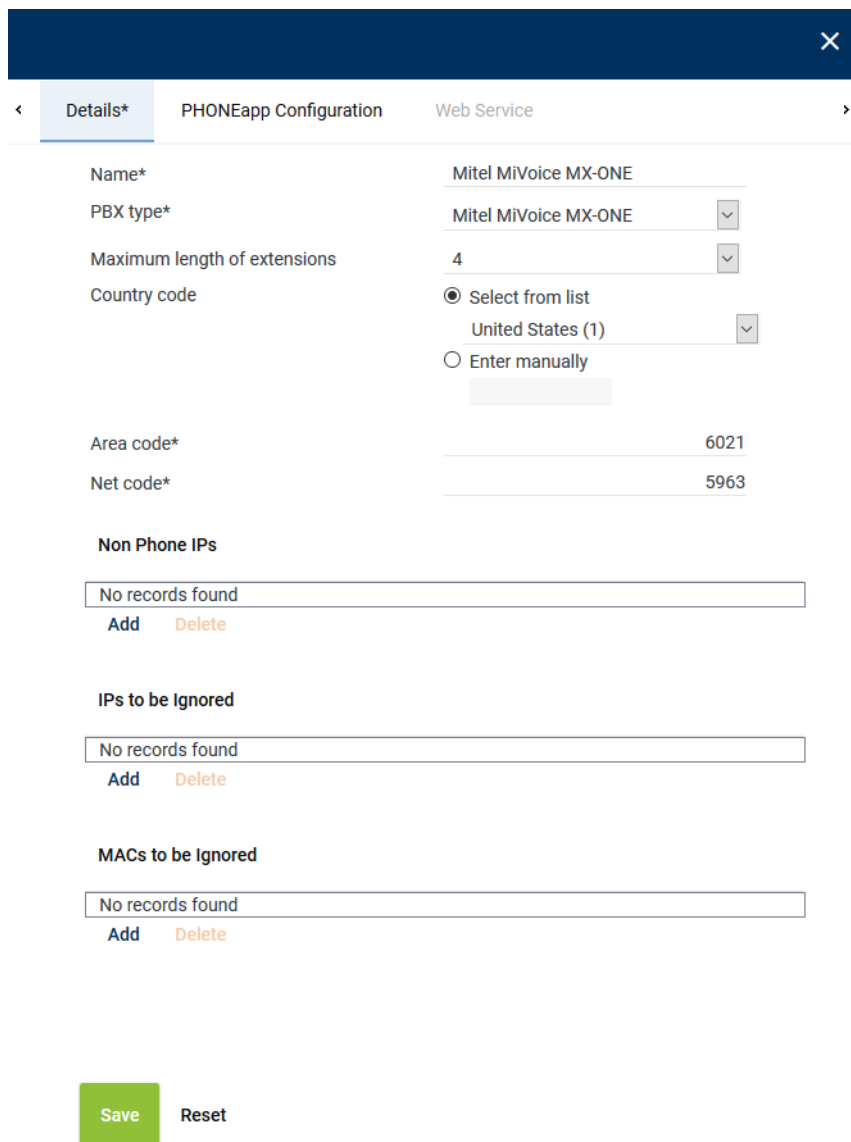
*Module Help* Opens the module-specific online help.



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

### Create new PBX

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



**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. 54: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the <a href="#">PBX</a> from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <li><i>Select from list</i></li> </ul>

Parameter	Value/Description
	Select the country code from the drop-down list. <ul style="list-style-type: none"> <li>• <i>Enter manually</i></li> </ul> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka <i>094</i> .
Area code	Enter the area code without the preceding 0, e. g. 6021.
Net code	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 15: Create PBX

- 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

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

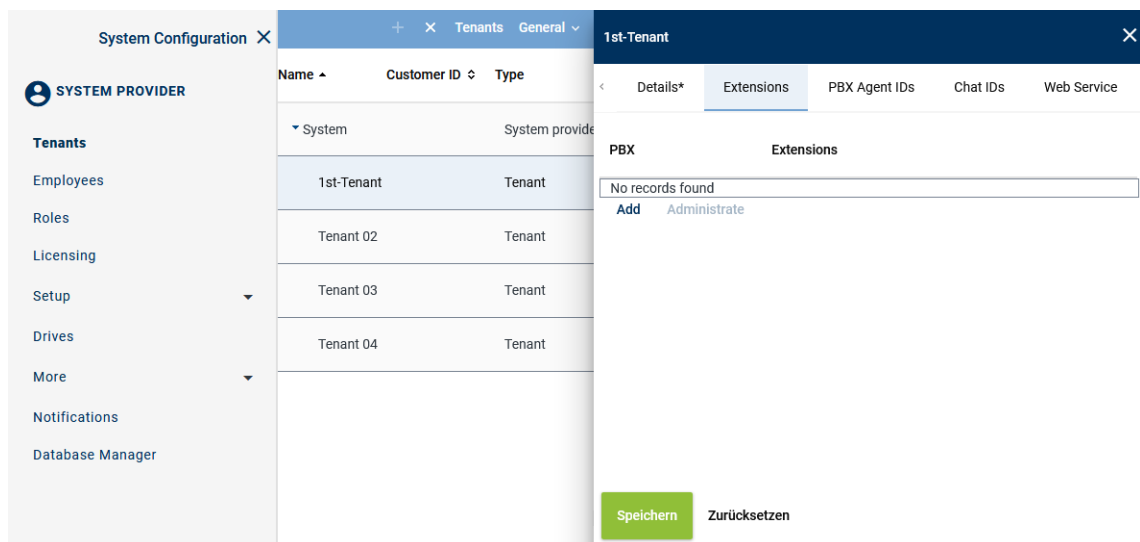


Fig. 55: Tenants - main view - tab Extensions

##### 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. 56: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>ZIP</li> <li>TXT</li> <li>CSV</li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>Click on the button <span style="background-color: #f1f3f4; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>Click on the button <i>Choose File</i>.</li> <li>Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>Click on the button <span style="background-color: #4285f4; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34

55 / 489

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

Enter country codes as number ranges as follows:

+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions* Activate the check box to replace the list of extensions.

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

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

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

### Remove extensions

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

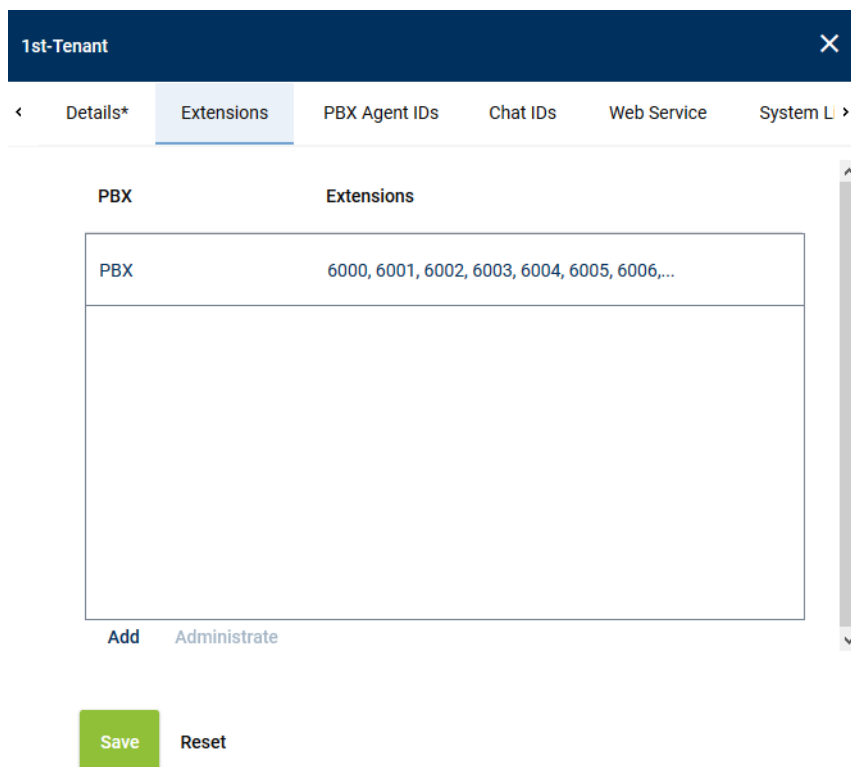


Fig. 57: Remove extensions

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. 58: 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.

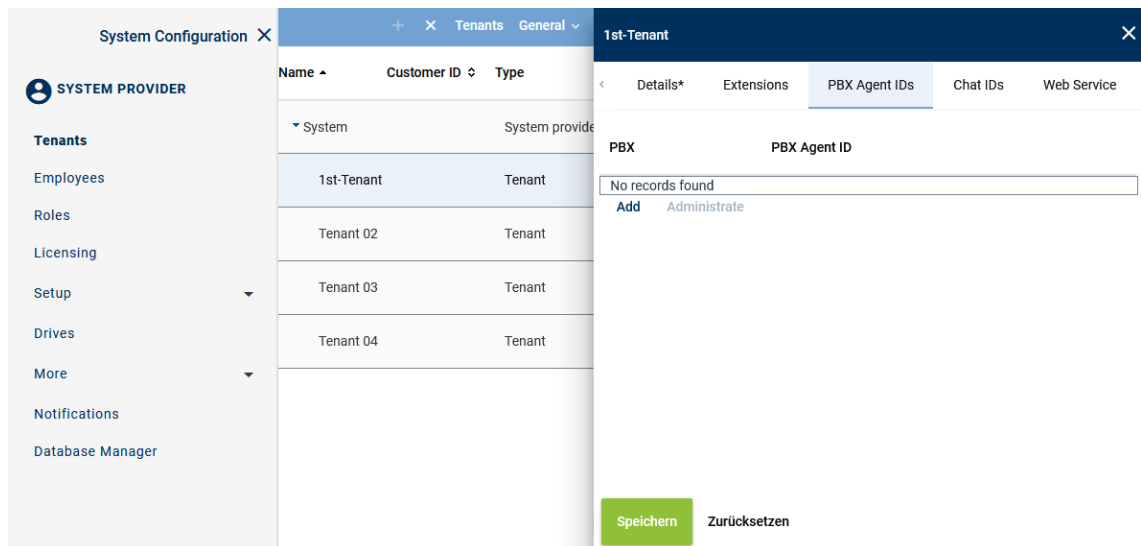


Fig. 59: Tenants - main view - tab PBX Agent ID

### 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:

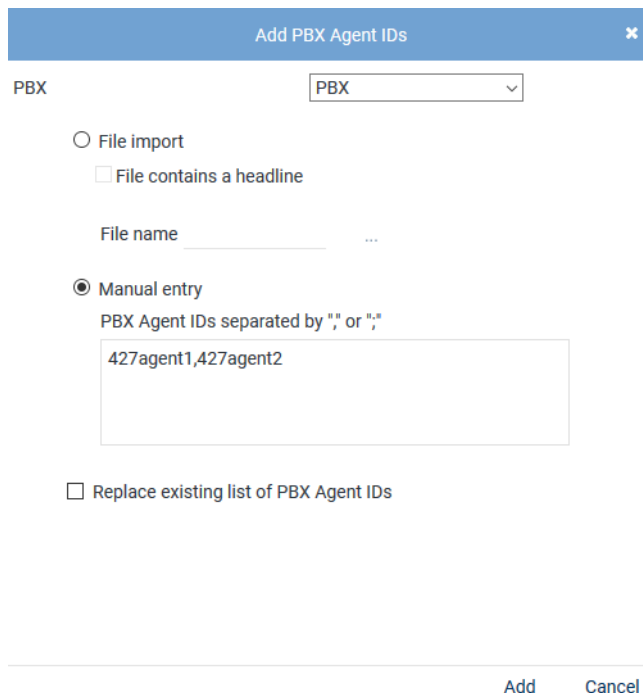




Fig. 60: Assign PBX Agent IDs to tenants

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 the option to import PBX Agent IDs from an existing <a href="#">CSV</a> 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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> 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"> <li>• Click on the button  behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p><b>NOTICE! Wildcards cannot be used!</b></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. 61: 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*.

### 7.3.2.1.5 Configure additional data

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

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

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

**System Configuration** ✕

**SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 62: 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. 63: 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. 64: 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 Basic

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

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

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

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

⇒ The following window appears:

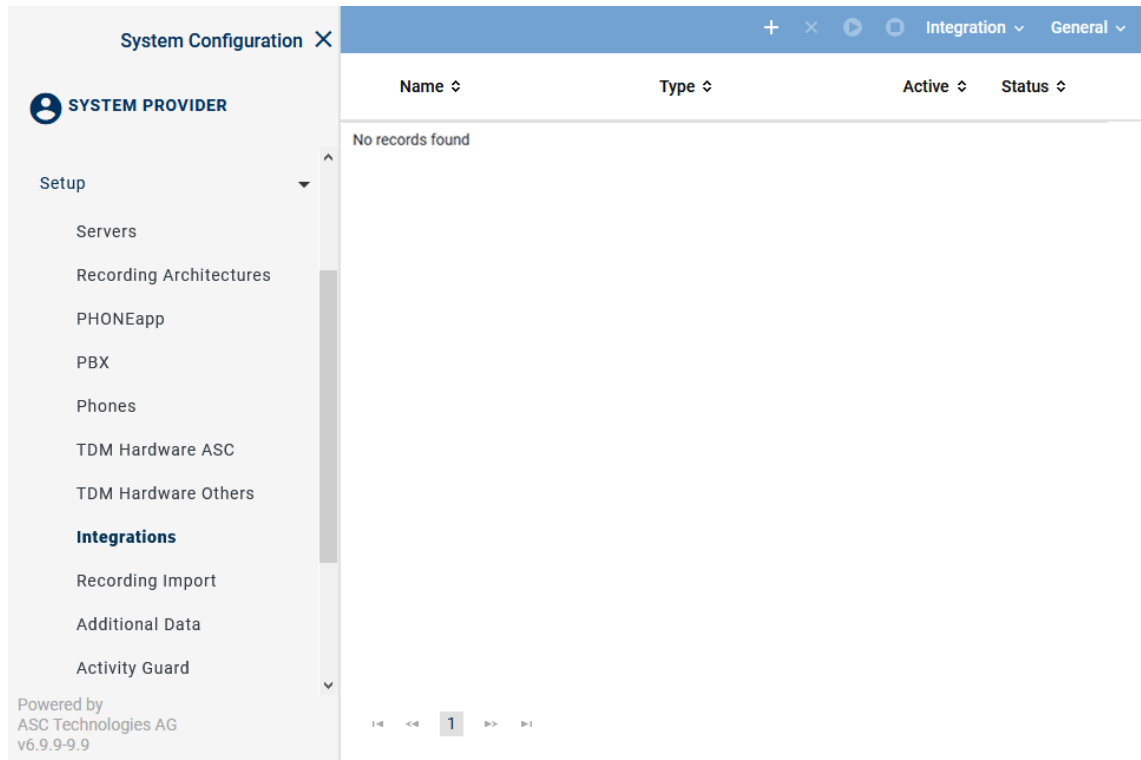




Fig. 65: Integrations - main view

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



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



### Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 66: Toolbar Integrations module

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

	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

- 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.

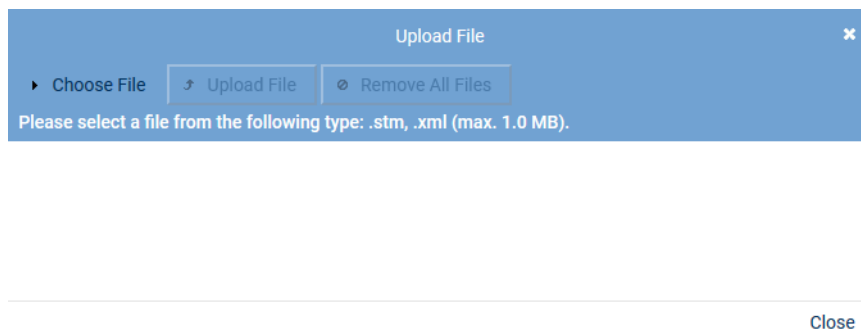


Fig. 67: Choose file

- 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*.

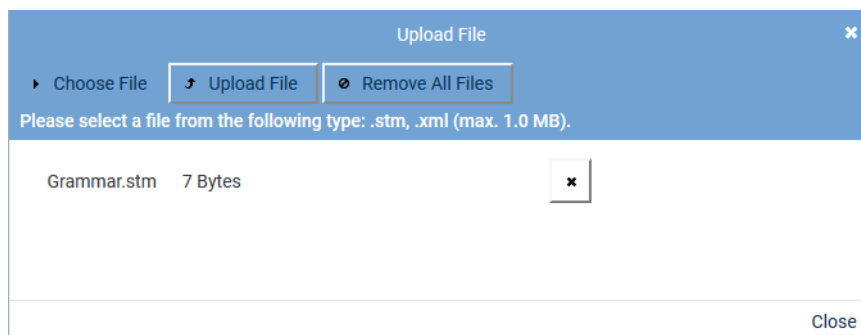



Fig. 68: Upload grammar

- 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. 69: Create integration type

- Enter the following parameters:

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

Tab. 16: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

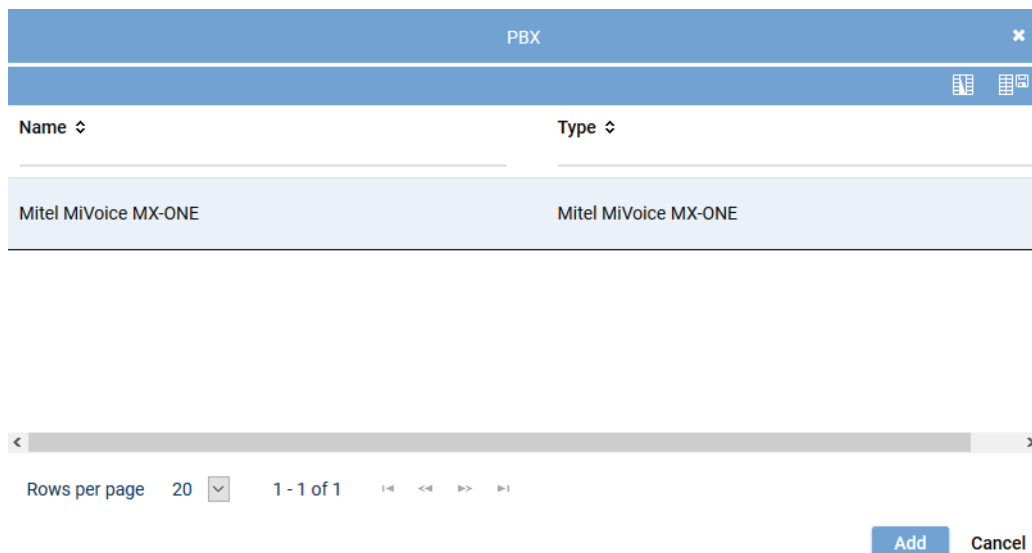


Fig. 70: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

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

- 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. 71: 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		✖		⚙	
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. 72: 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.

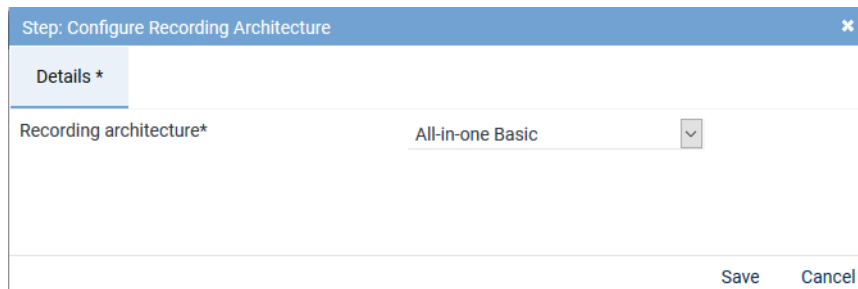



Fig. 73: Configuration step - Configure Recording Architecture

- 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab *MiVoice MX-ONE (CSTA)*

- Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\*
MBG\*

CTIconnect Module

Connection Data

Additional Data

Failover waiting time\*
10

Failover repetitions\*
3

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}\$

Save
Cancel

Fig. 74: CTI connection data - tab MiVoice MX-ONE (CSTA)

By configuring the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

The [CSTA](#) connection is used to monitor the configured monitor points and to start the recording by means of the intrusion feature.



Following an update, you must configure this section 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. 75: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 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 MiVoice MX-ONE (CSTA)

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.

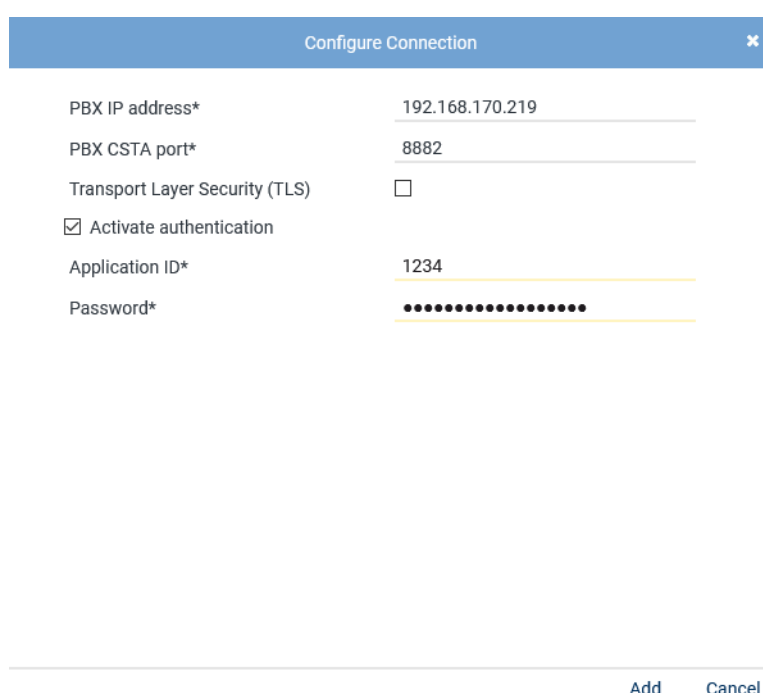


Connection Data
PBX IP address
No records found

Add Edit Delete

Fig. 76: 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

PBX IP address\*

192.168.170.219

PBX CSTA port\*

8882

Transport Layer Security (TLS)

☐

☒ Activate authentication

Application ID\*

1234

Password\*

.....

Add

Cancel

Fig. 77: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the <a href="#">CSTA</a> connection is supposed to run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate this check box to use the connection with <a href="#">TLS</a> .
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14</a> .
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14</a> .



Parameter	Value/Description
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 18: Configure connection data

- 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.

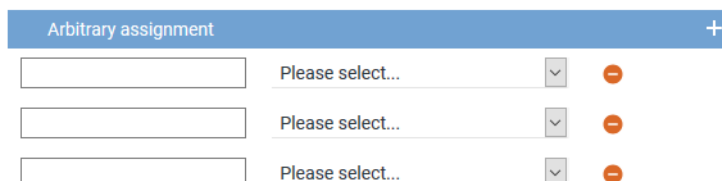



Fig. 78: Arbitrary assignment of the additional data

The following additional data is always available:

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

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

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



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



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

### Configure 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 CTIconnect 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. 79: Configure switching conditions

<b>Failover waiting time</b>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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.
<b>Failover repetitions</b>	Enter how many times the CTI <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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]?$|^\\s[0-9]{4}[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 80: 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.



As parallel recording is only possible via the **MBG**, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

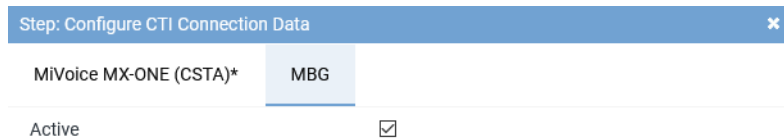


Fig. 81: Activate CTIconnect connection data for [MBG](#)

**Active** Activate the check box to display the configuration parameters and to activate the connection to the [MBG](#).

☒ = Connection has been activated.

☐ = Connection has not been activated.



Following an update, you must configure this section again.

### Group field CTIconnect Module

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

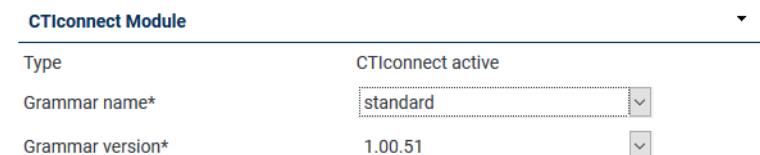


Fig. 82: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 19: 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 MBG

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

**Connection Data** ▼

---

Connection data

No records found

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

Fig. 83: Group field Connection Data

1. In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

Configure Connection
✕

Connection data*	192.168.170.116
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>
<input checked="" type="checkbox"/> Use pre-shared key	
Pre-shared key (PSK)*	●●●●●●●●

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

Fig. 84: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the <a href="#">MBG</a> .
<i>PBX port</i>	Enter the port for the <a href="#">MBG</a> or the <a href="#">SRC</a> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <a href="#">MBG</a> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 20: 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 MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

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.

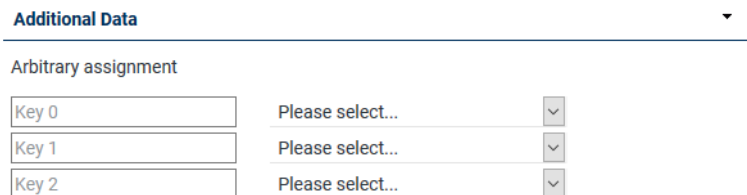


Fig. 85: CTI connection data - additional data module 1

2. Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
3. From the drop-down list, select the entry which is supposed to appear as column headline in the players.
4. Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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.

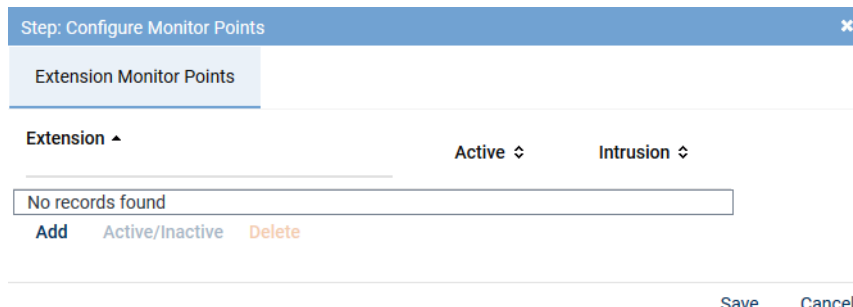


Fig. 86: Configuration step - configure monitor points

### Tab 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.

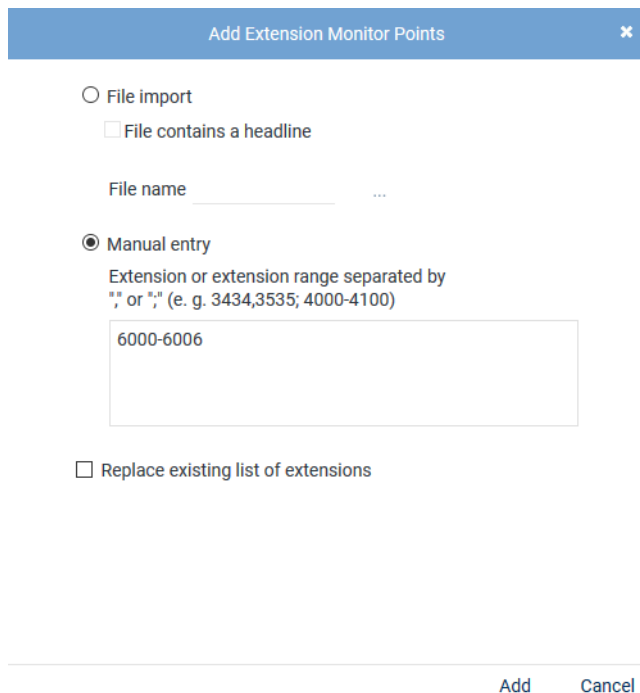



Fig. 87: Add extension monitor points

<b>File import</b>	<p>Select this option to import extensions from an existing <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>↗</b> (<i>Upload file</i>).</li> </ul>
<b>File contains a headline</b>	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
<b>File name</b>	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> </ul>

	<ul style="list-style-type: none"> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  (<i>Upload file</i>).</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>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><b>NOTICE! Wildcards cannot be used!</b></p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; 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"/>
<a href="#">Add</a> <a href="#">Active/Inactive</a> <a href="#">Delete</a>		
<div>Save   Cancel</div>		

Fig. 88: Configured extension monitor points



<i>Add</i>	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.
<i>Active/Inactive</i>	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.
<i>Delete</i>	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.
<i>Intrusion</i>	<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<sup>connect</sup> 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. 16](#).

### Global recording settings

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

Step: Global Recording Settings
✕

Details\*

Transport protocol	UDP	▼
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. 89: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i>, the transport protocol applies for the SIP communication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p><b>TCP</b> = unencrypted</p> <p><b>UDP</b> = unencrypted</p> <p><b>TLS</b> = encrypted</p>
<i>Port SIP signaling</i>	Enter the port for <b>SIP</b> signaling that is opened on the recording server for incoming <b>SIP</b> communication and that has been selected in the outgoing <b>SIP</b> notifications as the port of the recording server. Default <b>5060</b> .
<i>Remote SIP port</i>	Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by <b>SIP</b> to start <i>active-stream recording</i> . Default <b>7300</b> .
<i>Activate SIP authentication</i>	Activate the check box if <b>SIP</b> 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 <b>SIP</b> registration of extensions recorded with intrusion feature. The user name is configured in the <b>PBX</b> and applies for all extensions to be registered.

Parameter	Value/Description
<i>Password of the SIP registration</i>	Enter the password for <a href="#">SIP</a> registration of extensions recorded with intrusion feature. The password is configured in the <a href="#">PBX</a> 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 <a href="#">PBX</a> .
<i>PBX port</i>	Enter the port for the communication with the <a href="#">PBX</a> , default 5060.


Tab. 21: Global recording settings

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



Following an update, you must configure this section 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.

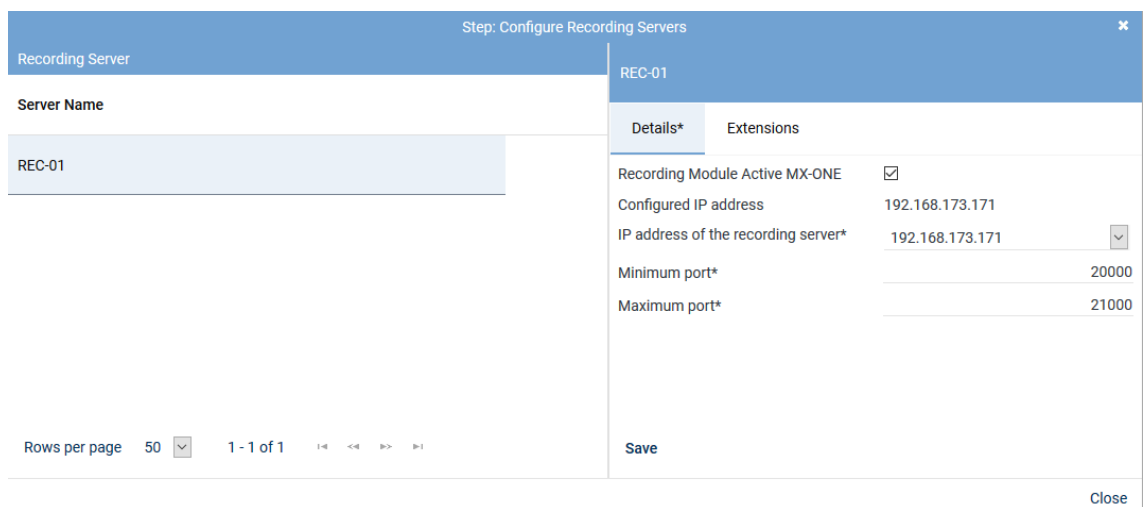


Fig. 90: Configuration step - Configure recording servers

- 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 <a href="#">RTP</a> 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 <b>RTP</b> data from the recording server, e. g. <b>21000</b> .

Tab. 22: 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.



Following an update, you must configure this section 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 CTI~~connect~~ module of the integration.



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

### Configure add-on for 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. 91: 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	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 23: 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. 24: 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.

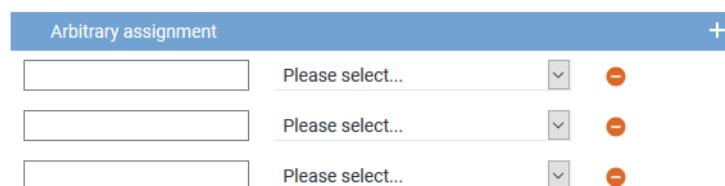



Fig. 92: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*

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

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



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



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

### **Configure add-on for 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<sup>connect</sup> 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

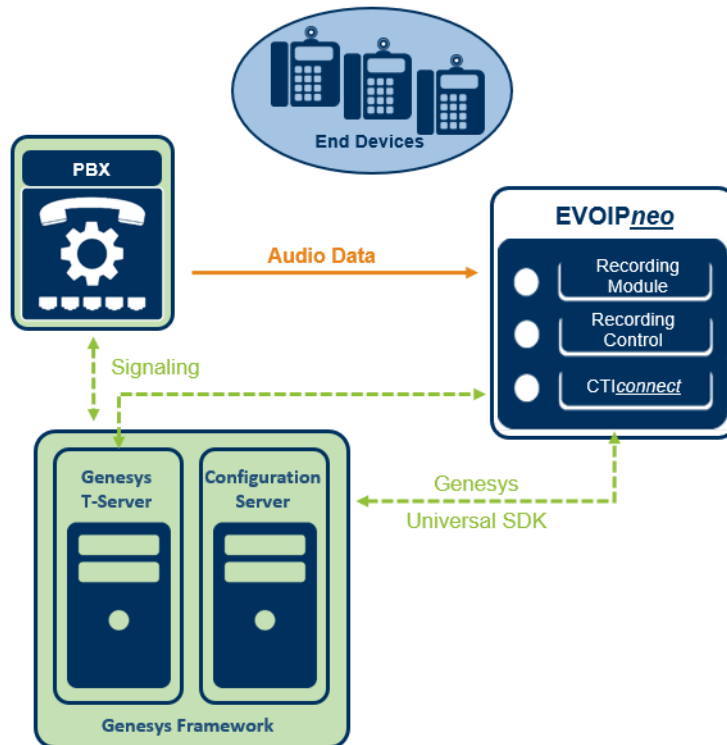


Fig. 93: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

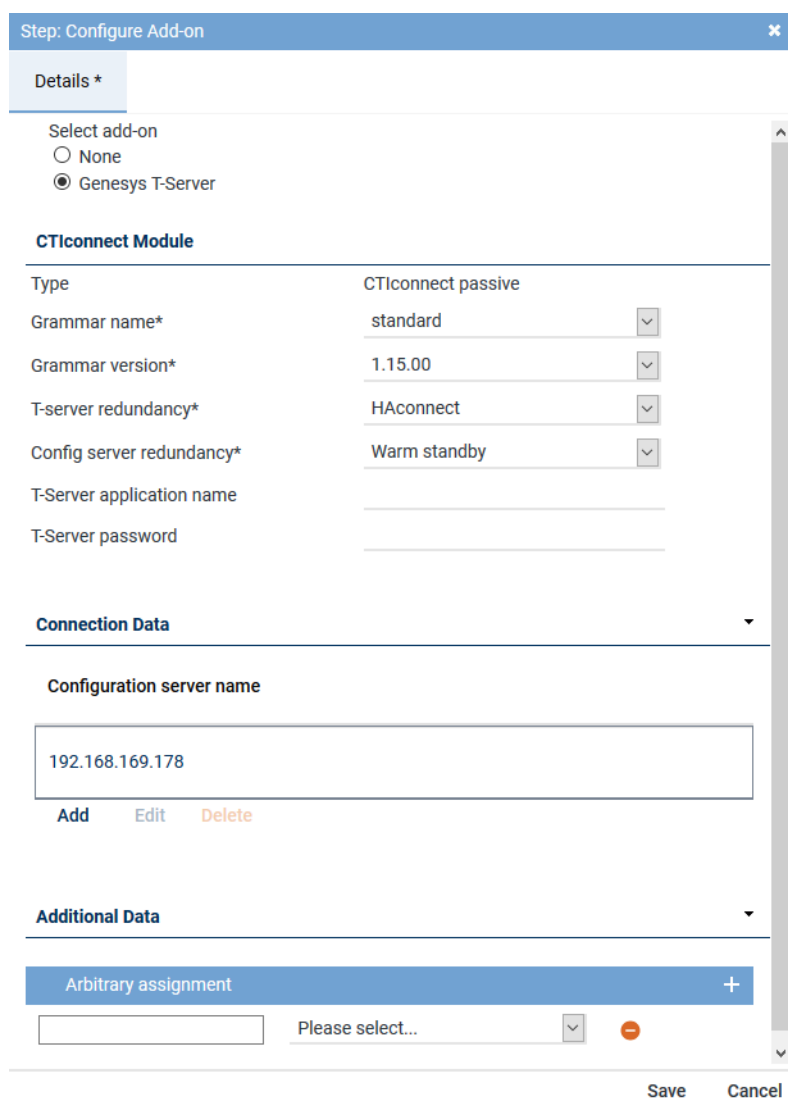


Fig. 94: Configure add-on for Genesys T-Server

### 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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. 25: 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:

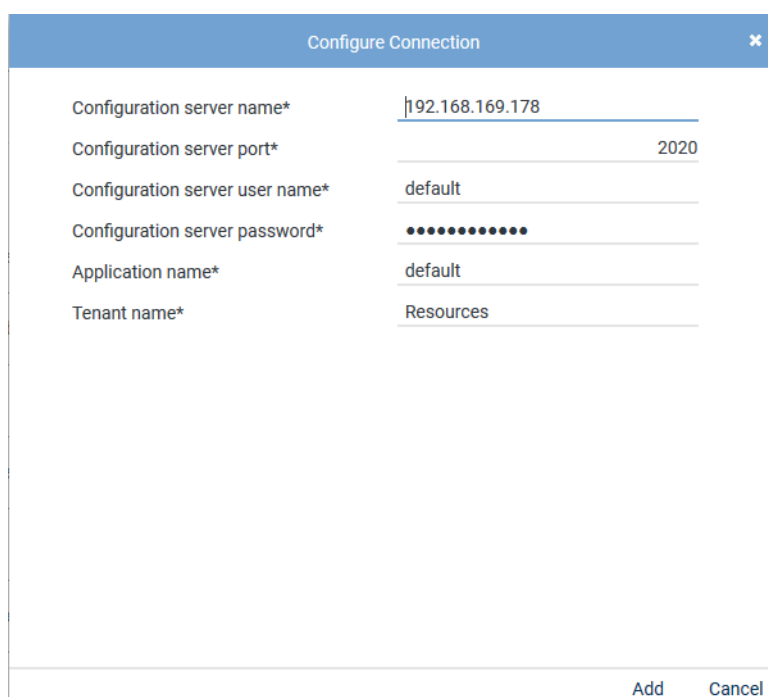


Fig. 95: Configure connection data

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. 26: 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.

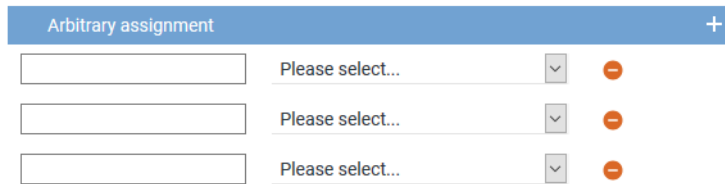



Fig. 96: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

### Configure miscellaneous settings

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

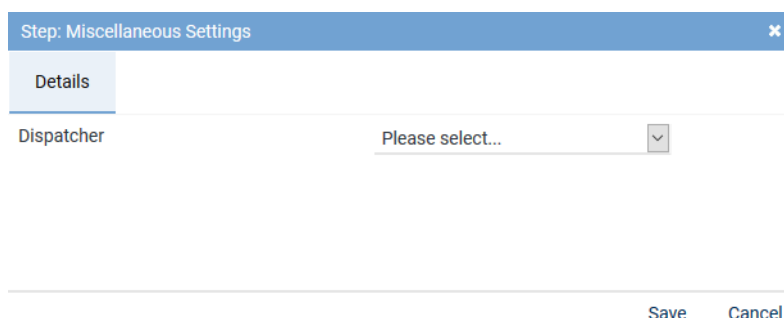


Fig. 97: Configure miscellaneous settings

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. 98: 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. 99: 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. 100: 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:

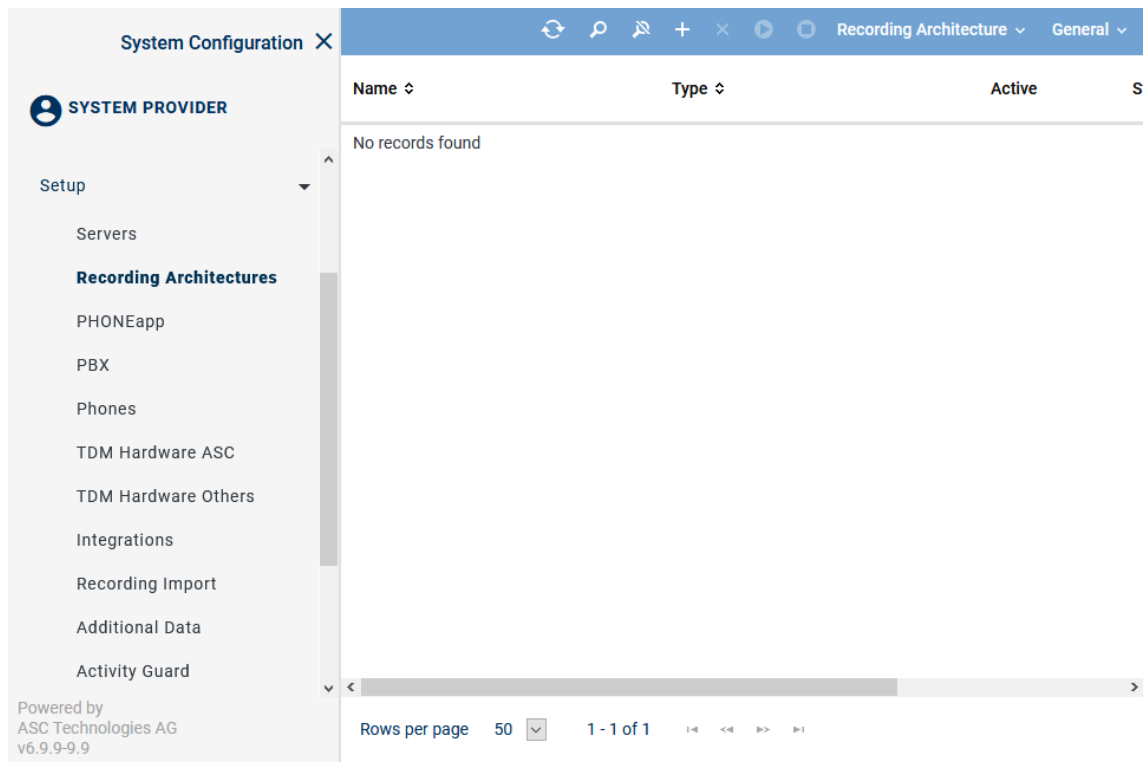




Fig. 101: Recording architectures - main view

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



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








### Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 102: Toolbar Recording Architectures module

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


		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. <b>NOTICE!</b> You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	Deactivates the selected recording architecture. <b>NOTICE!</b> You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
<i>Recording Architecture</i>	<i>Standby Management</i>	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

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

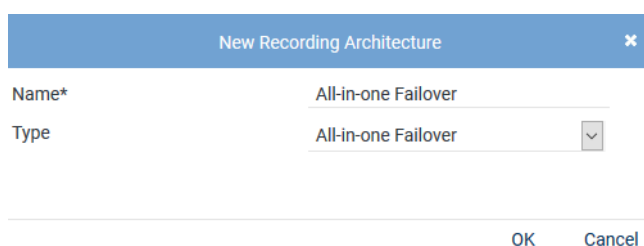


Fig. 103: Create recording architecture - All-in-one Failover

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




3. From the drop-down list *Type*, select the recording architecture type *All-in-one Failover*.  
**NOTICE!** The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.  
⇒ Your entries now appear in the detail view.

All-in-one Failover
All-in-one Failover X

Details\*

Server Assignment\*

 Help

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

Integration Type
⌵ ⌶

Name
No records found

Save


Reset

Fig. 104: 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. 450](#).

<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><b>NOTICE!</b> 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><b>NOTICE!</b> 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><b>NOTICE!</b> 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.

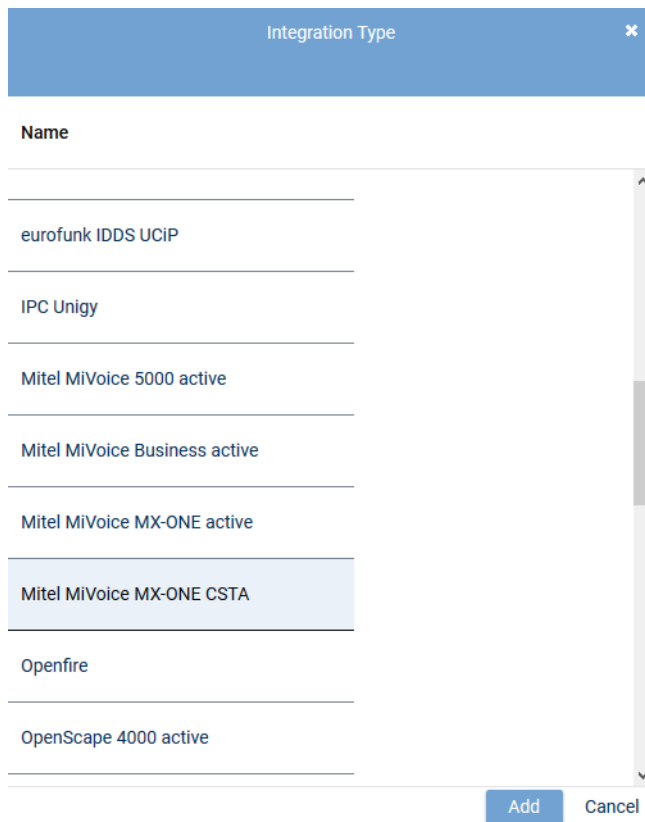


Fig. 105: Select integration type



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 server for All-in-one Failover Recording

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

All-in-one Failover
All-in-one Failover
×

Details\*

Server Assignment\*

Primary server\*

REC-01

+

-

Used in activated architecture

No

Standby server\*

REC-02

+

-

Used in activated architecture

No

Recording type  
☐ VoIP/Video  
☐ TDM  
☐ Screen  
☐ Chat

Save

Reset

Fig. 106: Recording Architecture - tab Server Assignment

2. 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:\	
<div>           Rows per page 20 <span>▼</span>           1 - 8 of 8           <span style="float: right;">             &lt;&lt; &lt; &gt; &gt;&gt;           </span> </div>			
			<div>Add Cancel</div>


Fig. 107: 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.

4. 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. 108: 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. 109: Recording architecture - activate recording architecture

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



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



For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See [chapter "Standby management for failover architectures"](#), p. 450.



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

### 7.3.2.2.2 Configure server

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

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

⇒ The following window appears:

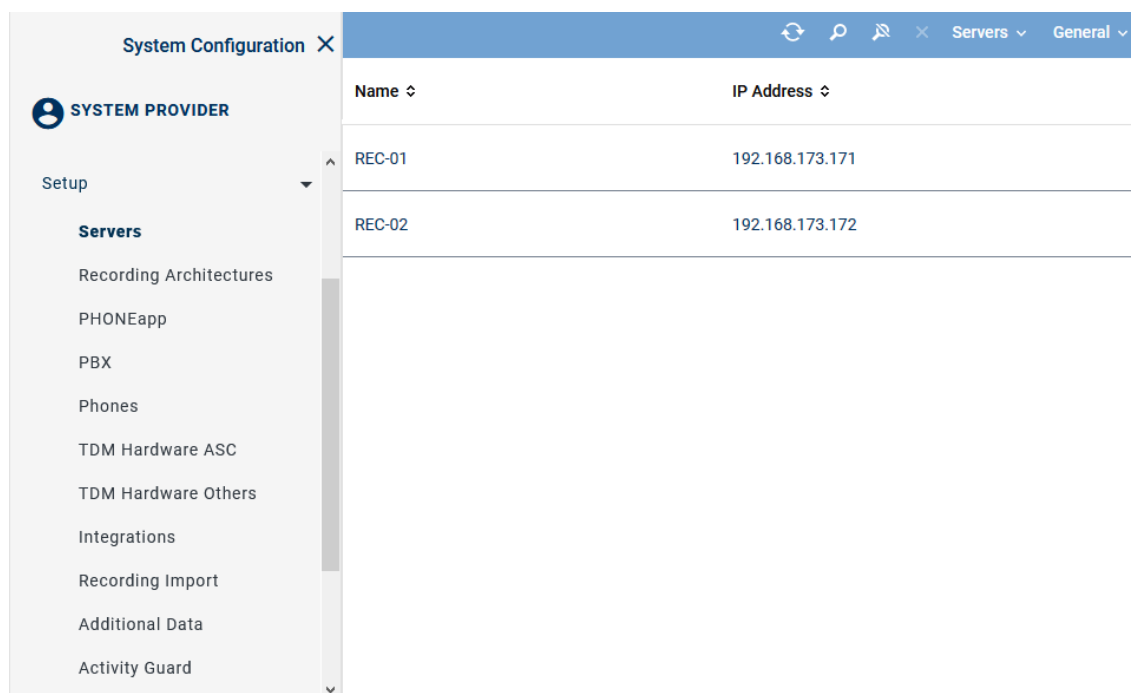


Fig. 110: Servers - main view

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

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

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

### Toolbar of the Servers module

The toolbar offers the following functions.

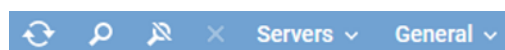








Fig. 111: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
		The icon  is displayed whenever the search has been adjusted by means of a filter.

	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 98</a> .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



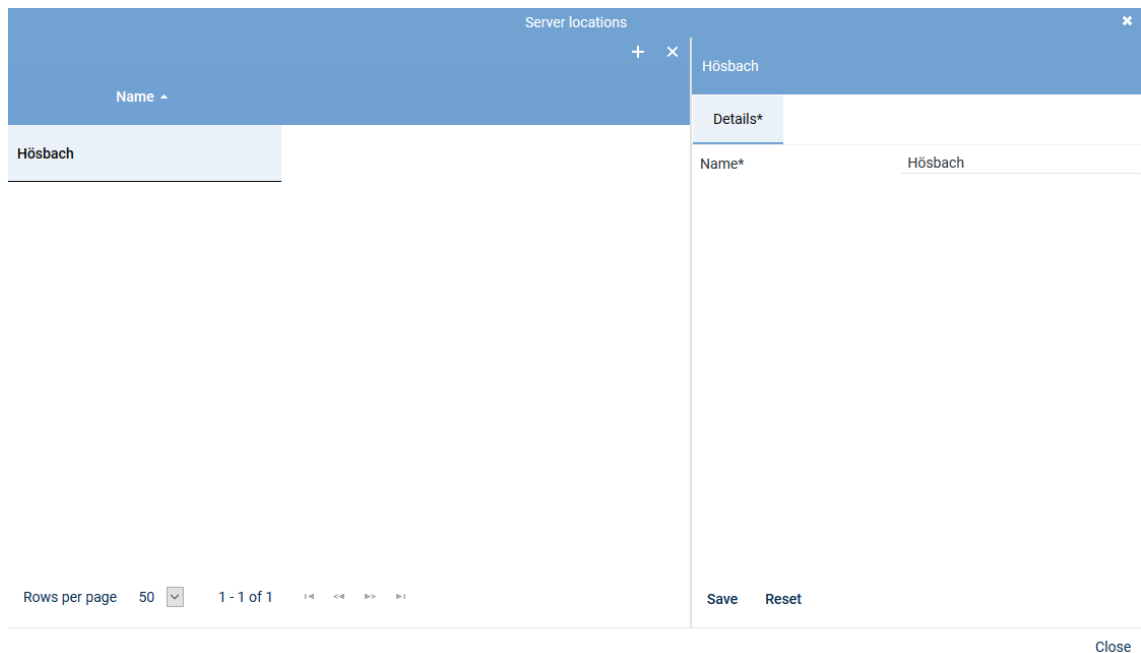
For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

### Administrate server locations

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


#### Add server locations

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. 112: Add server locations

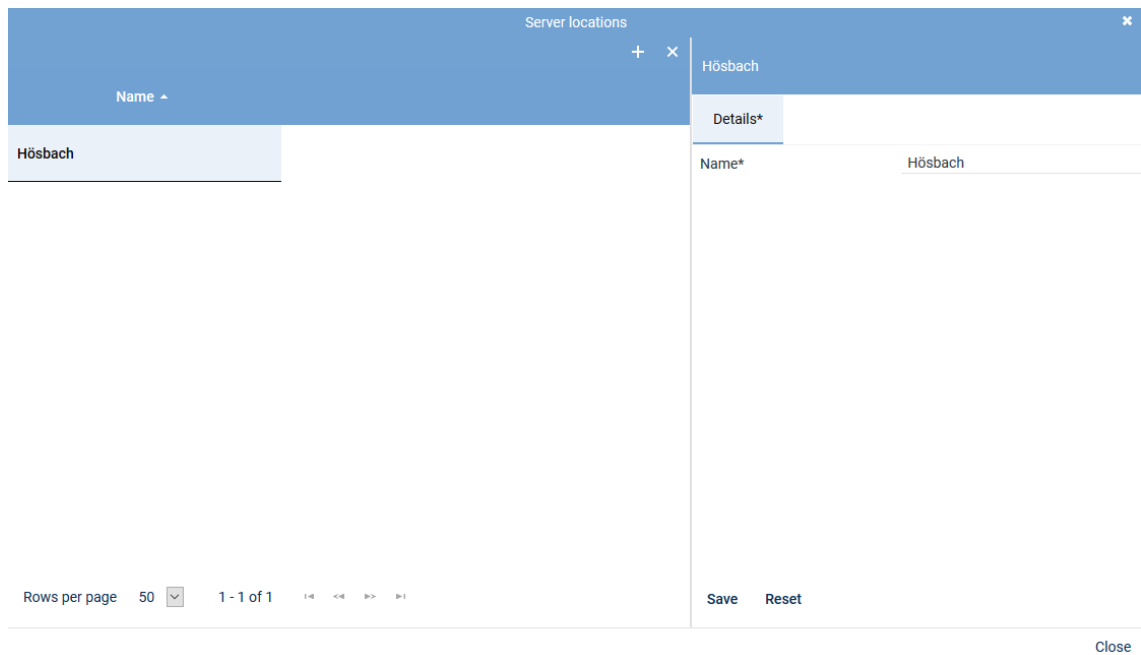
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

### Delete server location




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

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



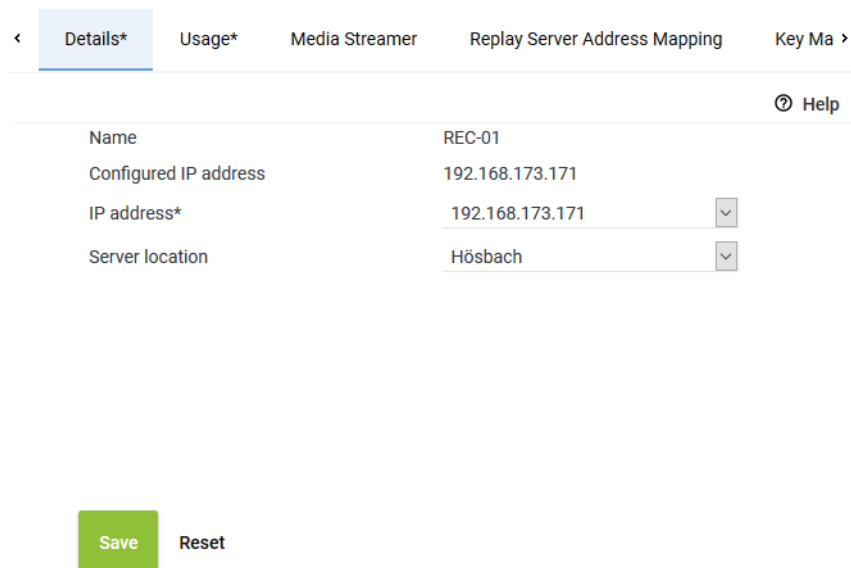
The screenshot shows a window titled "Server locations" with a close button (x) in the top right. Inside, there's a table with a header "Name" and a single row containing "Hösbach". To the right of the table is a "Details\*" tab. Below the table, there's a pagination bar showing "Rows per page 50" and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

Fig. 113: Delete server location



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

### Tab Details

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



The screenshot shows a window titled "Servers - tab Details" with a close button (x) in the top right. The window has a tabbed interface with "Details\*" selected. Below the tabs, there's a table 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 left, there are "Save" and "Reset" buttons. At the top right, there's a "Help" icon.

Fig. 114: Servers - tab Details

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



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

### Tab Usage

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



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

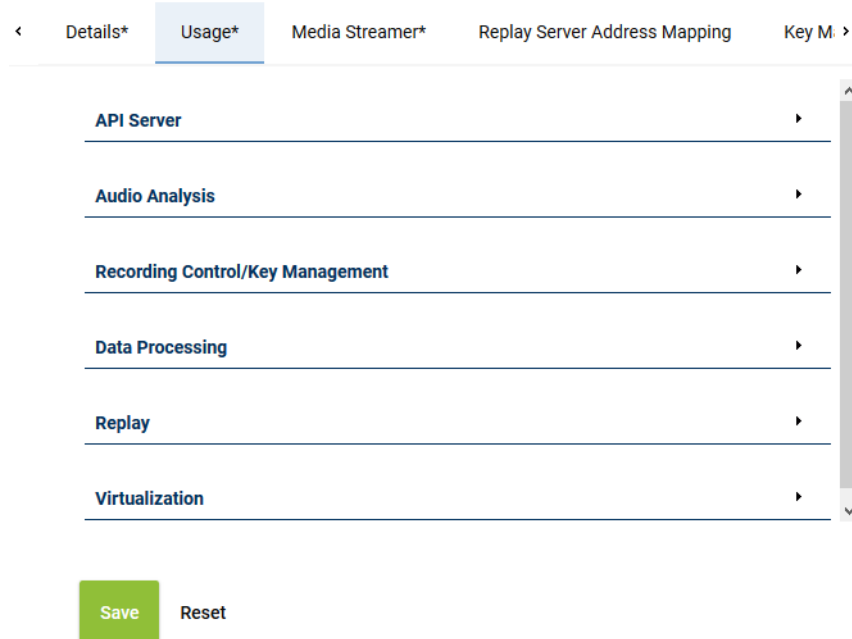


Fig. 115: Servers - tab usage

### Group field API Server

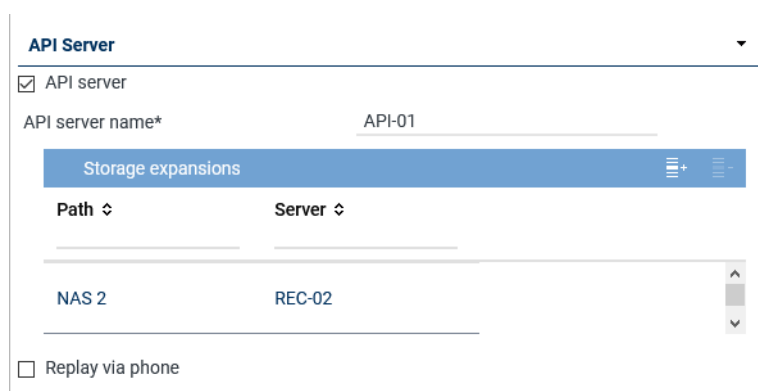




Fig. 116: Group field API Server

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


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

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

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

Parameter	Value/Description
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping"</a>, p. 112.</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"> <li>• By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay"</a>, p. 103.</li> <li>• By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul> <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><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWER<del>play</del> Pro</li> <li>• Application POWER<del>play</del> Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a <i>PBX</i>, see <a href="#">chapter "Tab Media Streamer"</a>, p. 110. To be able to do so, at least 1 <i>PBX</i> must have been configured in the system.</p>

### Add storage expansion for replay

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

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

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 117: Select storage expansion

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


### Group field Audio analysis

**Audio Analysis**

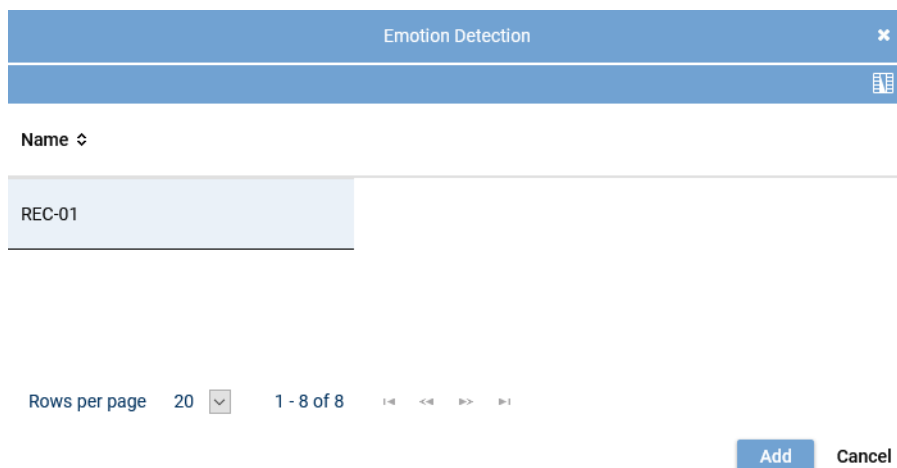
☒ Emotion detection

Stream audio data from\* REC-01 + -

Fig. 118: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis. <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function. <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> <li>Click on the button  to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 27: Configure audio analysis



Emotion Detection

Name ↕

REC-01
--------

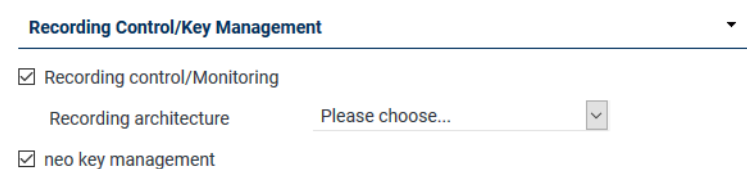
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 119: Select server for emotion detection

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

### Group field Recording Control/Key Management



Recording Control/Key Management

☒ Recording control/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 120: Group field Recording Control/Key Management

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

Tab. 28: Configure recording control/key management

### Group field Data Processing

**Data Processing** ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server

☒ Import

Recording architecture

Fig. 121: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 107</a>.</li> <li>By clicking on the icon  (Remove), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list"</a>, p. 107.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b> For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <li><i>Replay server</i> From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers.</li> </ul> <p><b>NOTICE!</b> For the export from <i>neo</i> to <i>neo</i>, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <li><i>Recording architecture</i> From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.</li> </ul>

Parameter	Value/Description
	<b>NOTICE!</b> If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 29: Data storage

### Add target server to a list

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



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

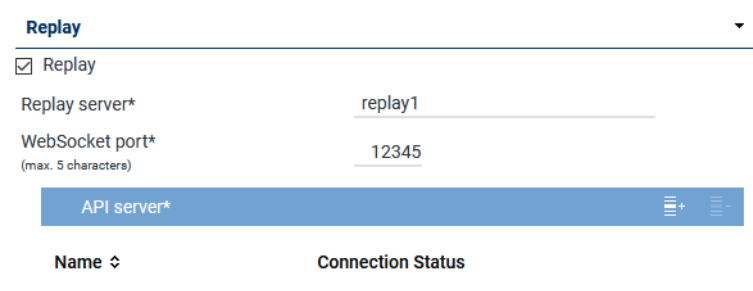
Fig. 122: Select server



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

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

### Group field Replay





**Replay**

☒ Replay

Replay server\*



WebSocket port\*   
(max. 5 characters)

API server\*  

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

Fig. 123: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API</a> 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 <a href="#">POWERplay</a> Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>• By clicking on the icon  (<i>Add</i>), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 108.</li> <li>• By clicking on the icon  (<i>Remove</i>), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 30: 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. 124: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 101](#).

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. 125: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> </ul>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li><i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 31: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

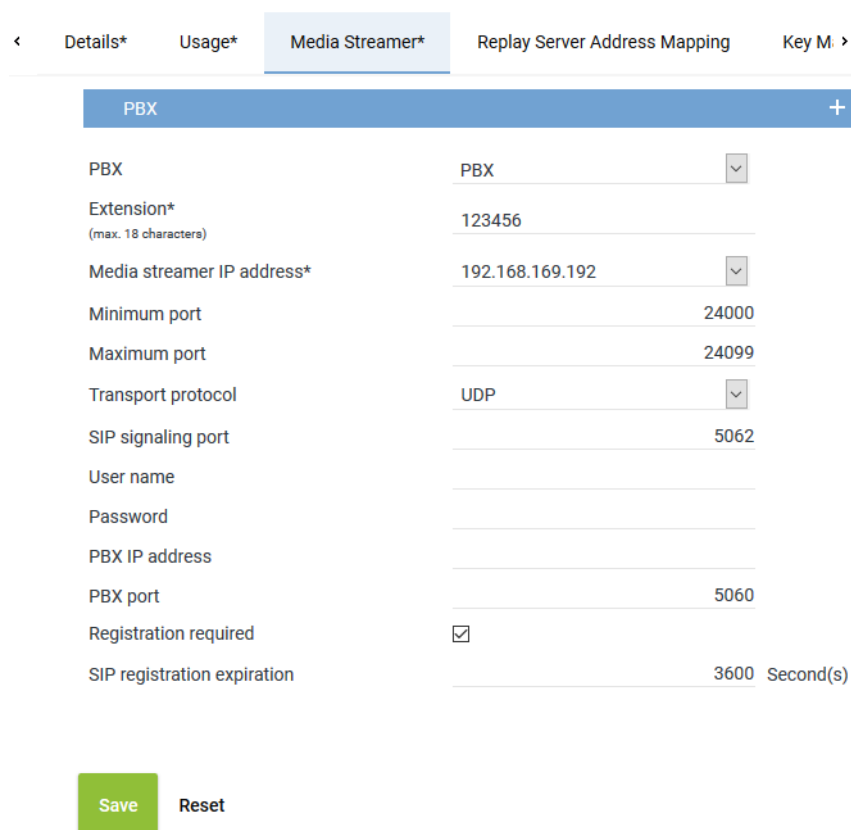
### Tab Media Streamer

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

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



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



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

PBX +

PBX	PBX	▼
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. 126: Servers module - tab Media Streamer

- Enter the following parameters:

<b>PBX</b>	<b>PBX</b> that the Media Streamer is supposed to be mapped to. Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.
------------	--

	<p>If no PBX has been created in the system yet, you can create a <a href="#">PBX</a> via the blue bar <i>PBX</i>, see <a href="#">chapter "Create PBX"</a>, p. 116.</p>
<i>Extension</i>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <i>8000</i>.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <a href="#">SIP</a> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p> <p><b>NOTICE! The port range must not have less than 64 ports.</b></p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the <a href="#">SIP</a> communication.</p> <p><a href="#">TCP</a> = unencrypted  <a href="#">UDP</a> = unencrypted  <a href="#">TLS</a> = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the <a href="#">SIP</a> communication.</p> <p>Port for data exchange: <i>5062</i></p>
<i>User name</i>	Enter the user name for the authentication on the <a href="#">SIP</a> server.
<i>Password</i>	Enter the password for the authentication on the <a href="#">SIP</a> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<i>PBX port</i>	<p>Enter the port of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the value <i>5060</i>.</p>
<i>Registration required</i>	<p>Select whether the <a href="#">SIP</a> extension has to be registered with the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p><input checked="" type="checkbox"/> = <a href="#">SIP</a> extension has to be registered.  <input type="checkbox"/> = <a href="#">SIP</a> extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

### Tab Replay Server Address Mapping

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

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



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

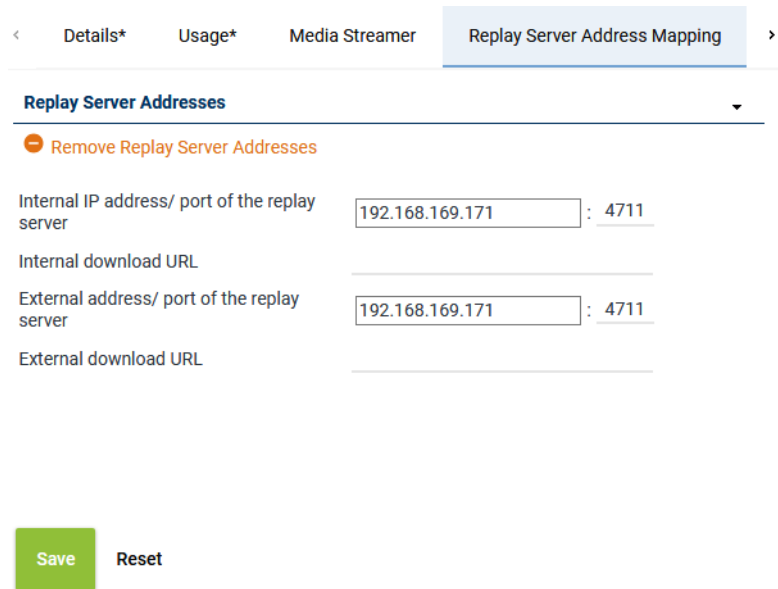


Fig. 127: Servers Module - tab Replay Server Address Mapping

### Group field Replay Server Addresses

1. Enter the following parameters

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

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



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

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



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



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

### Tab Key Management

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

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

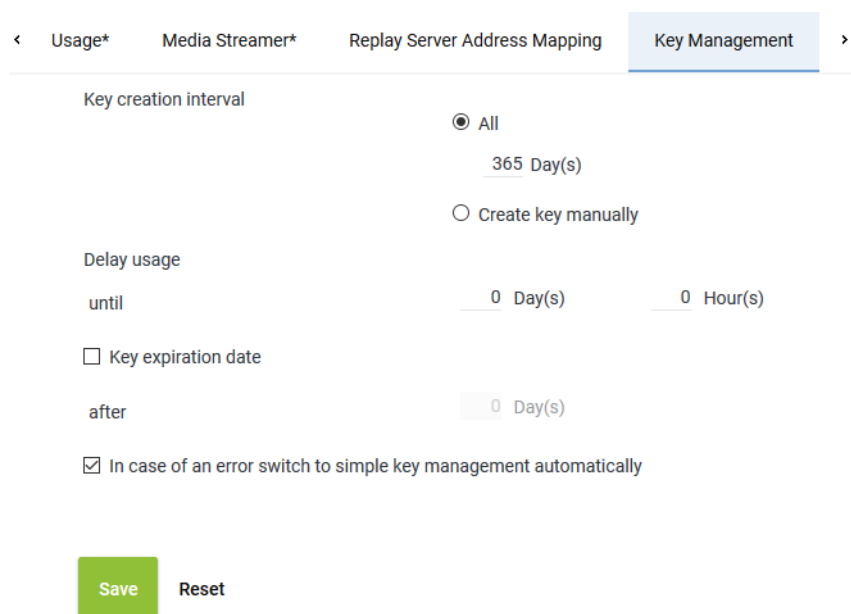


Fig. 128: Servers module - tab Key Management

#### Key creation interval

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

- *All*

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

Possible time interval: 1 to 365 days

Default value: 365 days

- *Create key manually*

Select that a key is supposed to be generated manually.

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

<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*

In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.

- *ASC License Management System*

**NOTICE! License Management does not support encryption.**

**For licensing, there are the following options:**

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.

In this case, no separate configuration is required.

- *Trusted Virtualization License*

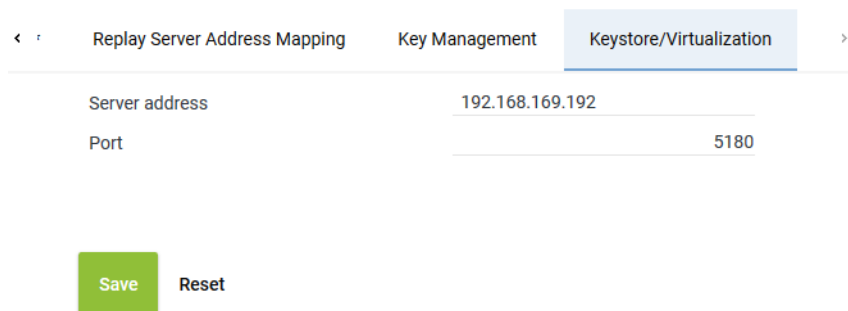
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



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

Fig. 129: Servers module - tab Keystore/Virtualization

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

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	Enter the port for the connection. 5180 = Dongle Manager 8181 = ASC License Management System



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

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

### 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:

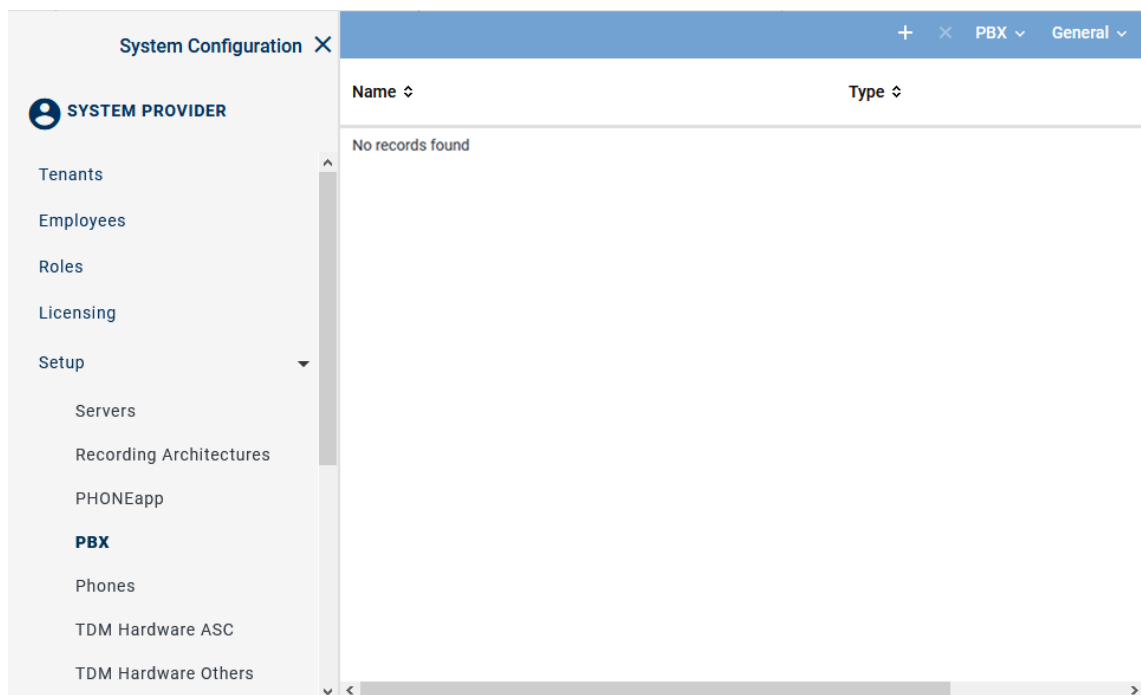


Fig. 130: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

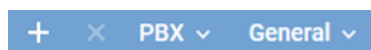




Fig. 131: Toolbar PBX module

	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.




<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Create new PBX

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

×

< 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. 132: 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 <a href="#">PBX</a> 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"> <li><i>Select from list</i> Select the country code from the drop-down list.</li> <li><i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka 094.</li> </ul>
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. 32: 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

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

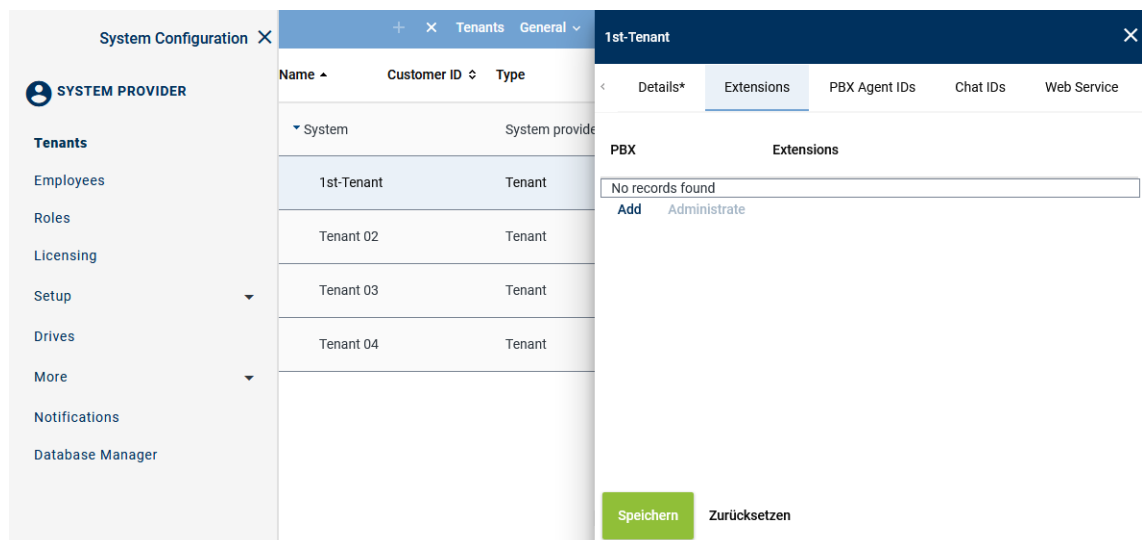


Fig. 133: Tenants - main view - tab Extensions

##### 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. 134: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>ZIP</li> <li>TXT</li> <li>CSV</li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>Click on the button <span style="background-color: #f0f0f0; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>Click on the button <i>Choose File</i>.</li> <li>Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>Click on the button <span style="background-color: #4a86e8; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34

120 / 489

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

Enter country codes as number ranges as follows:  
+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions*

Activate the check box to replace the list of extensions.

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

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

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

### Remove extensions

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

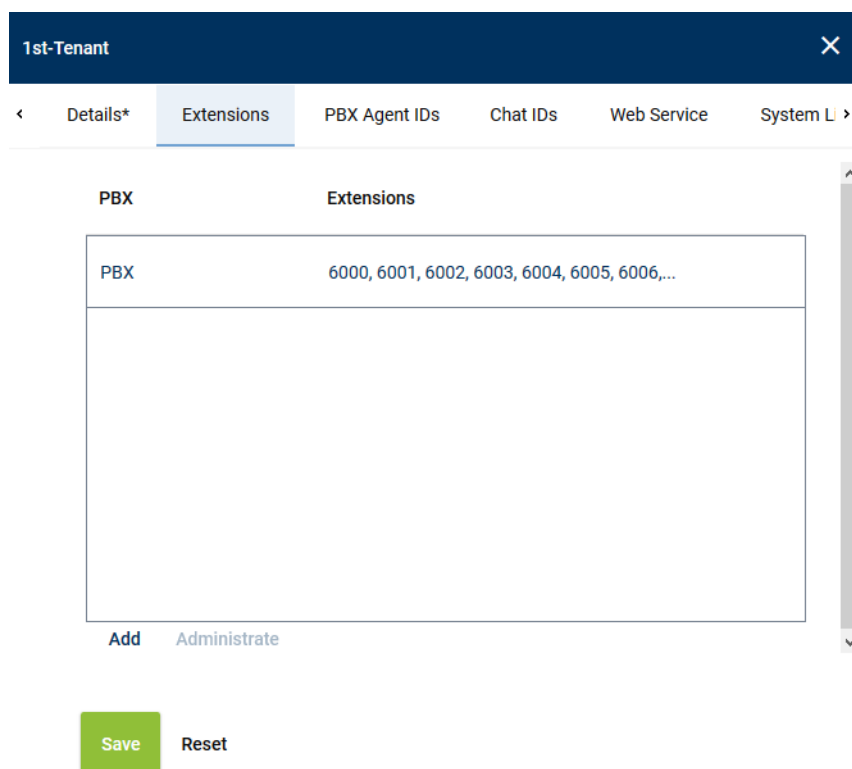


Fig. 135: Remove extensions

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. 136: 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.

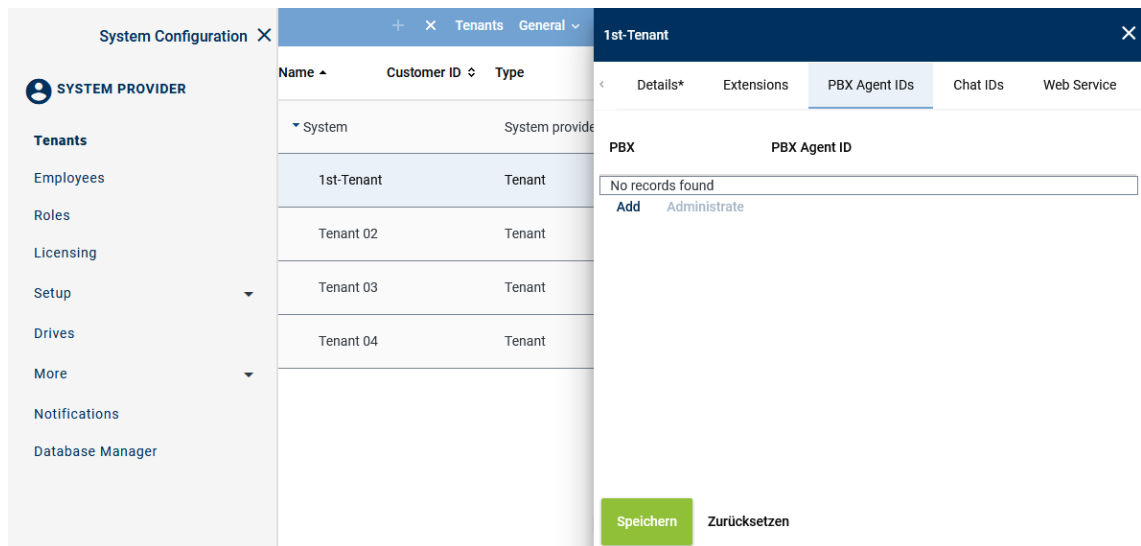
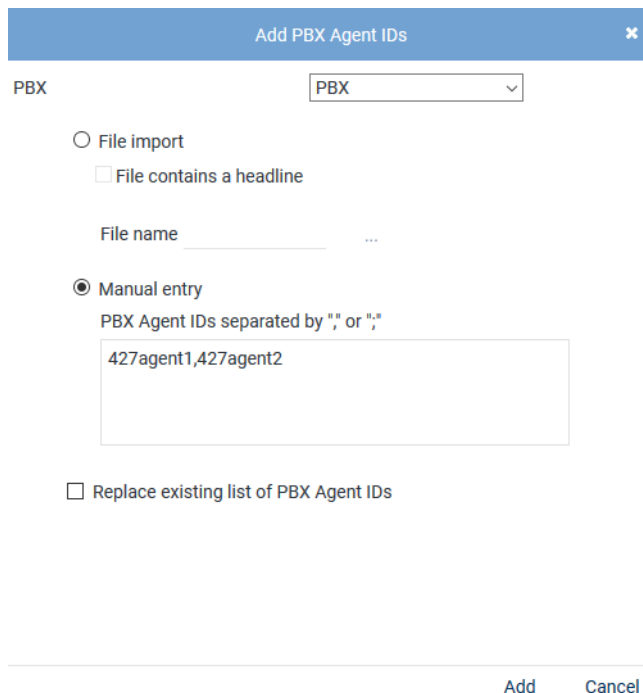


Fig. 137: Tenants - main view - tab PBX Agent ID

### 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:



The dialog box 'Add PBX Agent IDs' has a dropdown menu set to 'PBX'. It offers two options: 'File import' (with a sub-option 'File contains a headline') and 'Manual entry' (selected). The 'Manual entry' section has a text input field containing '427agent1,427agent2'. A checkbox 'Replace existing list of PBX Agent IDs' is at the bottom. 'Add' and 'Cancel' buttons are at the bottom right.

Fig. 138: 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 the option to import PBX Agent IDs from an existing <a href="#">CSV</a> 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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>Upload File</b>.</li> </ul>
<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><b>NOTICE! Wildcards cannot be used!</b></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. 139: 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.

**System Configuration** ✕

**SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 140: 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. 141: 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. 142: 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:

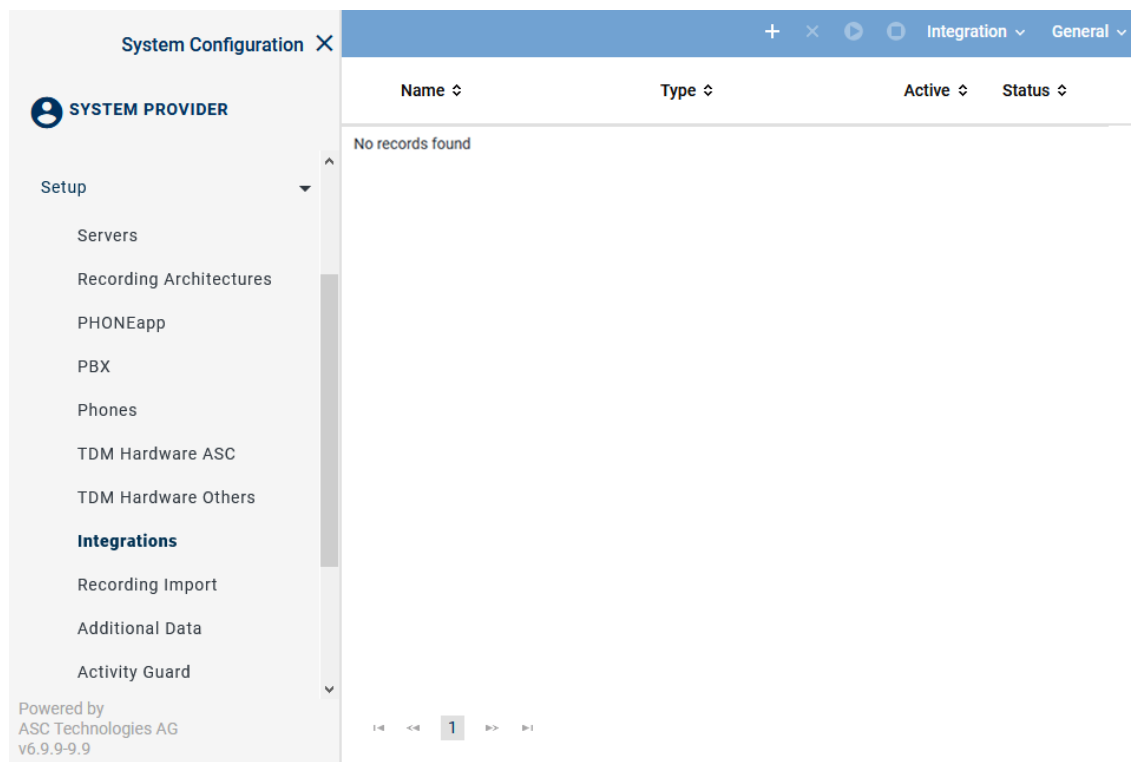




Fig. 143: Integrations - main view

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



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



### Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 144: Toolbar Integrations module

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

	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

- 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.

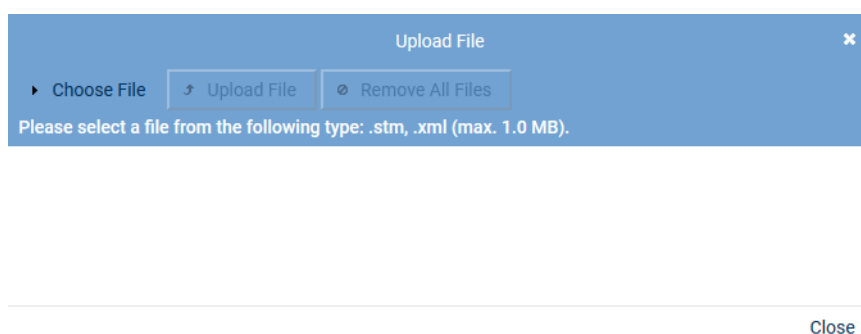


Fig. 145: Choose file

- 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*.

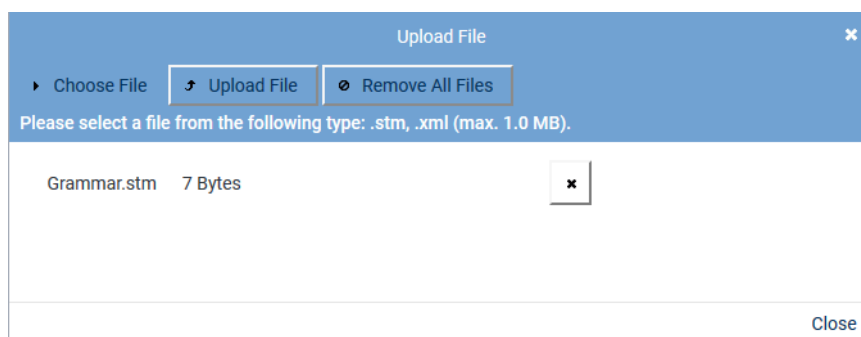



Fig. 146: Upload grammar

- 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. 147: Create integration type

- Enter the following parameters:

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

Tab. 33: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

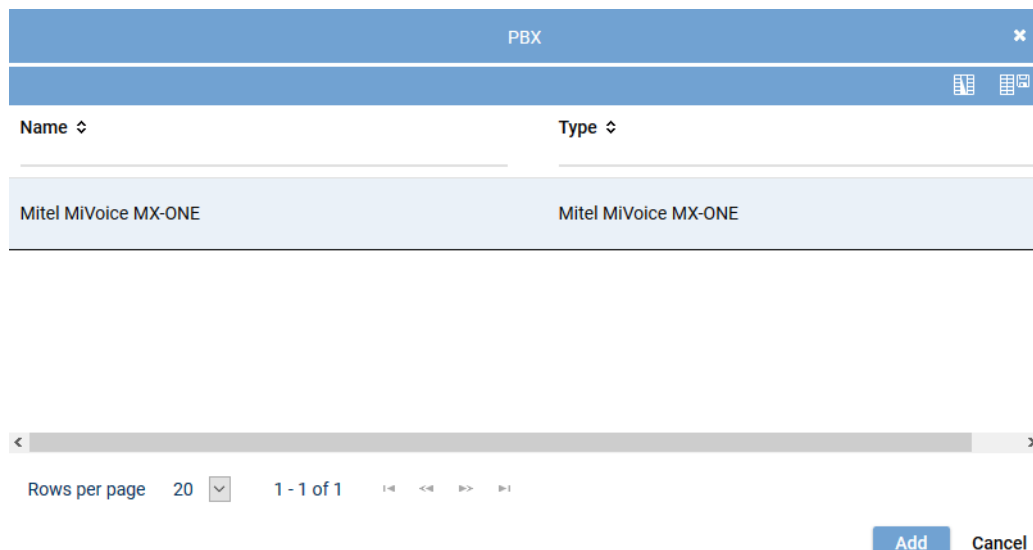


Fig. 148: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

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

- In the detail view on the bottom right, click on the button *Next*.

⇒ The tab *Recording Architecture* appears.

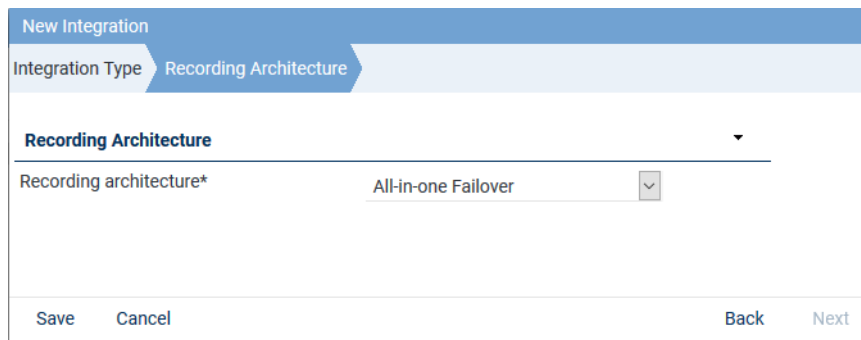


Fig. 149: Assign recording architecture - All-in-one Failover


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. 150: 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. 151: Configuration step - Configure Recording Architecture

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

### Configure CTI connection data

1. 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab *MiVoice MX-ONE (CSTA)*

By configuring the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

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

1. Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\*
MBG\*

CTIconnect Module

Connection Data

Additional Data

Failover waiting time*	10
Failover repetitions*	3
Regular expression for phone type identification*	<code>^[A-Za-z]*\s[0-9]{4}[a-zA-Z]?\$ ^[0-9]{4}[a-zA-Z]?\$ ^DBC[0-9]{5}\$</code>

Save
Cancel

Fig. 152: CTI connection data - tab MiVoice MX-ONE (CSTA)



Following an update, you must configure this section 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. 153: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 34: 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 MiVoice MX-ONE (CSTA)

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



In case, the connection to the CTI<sup>connect</sup> 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. 154: 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.

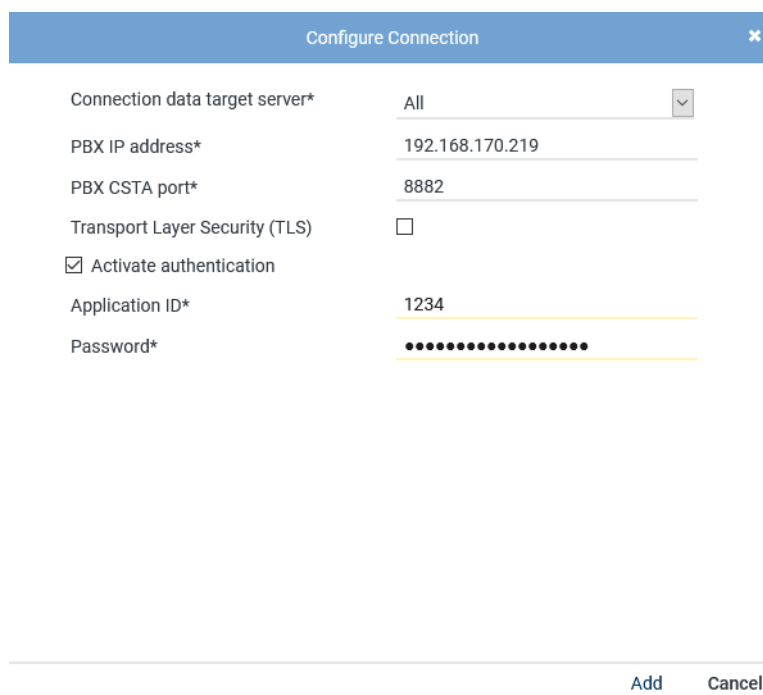


Fig. 155: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the <a href="#">CSTA</a> connection is supposed to run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate this check box to use the connection with <a href="#">TLS</a> .
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14</a> .
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14</a> .

Parameter	Value/Description
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 35: Configure connection data

- 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.

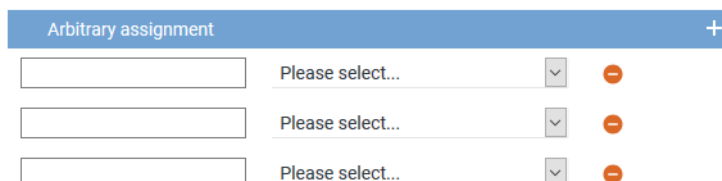



Fig. 156: Arbitrary assignment of the additional data

The following additional data is always available:

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

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

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



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



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

### Configure 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 CTIconnect 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. 157: Configure switching conditions

<b>Failover waiting time</b>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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.
<b>Failover repetitions</b>	Enter how many times the CTI <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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]?$|^\\s[0-9]{4}[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 158: 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.



As parallel recording is only possible via the **MBG**, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

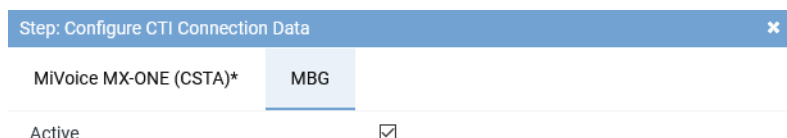


Fig. 159: Activate CTIconnect connection data for [MBG](#)

**Active** Activate the check box to display the configuration parameters and to activate the connection to the [MBG](#).

☒ = Connection has been activated.

☐ = Connection has not been activated.



Following an update, you must configure this section again.

### Group field CTIconnect Module

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

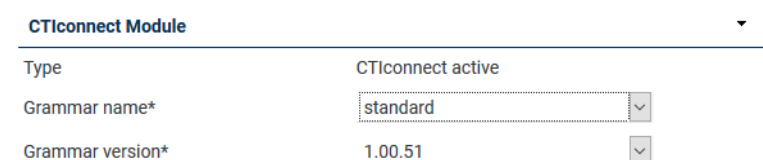


Fig. 160: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 36: Configure CTIconnect module



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 MBG

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

**Connection Data** ▼

---

Connection data

No records found

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

Fig. 161: Group field Connection Data

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

Configure Connection
✕

Connection data*	192.168.170.116
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>
<input checked="" type="checkbox"/> Use pre-shared key	
Pre-shared key (PSK)*	●●●●●●●●

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

Fig. 162: Configure connection

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the <a href="#">MBG</a> .
<i>PBX port</i>	Enter the port for the <a href="#">MBG</a> or the <a href="#">SRC</a> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <a href="#">MBG</a> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 37: 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.

### Group field Additional Data MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

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.

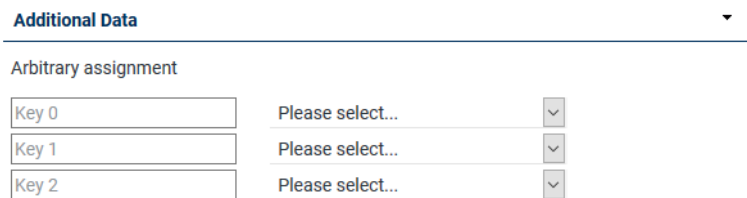



Fig. 163: CTI connection data - additional data module 1

2. Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
3. From the drop-down list, select the entry which is supposed to appear as column headline in the players.
4. Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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.

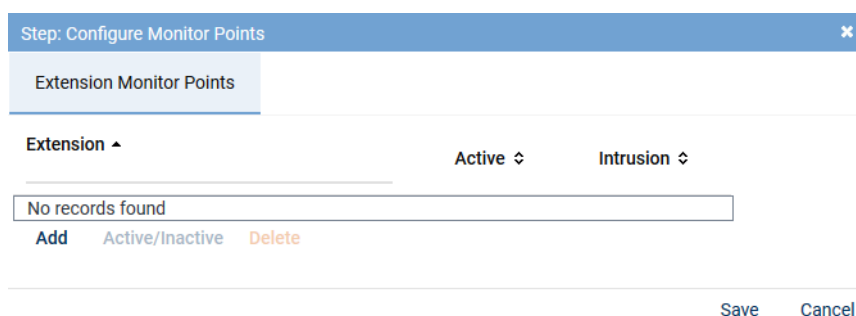


Fig. 164: Configuration step - configure monitor points

### Tab 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.

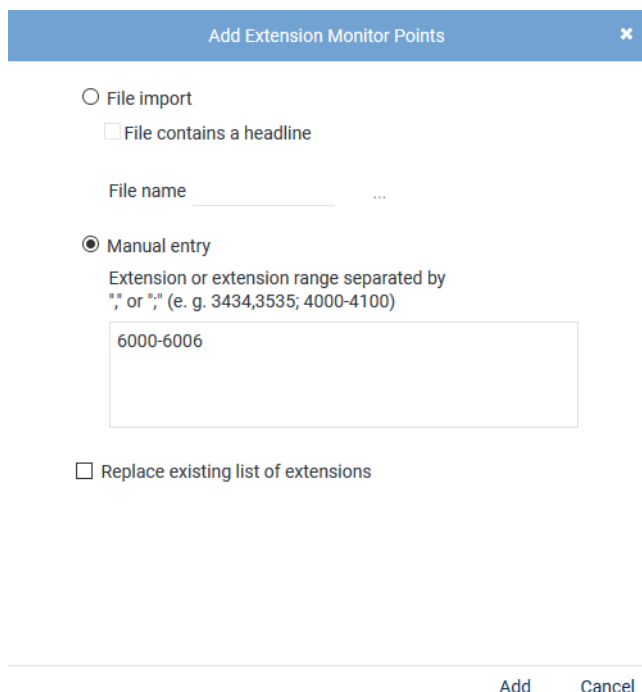






Fig. 165: Add extension monitor points

<b>File import</b>	<p>Select this option to import extensions from an existing <a href="#">CSV</a> 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"> <li>• Click on the button  behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  (<i>Upload file</i>).</li> </ul>
<b>File contains a headline</b>	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <a href="#">CSV</a> file may not contain more than 1 column. If commas or other column delimiters are found in the <a href="#">CSV</a> 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 <a href="#">CVS</a> file, you have to pack it in a ZIP file.</p>
<b>File name</b>	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button  behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  (<i>Upload file</i>).</li> </ul>
<b>Manual entry</b>	<p>Select this option to enter extensions or extension ranges manually.</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. You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.

**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 <span>✕</span>		
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 href="#">Add</a> <a href="#">Active/Inactive</a> <a href="#">Delete</a>		
<a href="#">Save</a> <a href="#">Cancel</a>		

Fig. 166: Configured extension monitor points

<b>Add</b>	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.
<b>Active/Inactive</b>	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.
<b>Delete</b>	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.
<b>Intrusion</b>	<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. 16](#).

### Global recording settings

- Click on the button  (*Edit configuration step*) in the line *Global recording settings* in the main view.
 

⇒ The window *Step: Global Recording Settings* appears.

Step: Global Recording Settings

Details\*

Transport protocol	UDP	
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. 167: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i>, the transport protocol applies for the SIP communication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
<i>Port SIP signaling</i>	Enter the port for SIP signaling that is opened on the recording server for incoming SIP communication and that has been selected in the outgoing SIP notifications as the port of the recording server. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by SIP to start <i>active-stream recording</i> . Default 7300.
<i>Activate SIP authentication</i>	Activate the check box if 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 SIP registration of extensions recorded with 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 SIP registration of extensions recorded with 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. 38: Global recording settings

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



Following an update, you must configure this section 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	REC-01
Server Name	<div>Details*</div> <div>Extensions</div>
REC-01	<div>Recording Module Active MX-ONE <input checked="" type="checkbox"/></div> <div>Configured IP address 192.168.173.171</div> <div>IP address of the recording server* 192.168.173.171 <input type="text"/></div> <div>Minimum port* 20000</div> <div>Maximum port* 21000</div>

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 168: 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 <b>RTP</b> data from the recording server, e. g. <b>20000</b> .
<i>Maximum port</i>	Enter the highest port configured on the PBX that is used to receive the <b>RTP</b> data from the recording server, e. g. <b>21000</b> .

Tab. 39: 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.



Following an update, you must configure this section 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*.

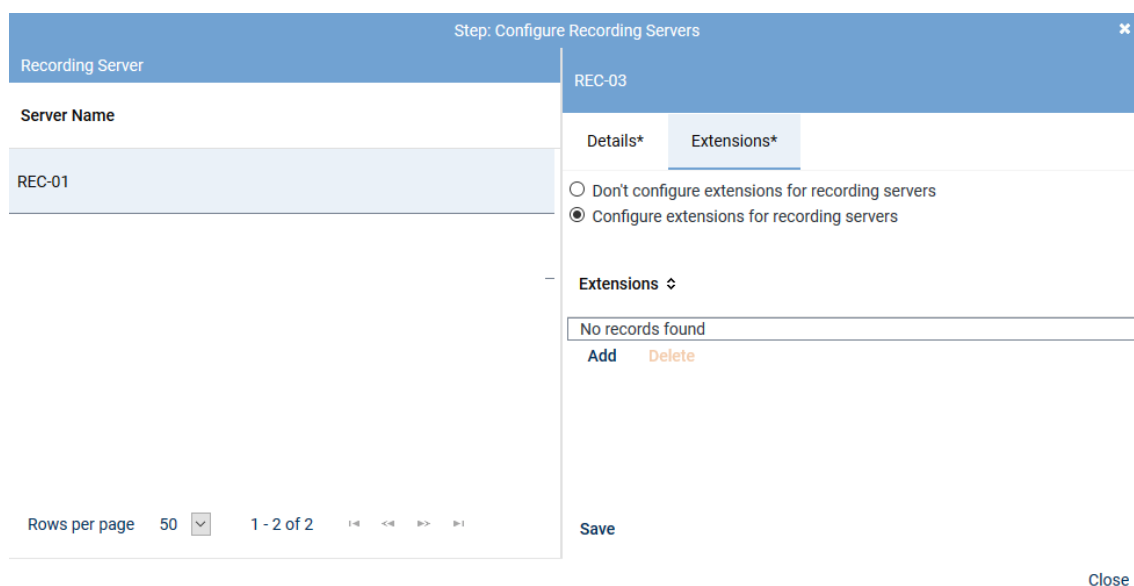


Fig. 169: Tab Extensions

**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.

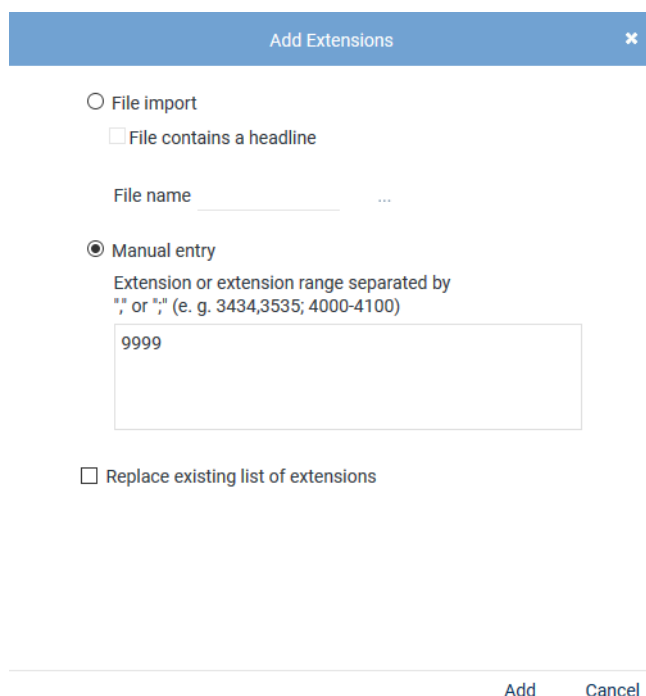


Fig. 170: Add extensions

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.

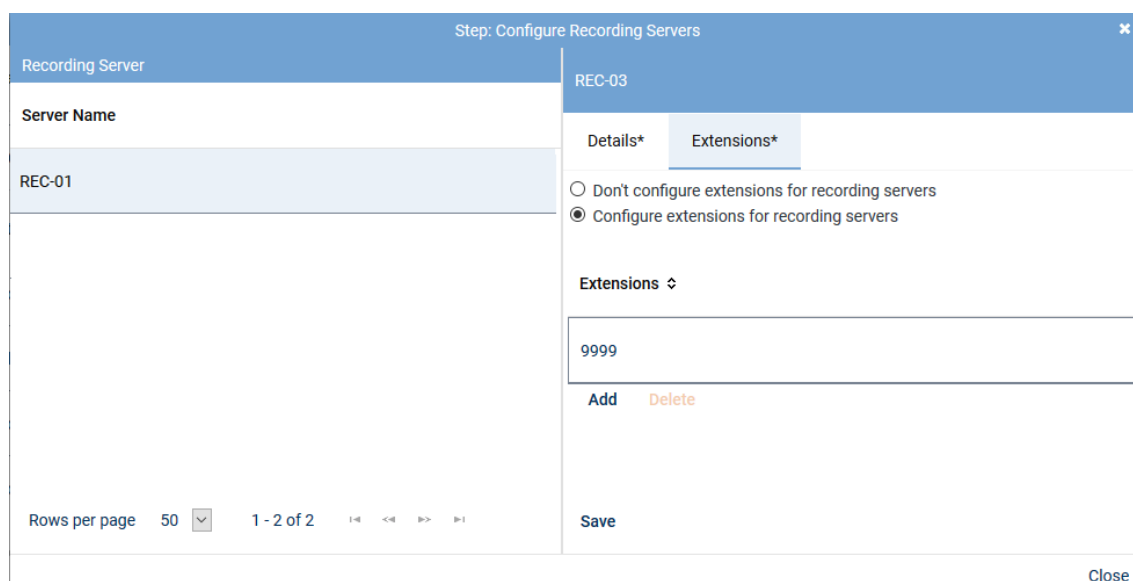



Fig. 171: Added extensions

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

### Configure recording servers

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

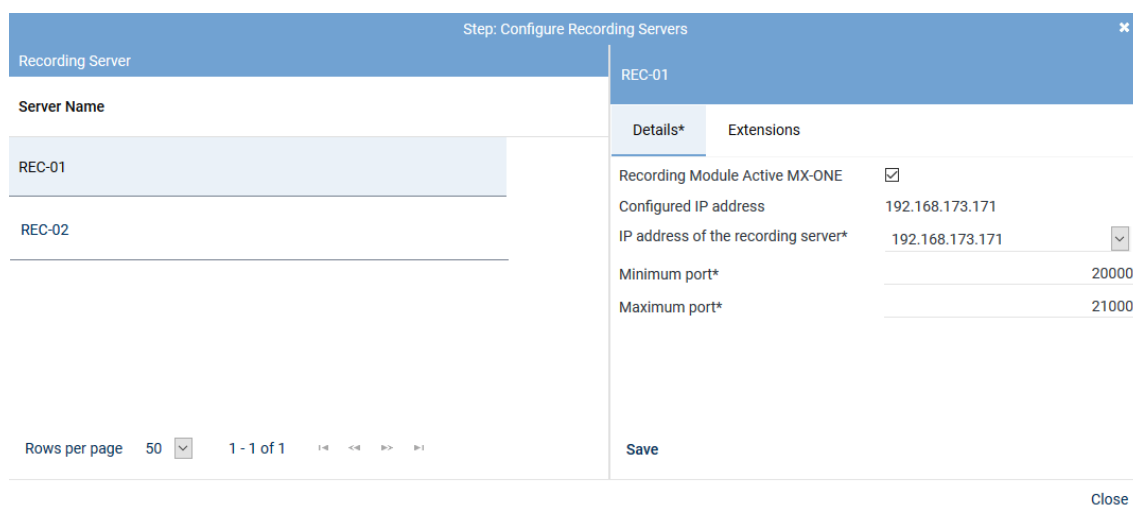


Fig. 172: Configuration step - Configure recording servers

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.

Parameter	Value/Description
<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 <b>RTP</b> 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 <b>RTP</b> data from the recording server, e. g. 21000.

Tab. 40: 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.



Following an update, you must configure this section 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*.

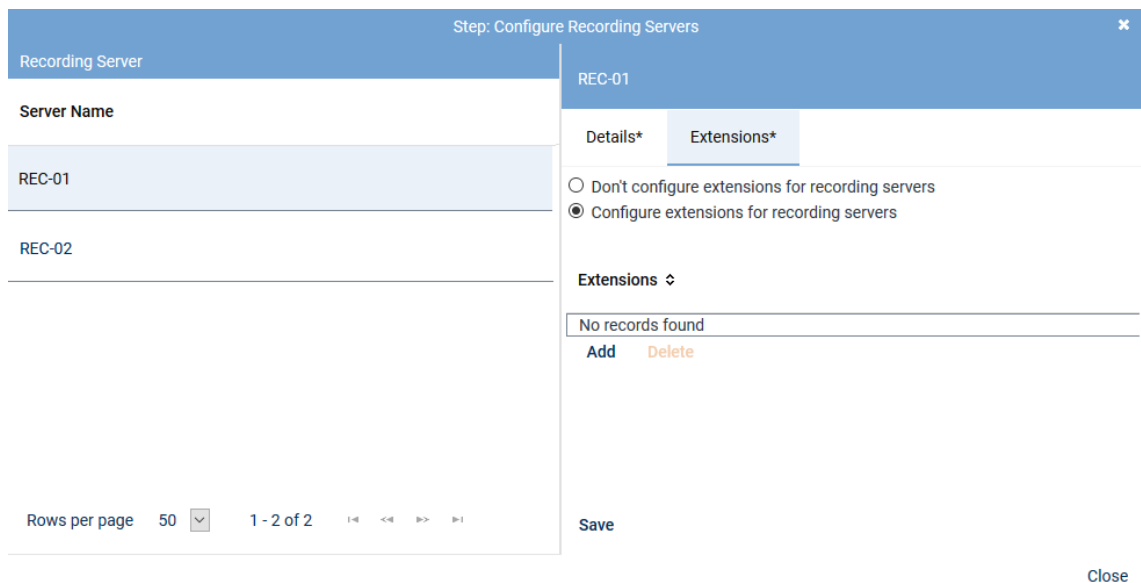


Fig. 173: Tab Extensions

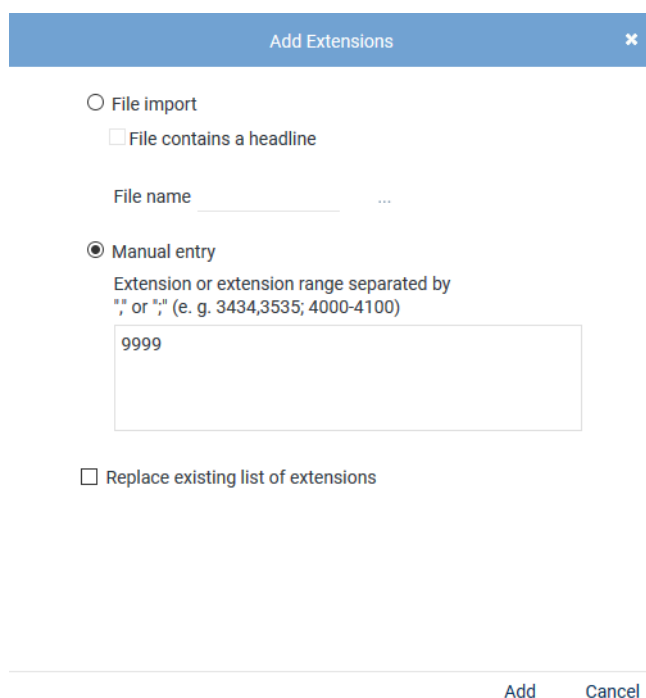
**Configure extensions of the recording server** Activate this option if you would like to configure extensions for the recording server so make the feature call intrusion work.

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.

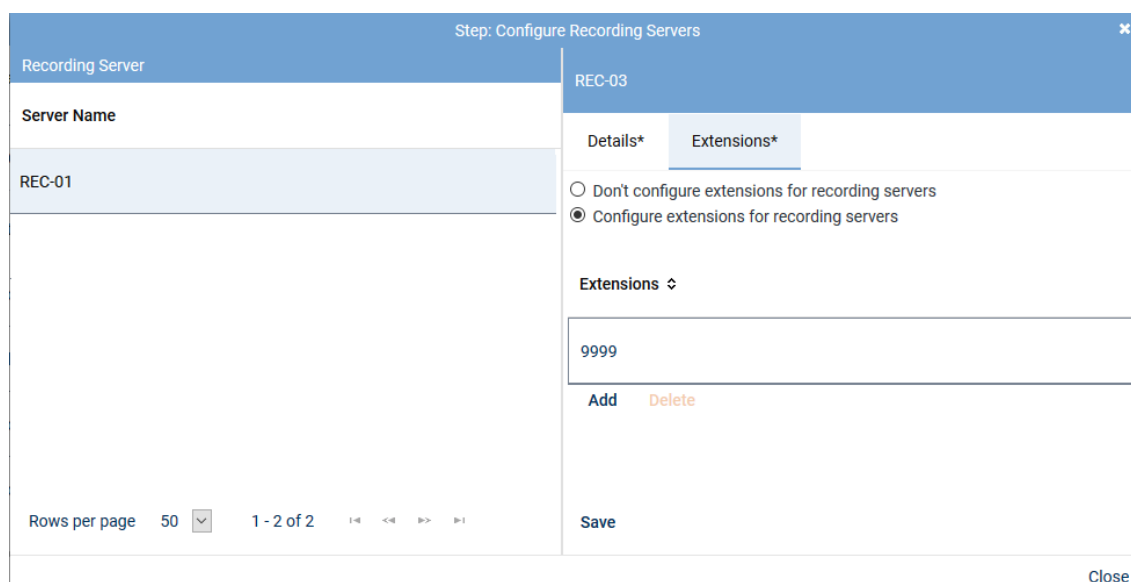
2. To add extensions, click on the button *Add* in the table *Extensions*.  
⇒ The window *Add Extensions* appears.



The **Add Extensions** dialog box has a title bar with a close button. It contains two radio buttons: **File import** and **Manual entry**. The **Manual entry** option is selected. Under **File import**, there is a checkbox for **File contains a headline** and a text field for **File name**. Under **Manual entry**, there is a text field for **Extension or extension range separated by " " or ";" (e. g. 3434,3535; 4000-4100)** containing the value **9999**. At the bottom, there is a checkbox for **Replace existing list of extensions**. At the bottom right, there are **Add** and **Cancel** buttons.

Fig. 174: 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.



The **Step: Configure Recording Servers** window has a title bar with a close button. It features a table with the following structure:

Recording Server	
Server Name	REC-03
REC-01	<div> <div>Details*</div> <div>Extensions*</div> </div> <div> <input type="radio"/> Don't configure extensions for recording servers  <input checked="" type="radio"/> Configure extensions for recording servers         </div> <div>           Extensions ▾           <div>9999</div> <div>Add Delete</div> </div>

At the bottom left, there is a **Rows per page** dropdown set to 50 and a pagination indicator **1 - 2 of 2**. At the bottom right, there is a **Save** button and a **Close** button.

Fig. 175: 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.



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

#### **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. 176: 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	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 41: 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. 42: 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.

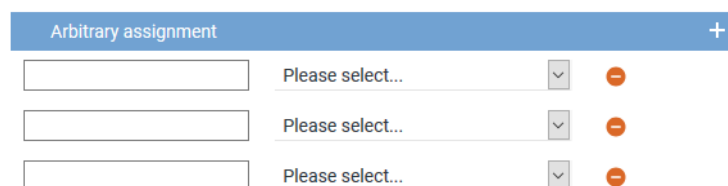



Fig. 177: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*

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

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



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



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

### **Configure add-on for 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<sup>connect</sup> 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

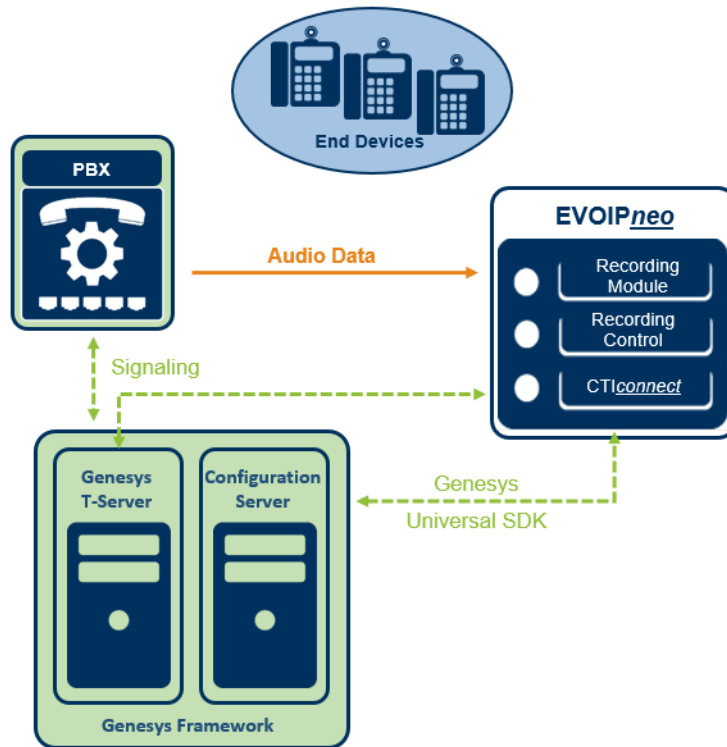


Fig. 178: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

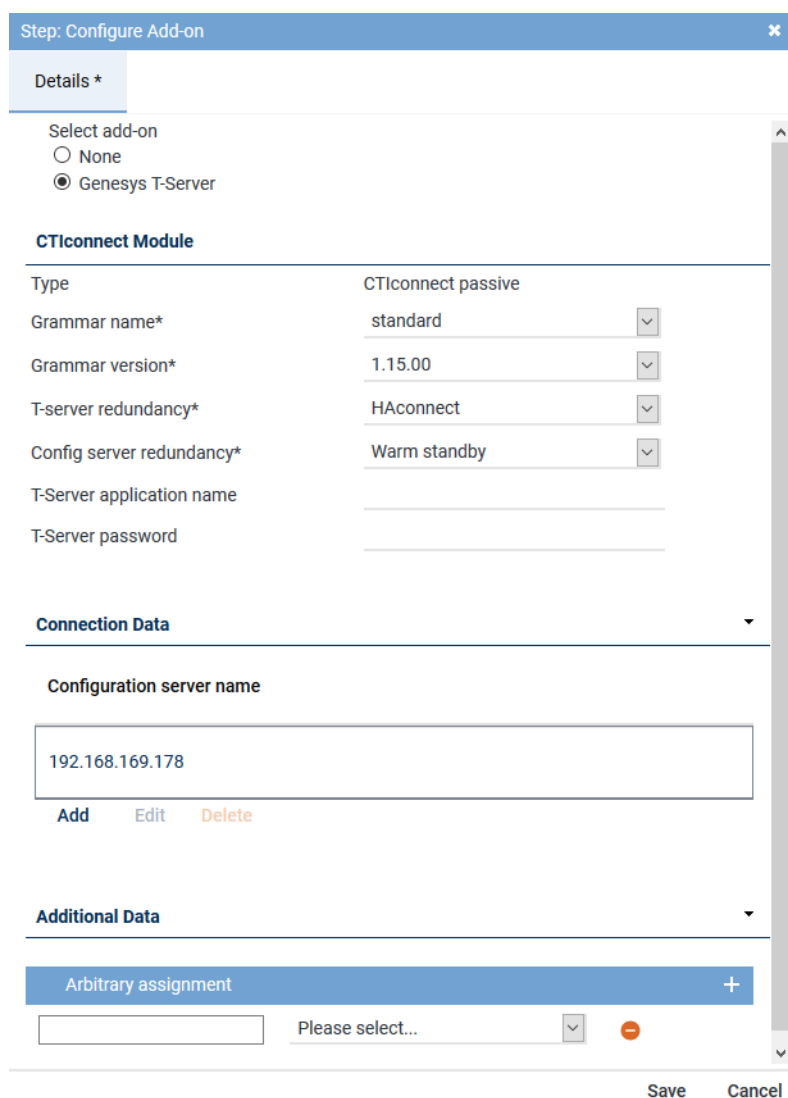


Fig. 179: Configure add-on for Genesys T-Server

### 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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. 43: 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:

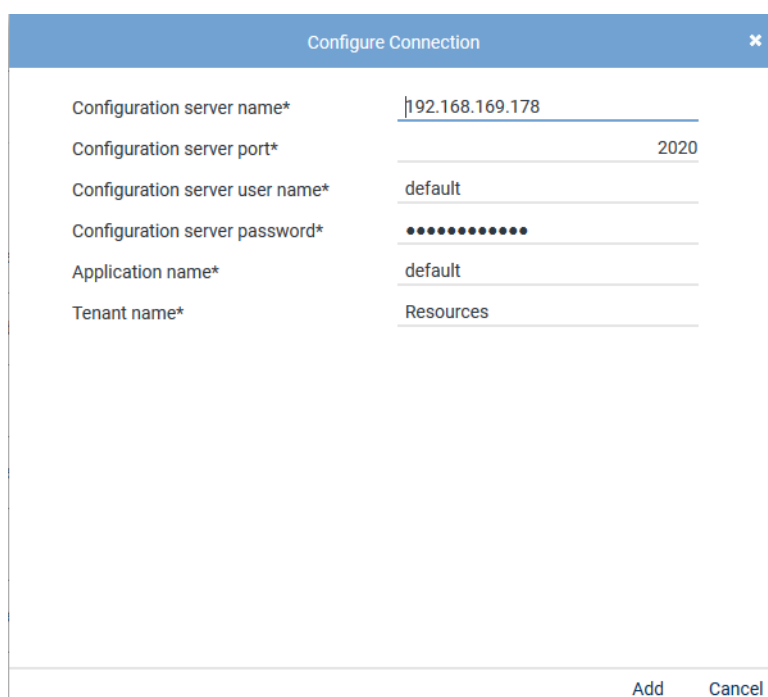


Fig. 180: Configure connection data

- 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. 44: 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. 181: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

### Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

▼

Save

Cancel

Fig. 182: 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. 183: 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. 184: 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. 185: Deactivate integration

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

### 7.3.2.3 Configure recording solution All-in-one Parallel 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:

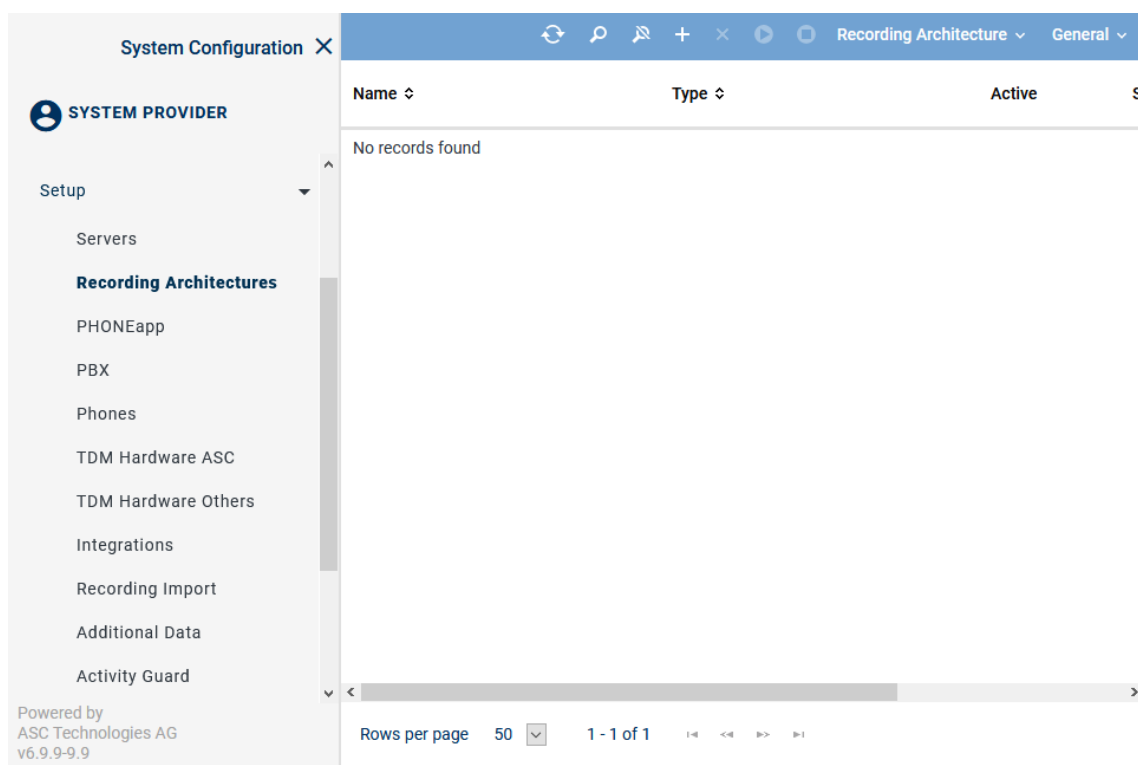




Fig. 186: Recording architectures - main view

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



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








### Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 187: Toolbar Recording Architectures module

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


		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. <b>NOTICE!</b> You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	Deactivates the selected recording architecture. <b>NOTICE!</b> You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
<i>Recording Architecture</i>	<i>Standby Management</i>	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Create recording architecture All-in-one Parallel Recording

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

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

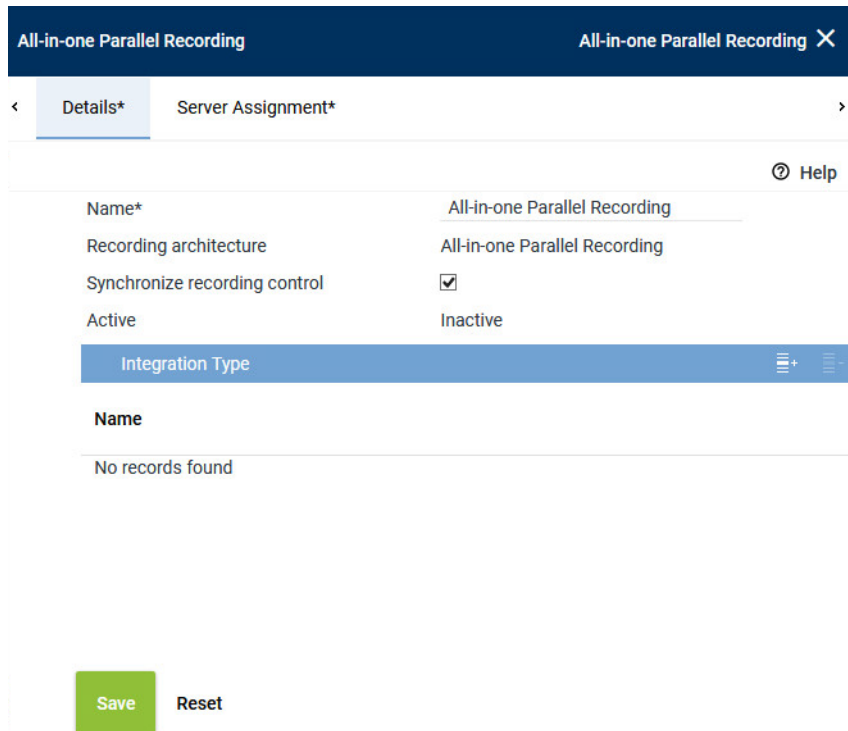
⇒ The window *New Recording Architecture* appears.



Fig. 188: Create recording architecture - All-in-one Parallel Recording

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

3. From the drop-down list *Type*, select the recording architecture type *All-in-one Parallel Recording*.  
**NOTICE!** The drop-down list only displays the supported recording architecture types.
4. Click on the button *OK*.  
⇒ Your entries now appear in the detail view.



The screenshot shows a configuration window titled 'All-in-one Parallel Recording'. It has two tabs: 'Details\*' (selected) and 'Server Assignment\*'. The 'Details\*' tab contains the following fields:

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

Below these fields is a section titled 'Integration Type' with a blue header bar. Under this section is a 'Name' field and a message 'No records found'. At the bottom of the window are two buttons: 'Save' (green) and 'Reset' (grey).


Fig. 189: Recording architecture - tab Details - All-in-one Parallel Recording

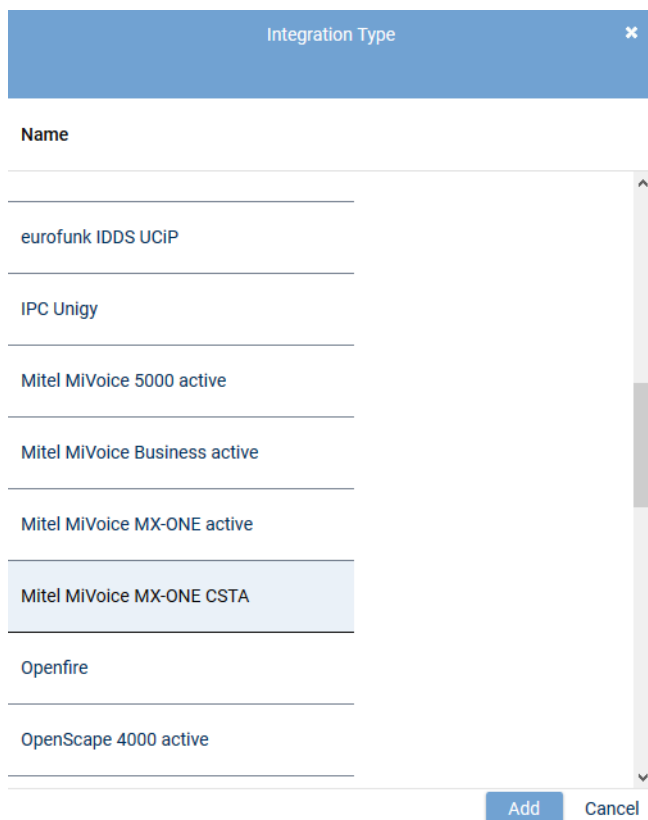
5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see [chapter "Synchronization of recording control", p. 442](#).

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

If you do not want to synchronize recording control, you can configure duplicate detection, see [chapter "Duplicates in parallel recording architectures", p. 445](#).

### 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" entry is currently selected.

Fig. 190: Select integration type



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

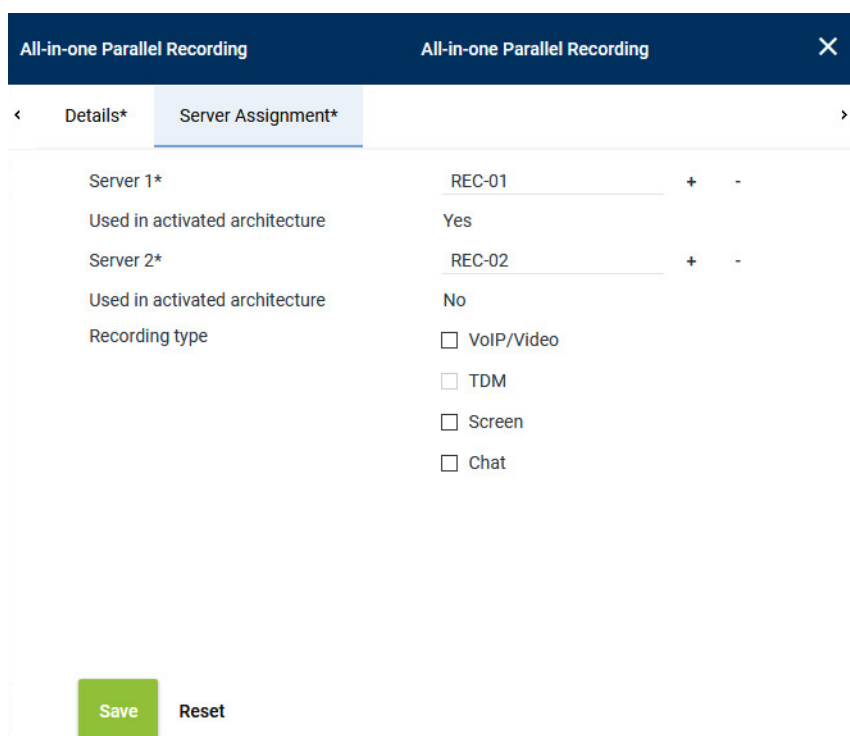


Any number of integration types can be assigned to a recording architecture.

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 Parallel Recording**

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



All-in-one Parallel Recording		All-in-one Parallel Recording	
<div> <div>Details*</div> <div>Server Assignment*</div> </div>			
Server 1*	REC-01	+	-
Used in activated architecture	Yes		
Server 2*	REC-02	+	-
Used in activated architecture	No		
Recording type	<input type="checkbox"/> VoIP/Video <input type="checkbox"/> TDM <input type="checkbox"/> Screen <input type="checkbox"/> Chat		
<div> <div>Save</div> <div>Reset</div> </div>			

Fig. 191: Recording Architecture - tab Server Assignment

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



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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 192: Recording Architecture - assign server - example

- Select *Server 1*.




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

- Click on the button *Add*.



⇒ The name of the server now appears in the detail view.

5. To delete an assignment, click on the button .
6. Repeat the steps and select Server 2 for the entry field *Server 2*.
7. Select the recording type you would like to use for these servers by activating the check box.

Recording type

☒ VoIP/Video

☒ TDM

☒ Screen

☒ Chat




Fig. 193: Recording Architecture - activate recording type

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



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

### Activate recording architecture

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










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

Fig. 194: Activate recording architecture

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



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



Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see [chapter "Configure duplicate detection", p. 446](#).



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

### 7.3.2.3.2 Configure server

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

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

⇒ The following window appears:

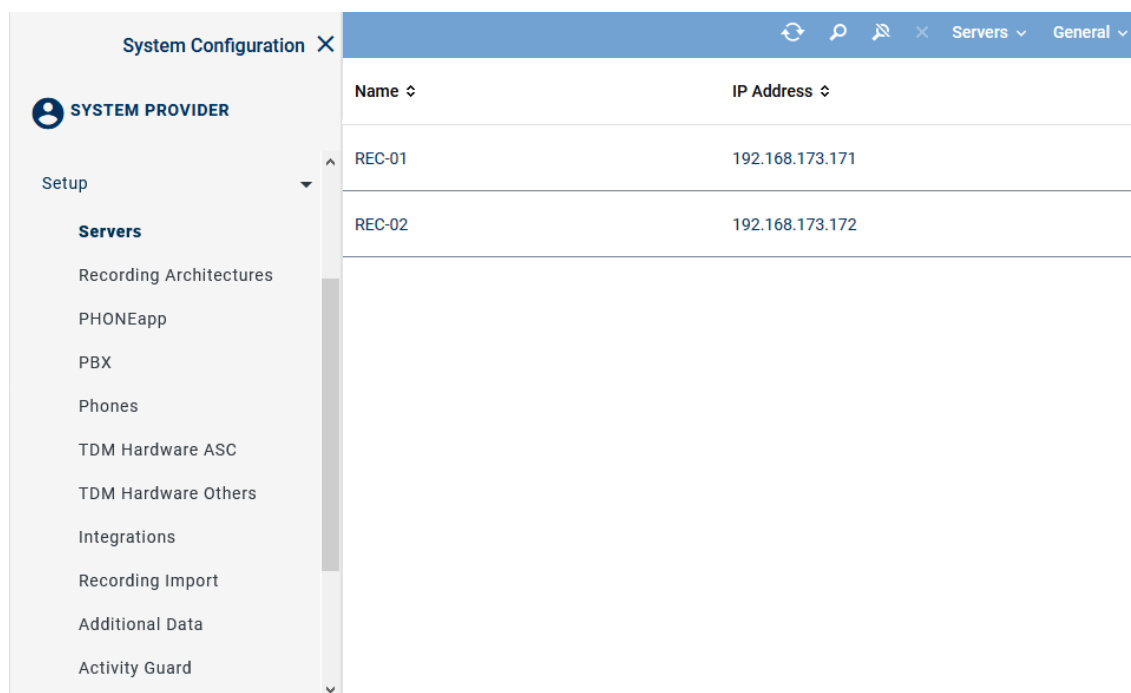


Fig. 195: Servers - main view

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

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

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

#### Toolbar of the Servers module

The toolbar offers the following functions.

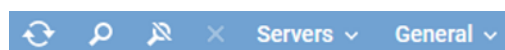








Fig. 196: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.
		The icon  is displayed whenever the search has been adjusted by means of a filter.

	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 167</a> .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Administrate server locations

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

#### Add server locations

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

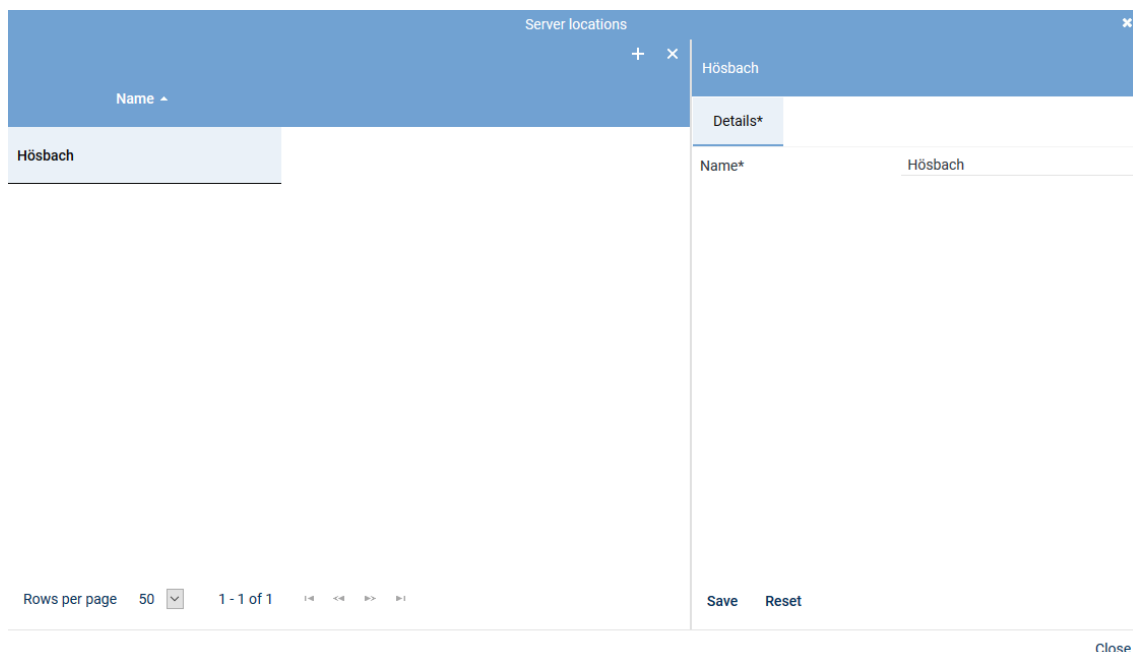



Fig. 197: Add server locations

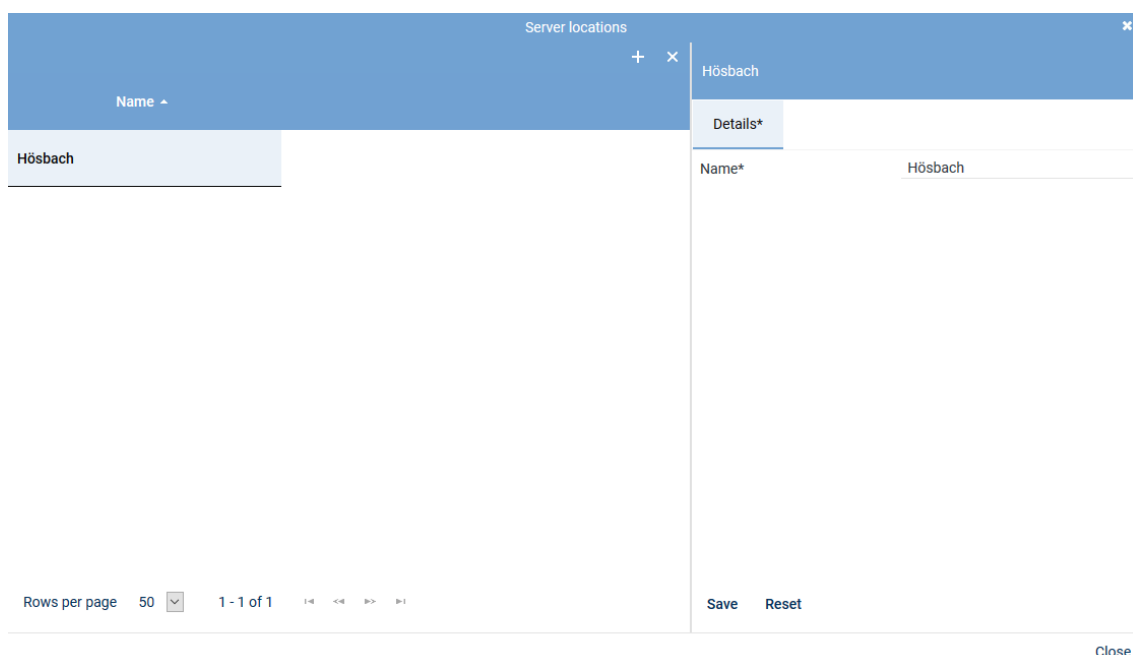
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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

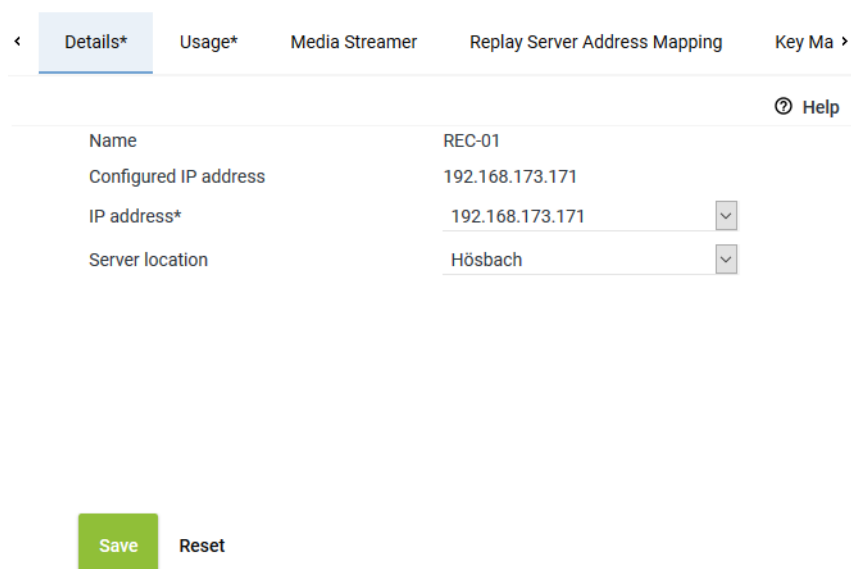
Close

Fig. 198: 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. 199: Servers - tab Details

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

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

### Tab Usage

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



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

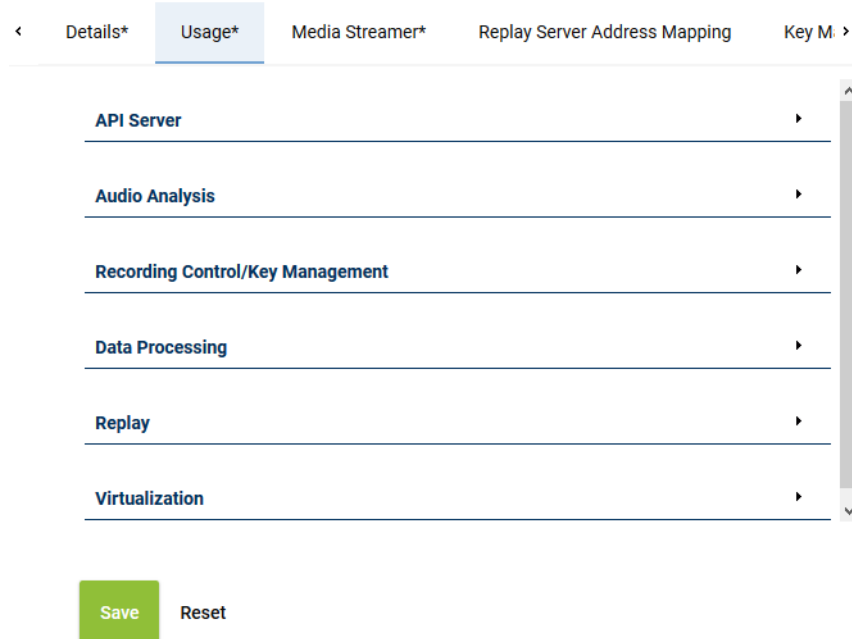


Fig. 200: Servers - tab usage

### Group field API Server

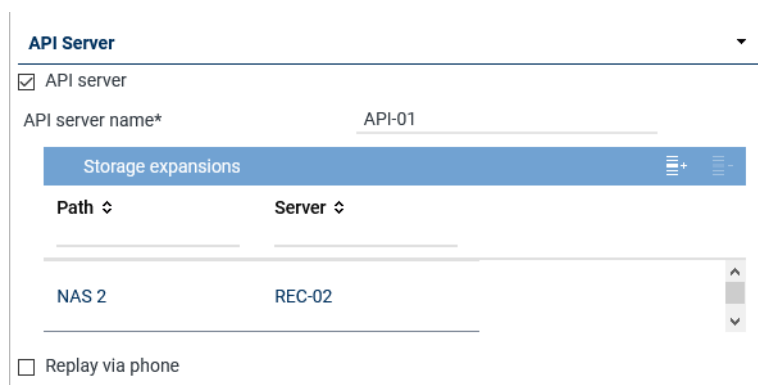




Fig. 201: Group field API Server

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


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

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

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

Parameter	Value/Description
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping"</a>, p. 181.</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"> <li>• By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay"</a>, p. 172.</li> <li>• By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul> <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><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWERplay Pro</li> <li>• Application POWERplay Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see <a href="#">chapter "Tab Media Streamer"</a>, p. 179. To be able to do so, at least 1 PBX must have been configured in the system.</p>

### Add storage expansion for replay

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

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

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 202: Select storage expansion

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


### Group field Audio analysis

**Audio Analysis**

☒ Emotion detection

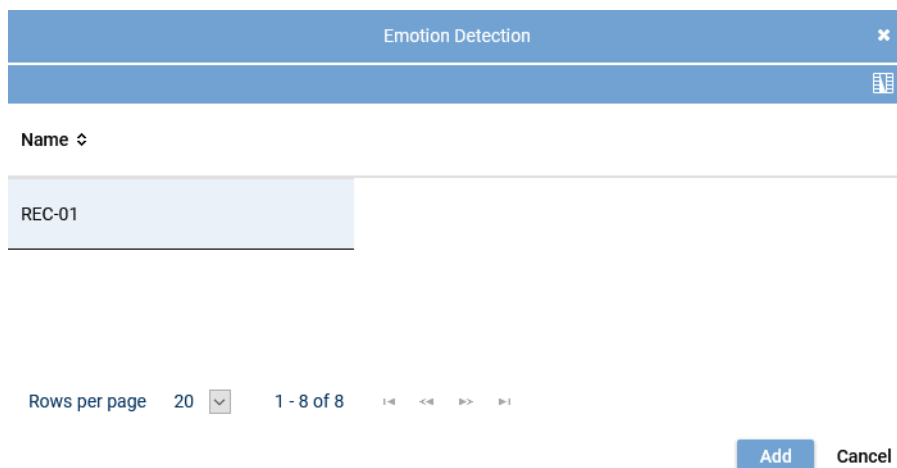
Stream audio data from\* REC-01 + -

Fig. 203: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis. <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function. <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> <li>Click on the button  to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 45: Configure audio analysis





Emotion Detection

Name ↕

REC-01
--------

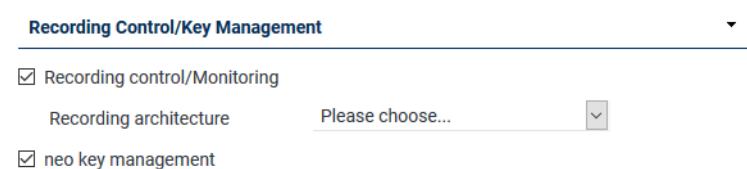
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 204: Select server for emotion detection

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

### Group field Recording Control/Key Management



Recording Control/Key Management

☒ Recording control/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 205: Group field Recording Control/Key Management

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

Tab. 46: Configure recording control/key management

### Group field Data Processing

**Data Processing** ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server

☒ Import

Recording architecture

Fig. 206: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 176</a>.</li> <li>By clicking on the icon  (Remove), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list"</a>, p. 176.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b> For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <li><i>Replay server</i> From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers.</li> </ul> <p><b>NOTICE!</b> For the export from <i>neo</i> to <i>neo</i>, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <li><i>Recording architecture</i> From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.</li> </ul>

Parameter	Value/Description
	<b>NOTICE!</b> If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 47: Data storage

### Add target server to a list

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



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

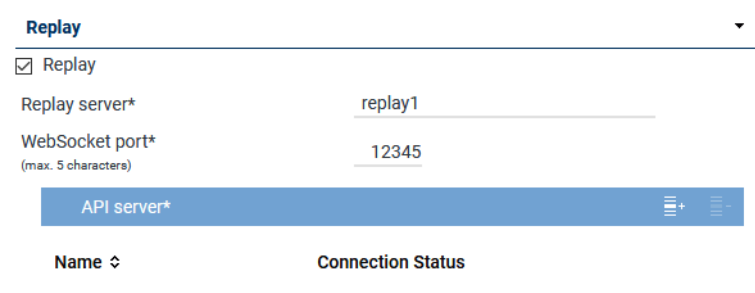
Fig. 207: Select server



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

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

### Group field Replay





**Replay**

☒ Replay

Replay server\*



WebSocket port\*   
(max. 5 characters)

API server\*  

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

Fig. 208: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API</a> 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 <a href="#">POWERplay</a> Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>• By clicking on the icon  (<i>Add</i>), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 177.</li> <li>• By clicking on the icon  (<i>Remove</i>), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 48: 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.

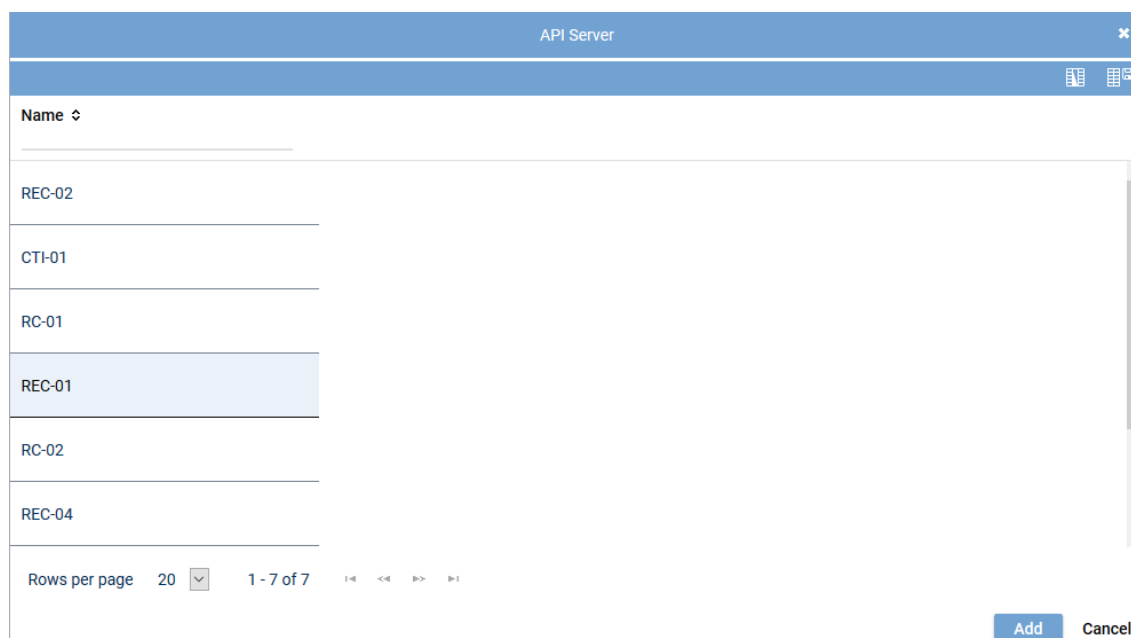


Fig. 209: Select server



Only those servers are available on which the **API** service has been installed and activated. See [chapter "Group field API Server", p. 170](#).

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. 210: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <code>TRUSTED_VIRTUALIZATION</code> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <code>licensing.asc.de</code> If you enter this domain, there is no key management.</li> </ul>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li><i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 49: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

### Tab Media Streamer

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

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



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

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

PBX +

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

Save

Reset

Fig. 211: Servers module - tab Media Streamer

- Enter the following parameters:

<b>PBX</b>	<b>PBX</b> that the Media Streamer is supposed to be mapped to. Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.
------------	--

	<p>If no PBX has been created in the system yet, you can create a <a href="#">PBX</a> via the blue bar <i>PBX</i>, see <a href="#">chapter "Create PBX"</a>, p. 185.</p>
<i>Extension</i>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <i>8000</i>.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <a href="#">SIP</a> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p> <p><b>NOTICE! The port range must not have less than 64 ports.</b></p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the <a href="#">SIP</a> communication.</p> <p><a href="#">TCP</a> = unencrypted  <a href="#">UDP</a> = unencrypted  <a href="#">TLS</a> = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the <a href="#">SIP</a> communication.</p> <p>Port for data exchange: <i>5062</i></p>
<i>User name</i>	Enter the user name for the authentication on the <a href="#">SIP</a> server.
<i>Password</i>	Enter the password for the authentication on the <a href="#">SIP</a> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<i>PBX port</i>	<p>Enter the port of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the value <i>5060</i>.</p>
<i>Registration required</i>	<p>Select whether the <a href="#">SIP</a> extension has to be registered with the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p><input checked="" type="checkbox"/> = <a href="#">SIP</a> extension has to be registered.  <input type="checkbox"/> = <a href="#">SIP</a> extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.



### Tab Replay Server Address Mapping

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

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



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

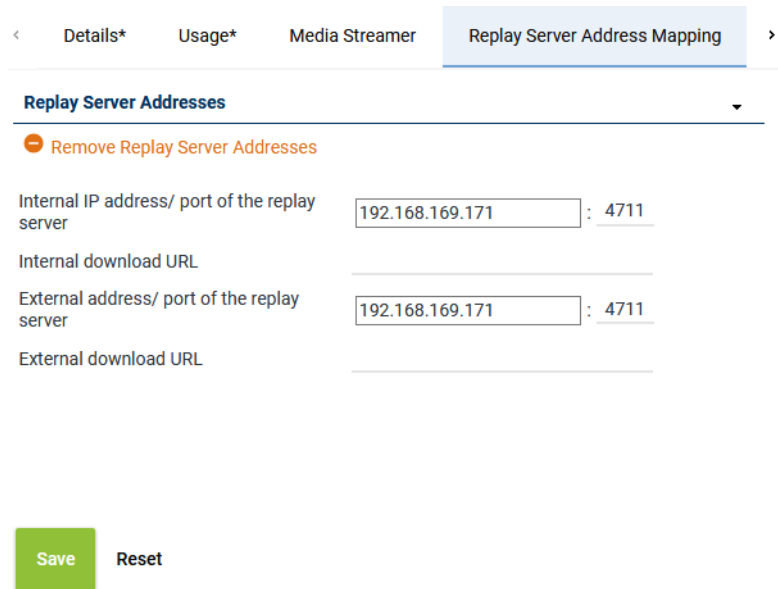


Fig. 212: Servers Module - tab Replay Server Address Mapping

### Group field Replay Server Addresses

1. Enter the following parameters

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

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



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

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



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



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

### Tab Key Management

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

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

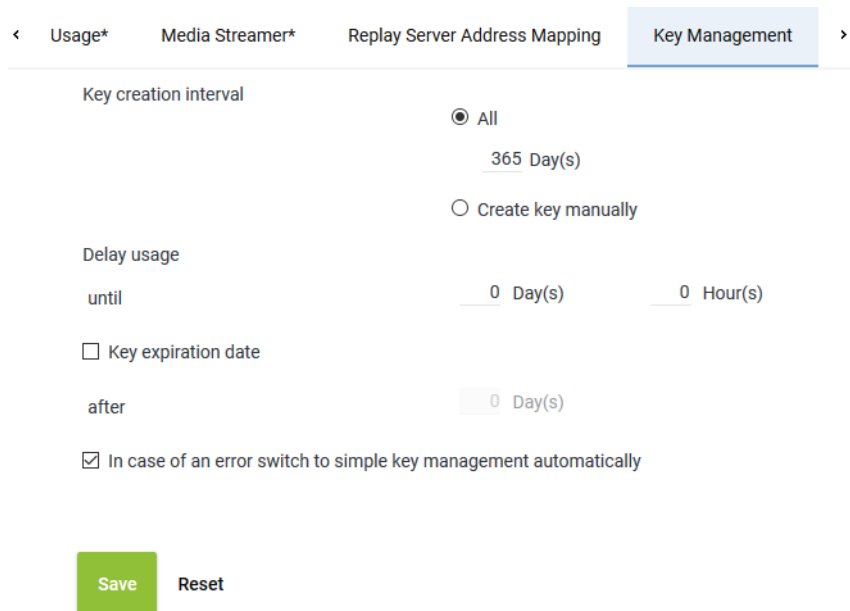


Fig. 213: Servers module - tab Key Management

<b>Key creation interval</b>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually.</li> </ul> <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
------------------------------	--

<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*

In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.

- *ASC License Management System*

**NOTICE! License Management does not support encryption.**

**For licensing, there are the following options:**

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.

In this case, no separate configuration is required.

- *Trusted Virtualization License*

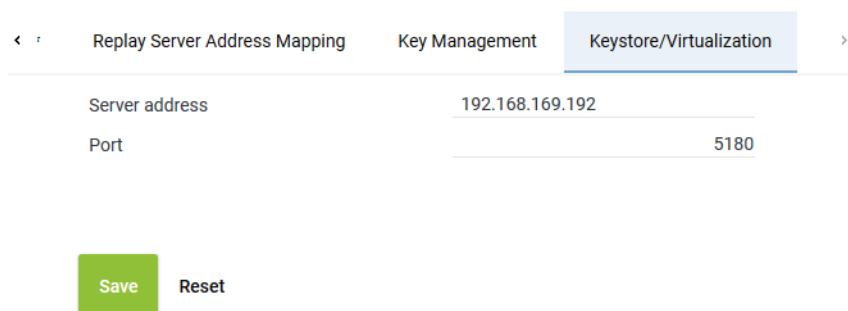
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



The screenshot shows a web interface for configuring the Keystore/Virtualization tab. It features three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is active. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom, there are two buttons: 'Save' (green) and 'Reset' (gray).

Fig. 214: Servers module - tab Keystore/Virtualization

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

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	Enter the port for the connection. 5180 = Dongle Manager 8181 = ASC License Management System



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

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

### 7.3.2.3.3 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.

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

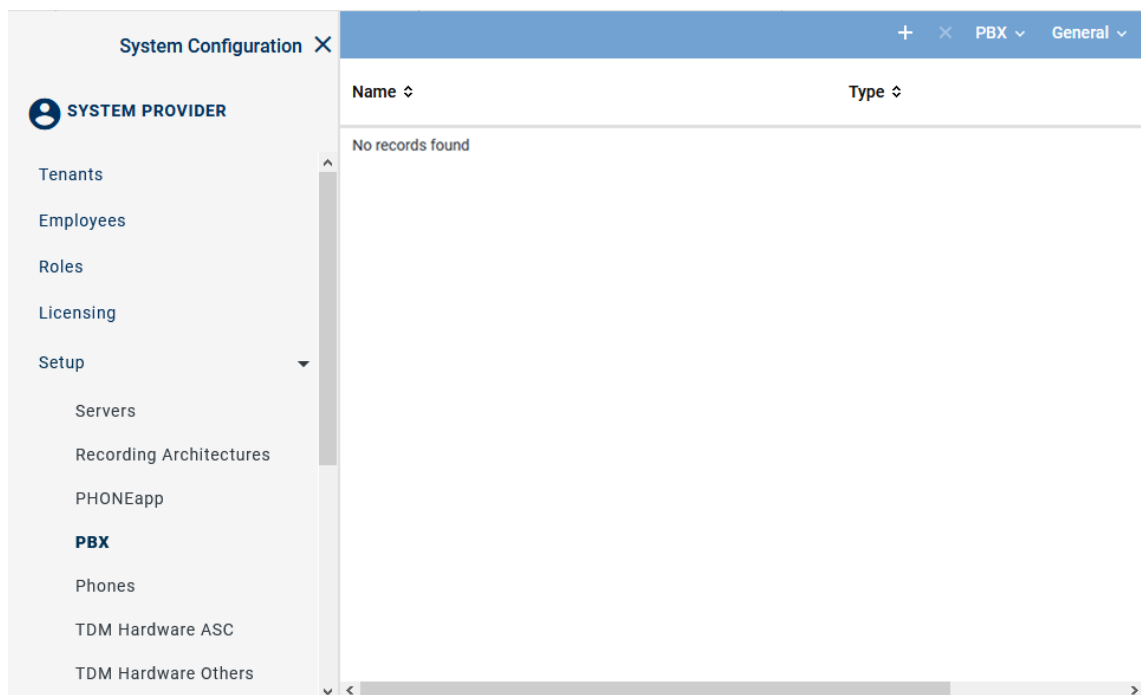


Fig. 215: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

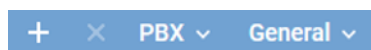




Fig. 216: Toolbar PBX module


	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.

<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Create new PBX

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

×

< 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. 217: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 50: 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

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

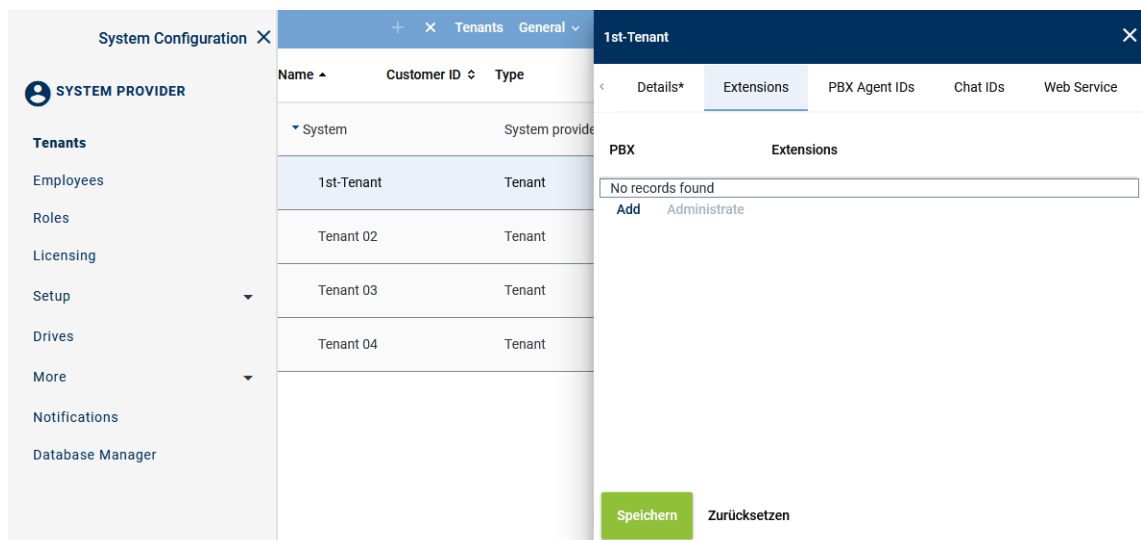


Fig. 218: Tenants - main view - tab Extensions

##### 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. 219: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>ZIP</li> <li>TXT</li> <li>CSV</li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>Click on the button <span style="background-color: #f1f3f4; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>Click on the button <i>Choose File</i>.</li> <li>Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>Click on the button <span style="background-color: #4285f4; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34

189 / 489

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

Enter country codes as number ranges as follows:  
+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions* Activate the check box to replace the list of extensions.

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

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

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

### Remove extensions

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

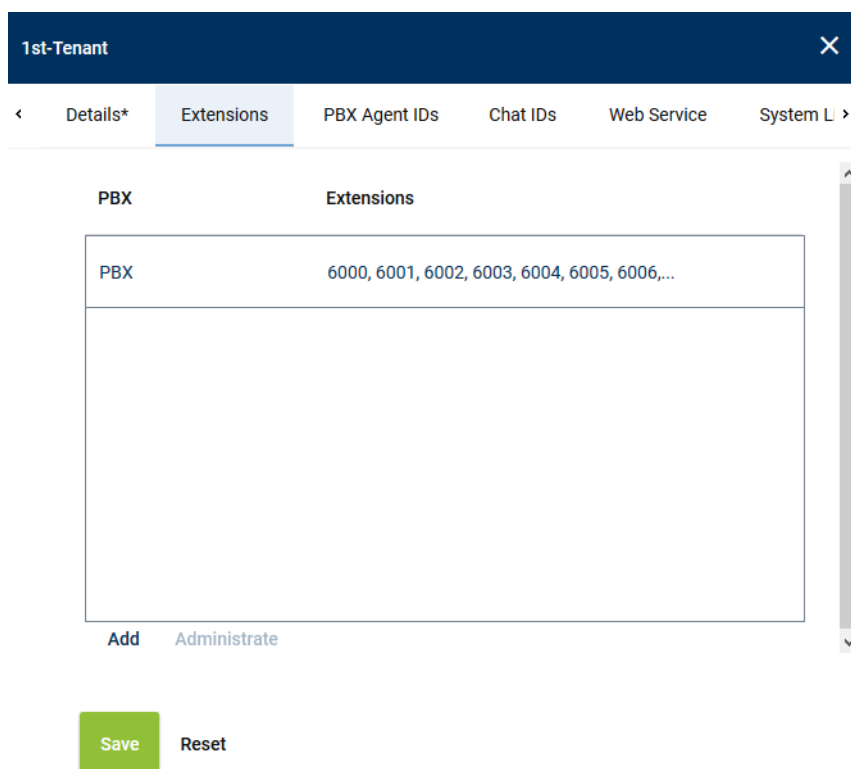


Fig. 220: Remove extensions

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. 221: 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.

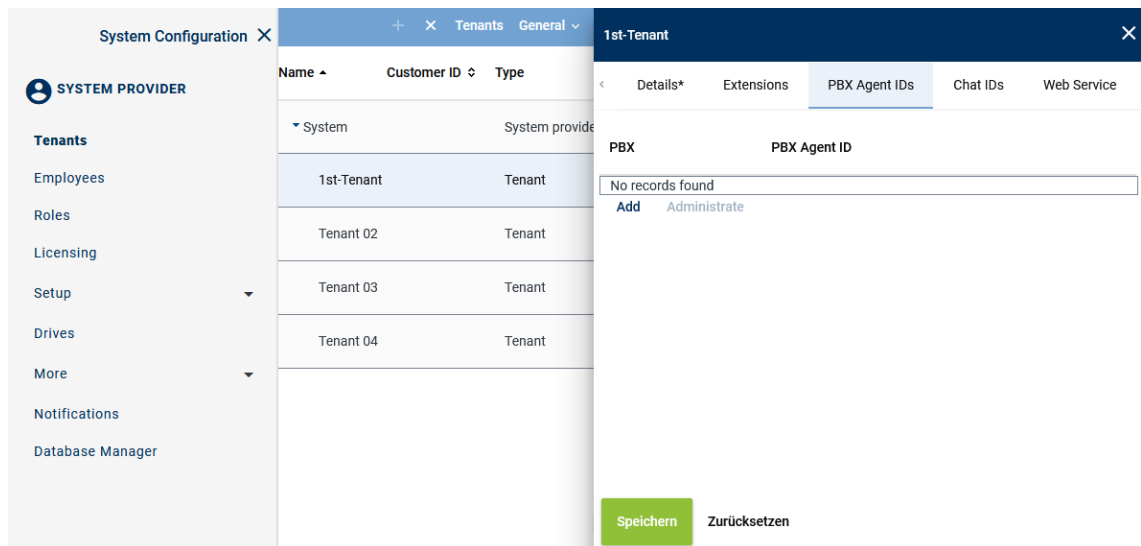
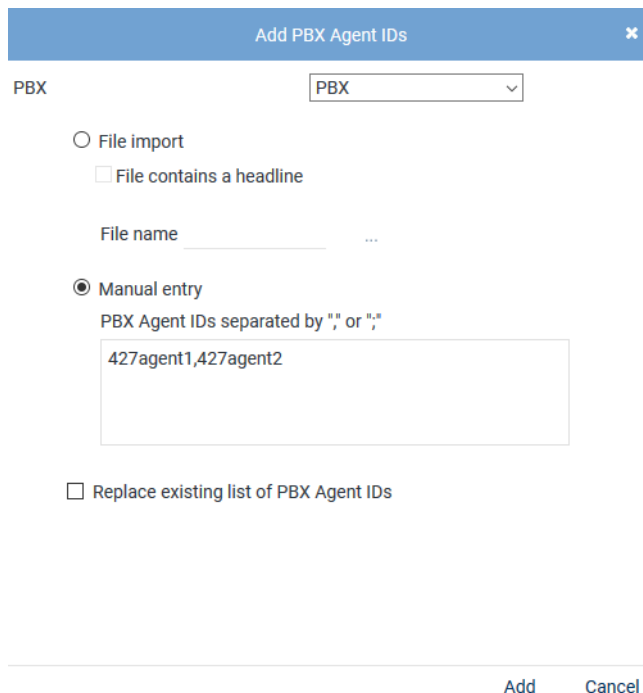


Fig. 222: Tenants - main view - tab PBX Agent ID

### 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:



The 'Add PBX Agent IDs' dialog box has a dropdown menu set to 'PBX'. It offers two options: 'File import' (with a sub-option 'File contains a headline') and 'Manual entry' (selected). The 'Manual entry' section has a text input field containing '427agent1,427agent2'. At the bottom, there is a checkbox for 'Replace existing list of PBX Agent IDs'. The dialog has 'Add' and 'Cancel' buttons at the bottom right.

Fig. 223: 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 the option to import PBX Agent IDs from an existing <a href="#">CSV</a> 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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
	<p><b>File name</b></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>Upload File</b>.</li> </ul>
<b>Manual entry</b>	<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><b>NOTICE! Wildcards cannot be used!</b></p>
<b>Replace existing list of PBX Agent IDs</b>	<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. 224: 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.

**System Configuration** ✕

**SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 225: 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. 226: 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. 227: 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 All-in-one Parallel Recording

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

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

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

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

⇒ The following window appears:

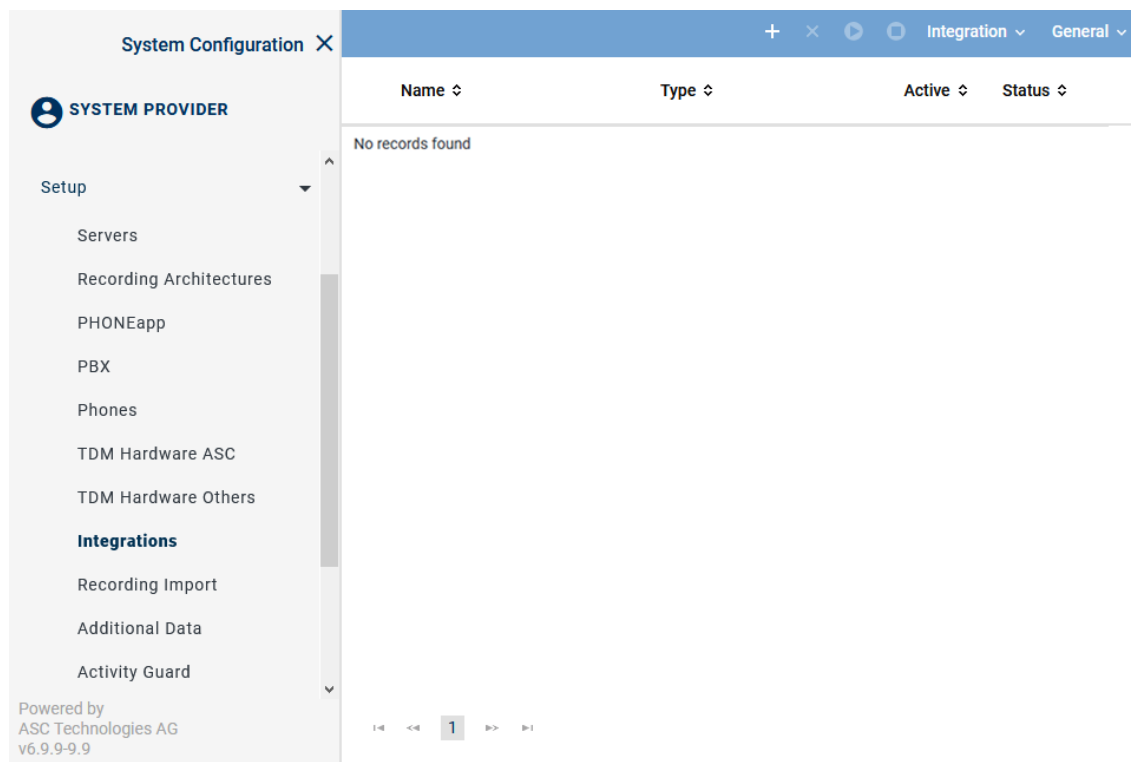




Fig. 228: Integrations - main view

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



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

### Toolbar of the Integrations module



The toolbar offers the following functions.



Fig. 229: Toolbar Integrations module

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



	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

- 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.

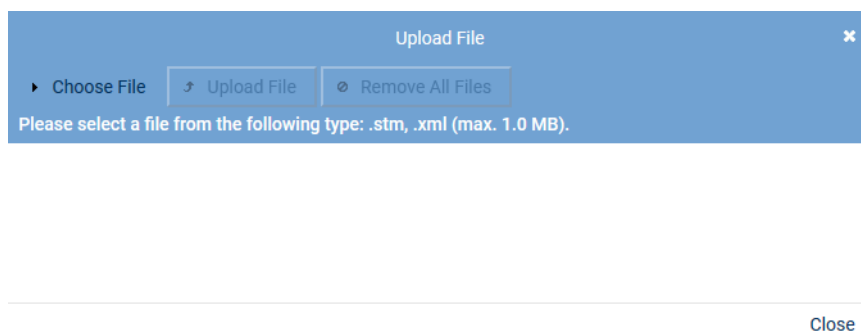


Fig. 230: Choose file

- 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*.

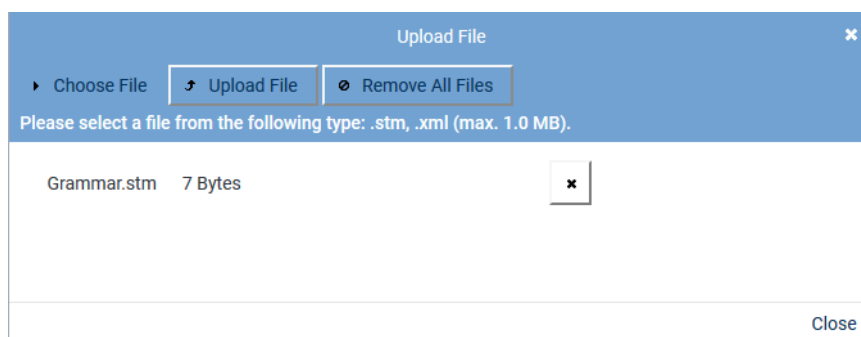



Fig. 231: Upload grammar

- 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. 232: Create integration type

- Enter the following parameters:

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

Tab. 51: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

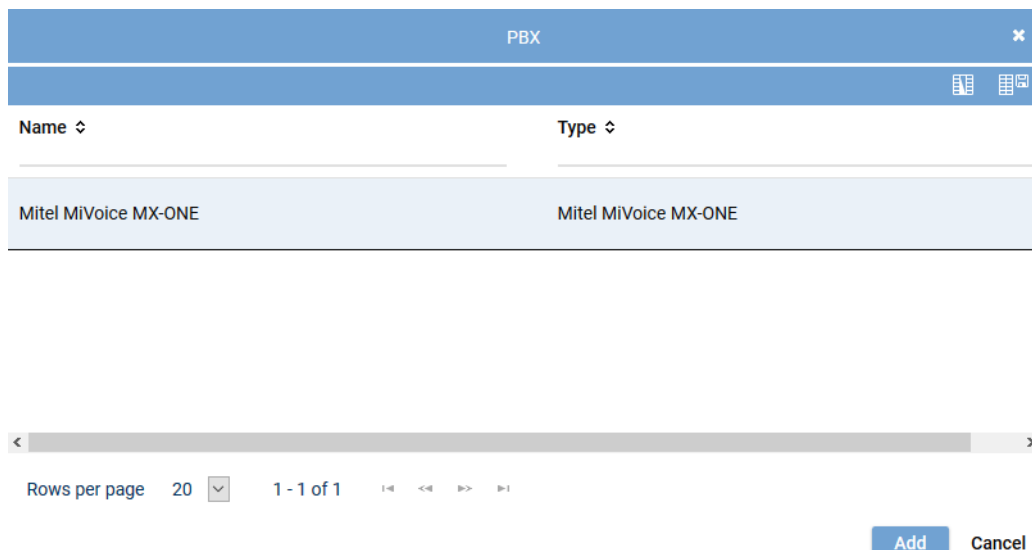


Fig. 233: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

### Assign recording architecture for All-in-one Parallel Recording

- In the detail view on the bottom right, click on the button *Next*.

⇒ The tab *Recording Architecture* appears.

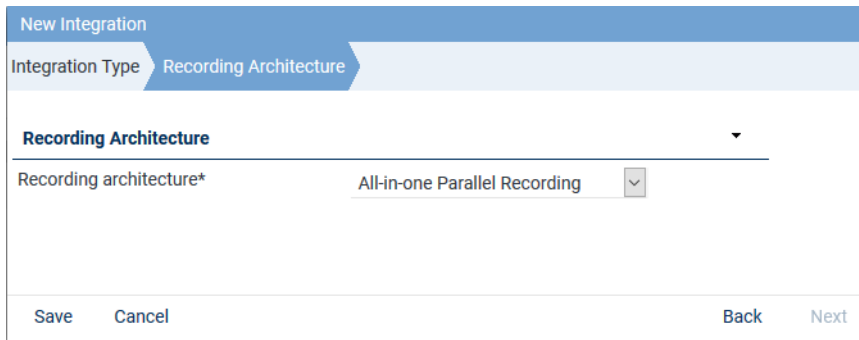


Fig. 234: Assign recording architecture - All-in-one Parallel

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



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


3. Click on the button *Save*.

⇒ The integration now appears in the main view.



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see [chapter "Duplicates in parallel recording architectures", p. 445](#).

### 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	✗				
Configure monitor points	✗				
Global recording settings	✗				
Configure recording servers	✗				
Configure add-on	✓				
Configure miscellaneous settings	✓				

Fig. 235: 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. 236: 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab MiVoice MX-ONE (CSTA)

In the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

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

- Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\* MBG

**CTIconnect Module**

Type CTIconnect active

Grammar name\* standard

Grammar version\* 1.00.12

**Connection Data Device Group 1**

**Connection Data Device Group 2**

**Additional Data**

Failover waiting time\* 10

Failover repetitions\* 3

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}$`

Save Cancel

Fig. 237: Configure tab MiVoice MX-ONE (CSTA)

Configure the **CSTA** connection so that monitoring can use it even if your recording runs via a **MBG**.



For parallel recording, you must configure the **MBG** in the tab **MBG**.

### 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. 238: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 52: 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 MiVoice MX-ONE (CSTA)

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.

Connection Data Device Group 1

PBX IP address

No records found

Add

Edit

Delete

Connection Data Device Group 2

PBX IP address

No records found

Add

Edit

Delete

Fig. 239: 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

PBX IP address\*

192.168.170.219

PBX CSTA port\*

8882

Transport Layer Security (TLS)

☐

☒ Activate authentication

Application ID\*

1234

Password\*

.....

Add

Cancel

Fig. 240: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<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 run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate this check box to use the connection with <i>TLS</i> .

Parameter	Value/Description
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14.</a>
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 53: Configure connection data

- 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.

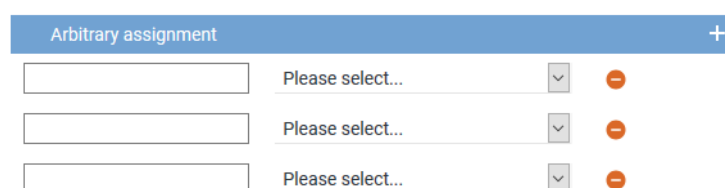



Fig. 241: Arbitrary assignment of the additional data

The following additional data is always available:

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

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



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



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

### Configure 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 CTIconnect 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. 242: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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 <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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. 243: 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.



As parallel recording is only possible via the **MBG**, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

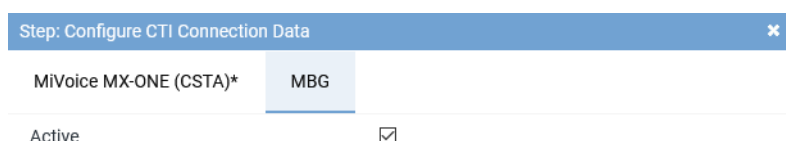


Fig. 244: Activate CTIconnect connection data for [MBG](#)

**Active** Activate the check box to display the configuration parameters and to activate the connection to the [MBG](#).

☒ = Connection has been activated.

☐ = Connection has not been activated.



Following an update, you must configure this section again.

### ATTENTION!

In parallel recording architectures, calls must be recorded by means of the [MBG](#).

### Group field CTIconnect Module

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

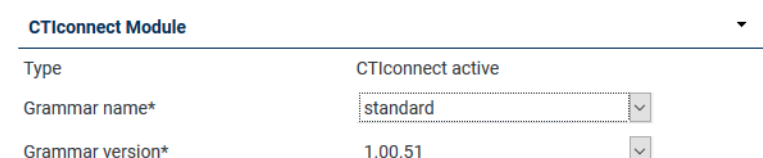


Fig. 245: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 54: 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

For this recording architecture, you can configure the connection data for 2 servers.

For every device group, you can enter one or several sets of connection data.

The entries of the first set of data will be used by default during the connection establishment. If errors occur during this connection, it will be switched to the configured alternative connection.

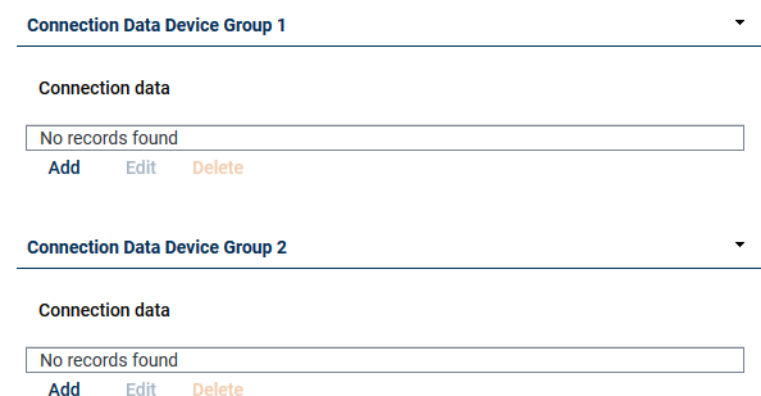


Fig. 246: Group field Connection Data

1. In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

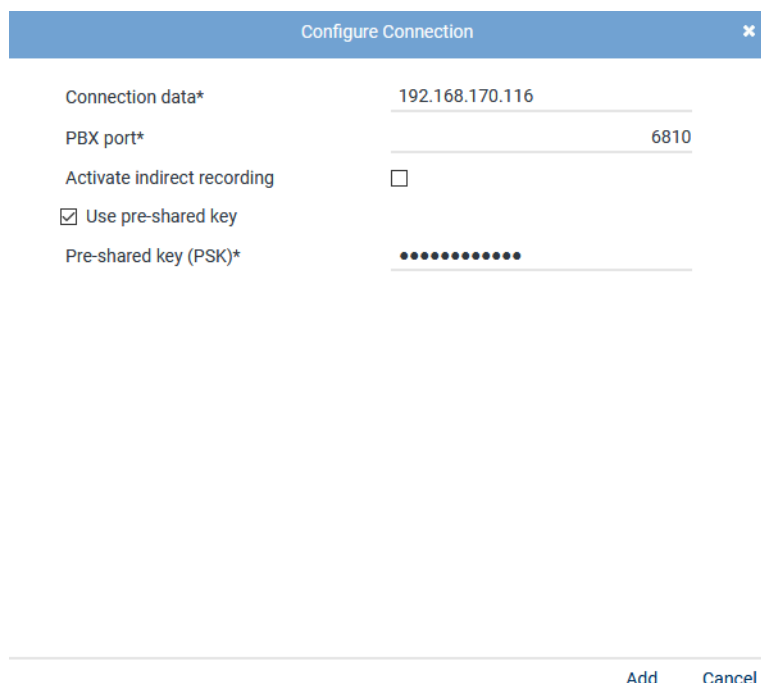


Fig. 247: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
Connection data	Enter the link to the <a href="#">MBG</a> .

Parameter	Value/Description
<i>PBX port</i>	Enter the port for the <b>MBG</b> or the <b>SRC</b> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <b>MBG</b> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 55: 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.

### Group field Additional Data MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

- 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.

**Additional Data** ▼

---

Arbitrary assignment

Key 0	Please select...	▼
Key 1	Please select...	▼
Key 2	Please select...	▼

Fig. 248: CTI connection data - additional data module 1

- Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
- From the drop-down list, select the entry which is supposed to appear as column headline in the players.
- Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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

- 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.

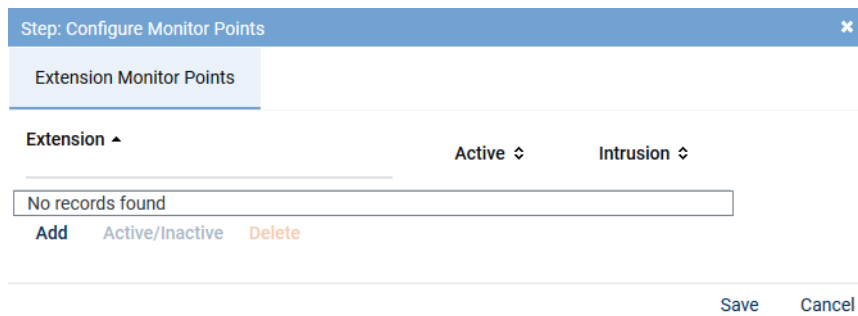


Fig. 249: Configuration step - configure monitor points

### Tab *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.

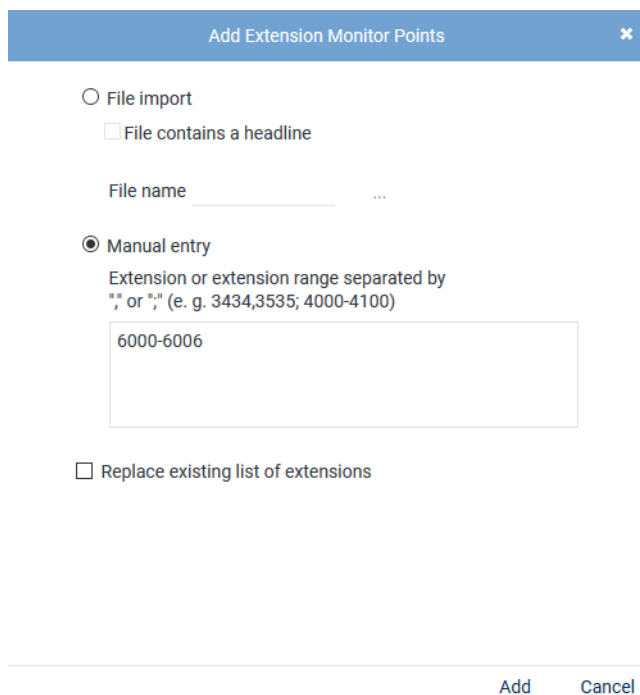




Fig. 250: Add extension monitor points

#### *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*.
- Click on the button *Choose File*.
- Select the respective ZIP file via the Explorer and click on the button *Open*.
- Click on the button **↗** (*Upload file*).

	<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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> 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"> <li>• Click on the button  behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  (<i>Upload file</i>).</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>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><b>NOTICE! Wildcards cannot be used!</b></p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; 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. 251: Configured extension monitor points

<b>Add</b>	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.
<b>Active/Inactive</b>	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.
<b>Delete</b>	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.



In parallel recording, you cannot use the Intrusion feature.

<b>Intrusion</b>	Do not enter a check mark in the line Intrusion when recording in parallel. <input type="checkbox"/> = 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<sup>connect</sup> 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. 16.

### 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.

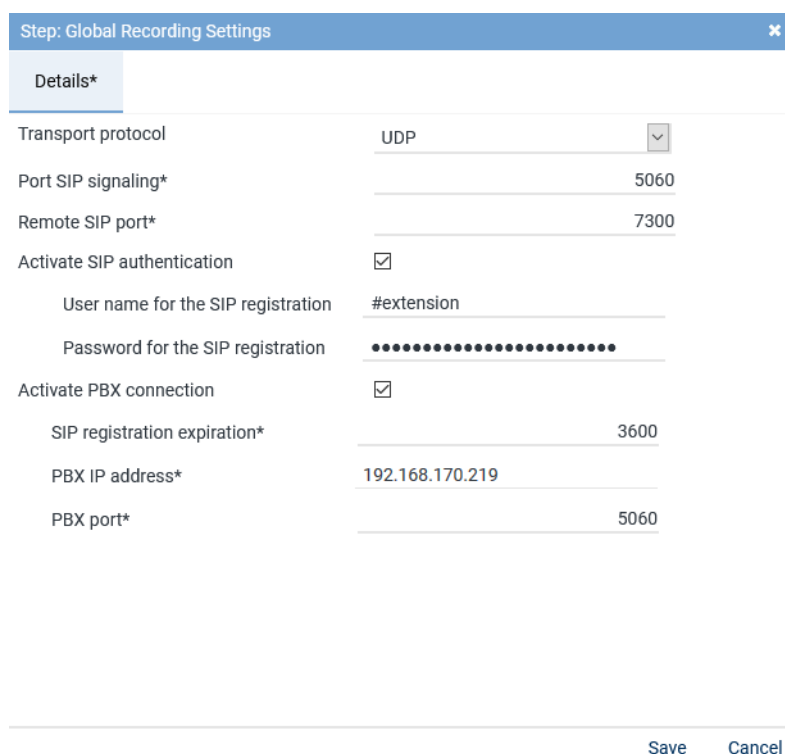


Fig. 252: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i>, the transport protocol applies for the SIP communication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
<i>Port SIP signaling</i>	<p>Enter the port for SIP signaling that is opened on the recording server for incoming SIP communication and that has been selected in the outgoing SIP notifications as the port of the recording server. Default 5060.</p>
<i>Remote SIP port</i>	<p>Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by SIP to start <i>active-stream recording</i>. Default 7300.</p>
<i>Activate SIP authentication</i>	<p>Activate the check box if 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>.</p>



Parameter	Value/Description
<i>User name of the SIP registration</i>	Enter the user name for <b>SIP</b> registration of extensions recorded with intrusion feature. The user name is configured in the <b>PBX</b> and applies for all extensions to be registered.
<i>Password of the SIP registration</i>	Enter the password for <b>SIP</b> registration of extensions recorded with intrusion feature. The password is configured in the <b>PBX</b> 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 <b>PBX</b> .
<i>PBX port</i>	Enter the port for the communication with the <b>PBX</b> , default 5060.


Tab. 56: Global recording settings

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



Following an update, you must configure this section 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.

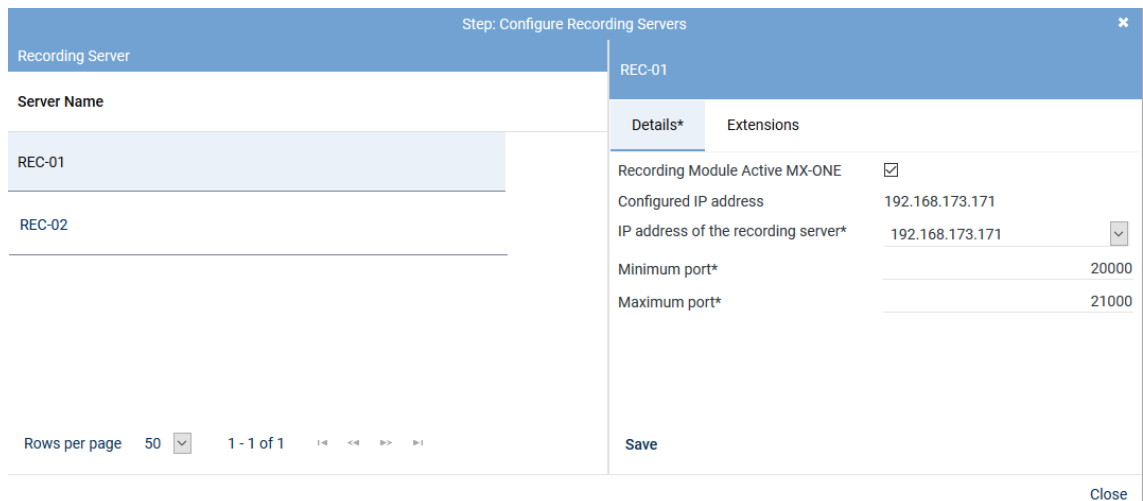


Fig. 253: Configuration step - Configure recording servers

- 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.

Parameter	Value/Description
<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 <b>RTP</b> 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 <b>RTP</b> data from the recording server, e. g. 21000.

Tab. 57: 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.



Following an update, you must configure this section 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 CTI connect module of the integration.



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

### Configure add-on for 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.

- 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	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
PRIVATEDATA	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
SERVICEGROUPID	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
SERVICEGROUPLIST	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA1	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL1	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA2	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL2	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA3	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL3	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
OASID	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>

Arbitrary assignment
+

	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>
	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>
	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>

Save Cancel

Fig. 254: 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	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 58: 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. 59: 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.

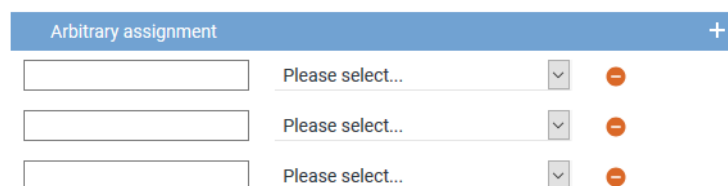



Fig. 255: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*

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

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



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



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

### **Configure add-on for 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<sup>connect</sup> 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

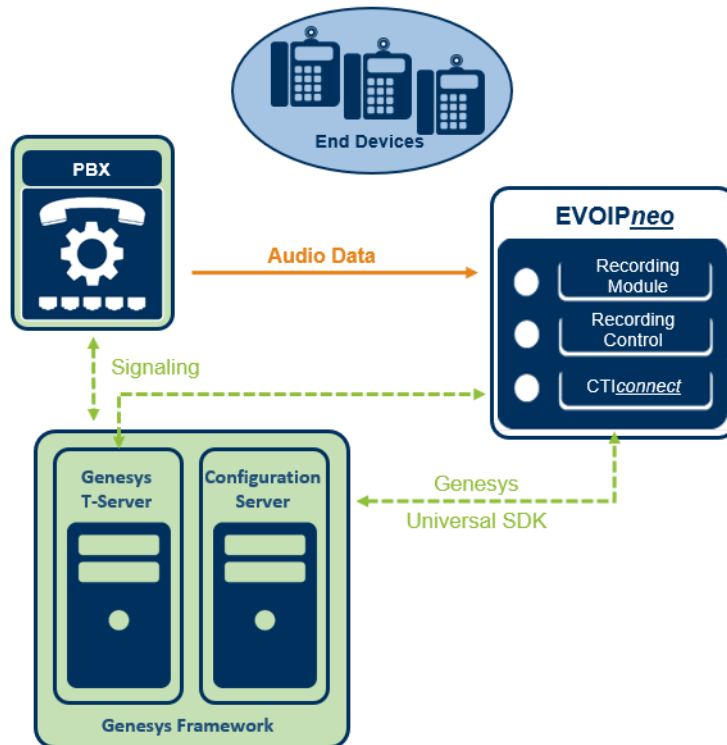


Fig. 256: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

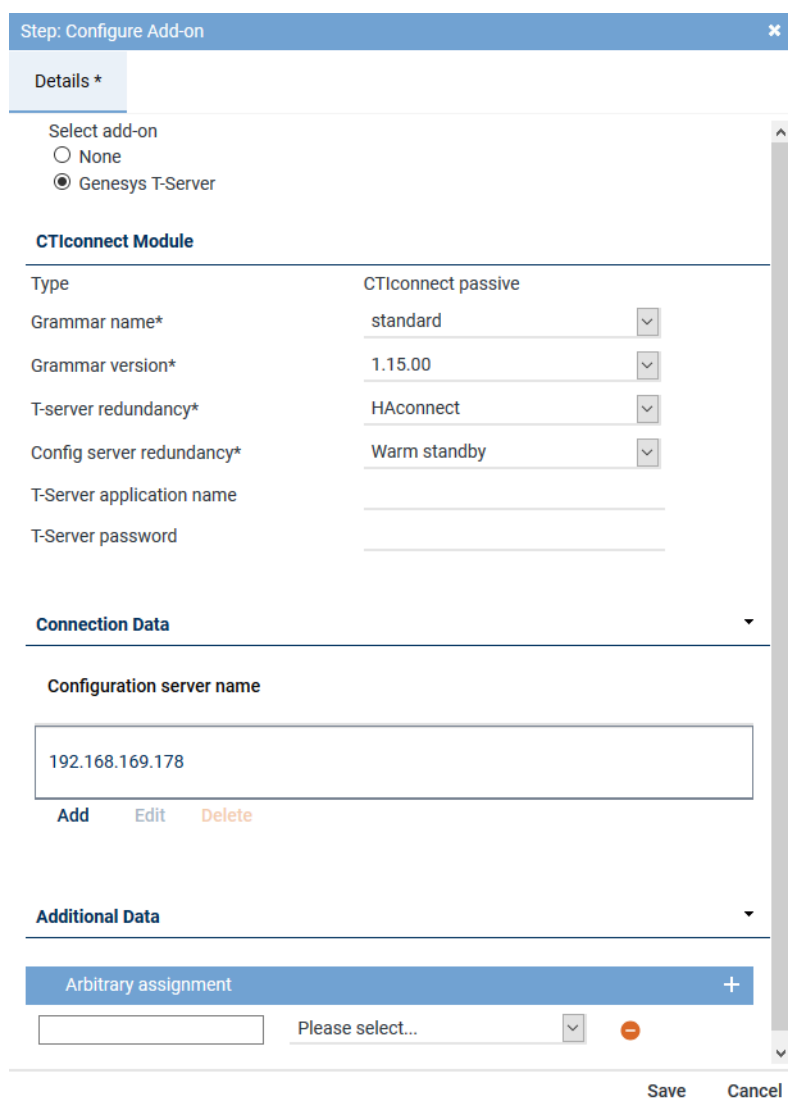


Fig. 257: Configure add-on for Genesys T-Server

### 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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. 60: 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:

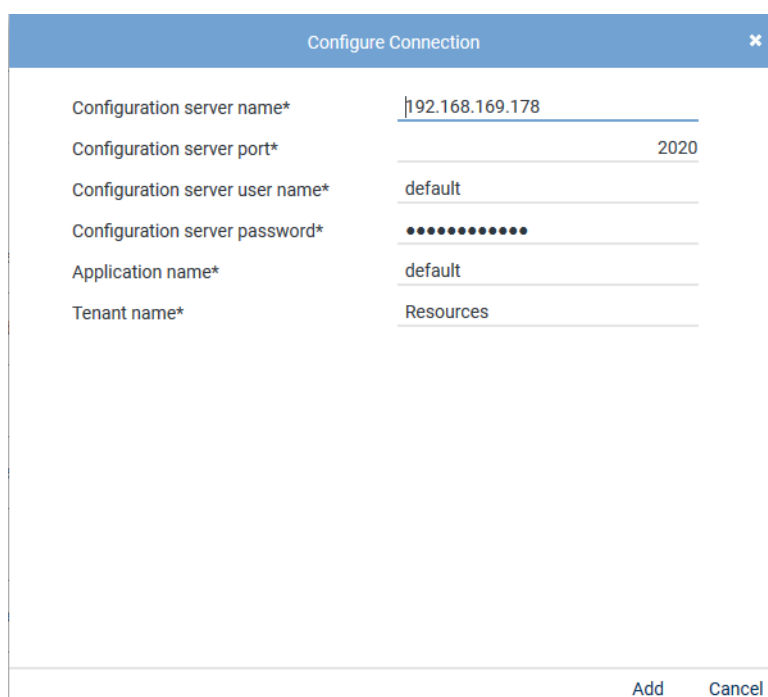


Fig. 258: Configure connection data

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. 61: 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. 259: Arbitrary assignment of the additional data

The following additional data is always available:

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

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



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



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

### Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

▼

Save

Cancel

Fig. 260: 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. 261: 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. 262: 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. 263: 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 Recording

### 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:

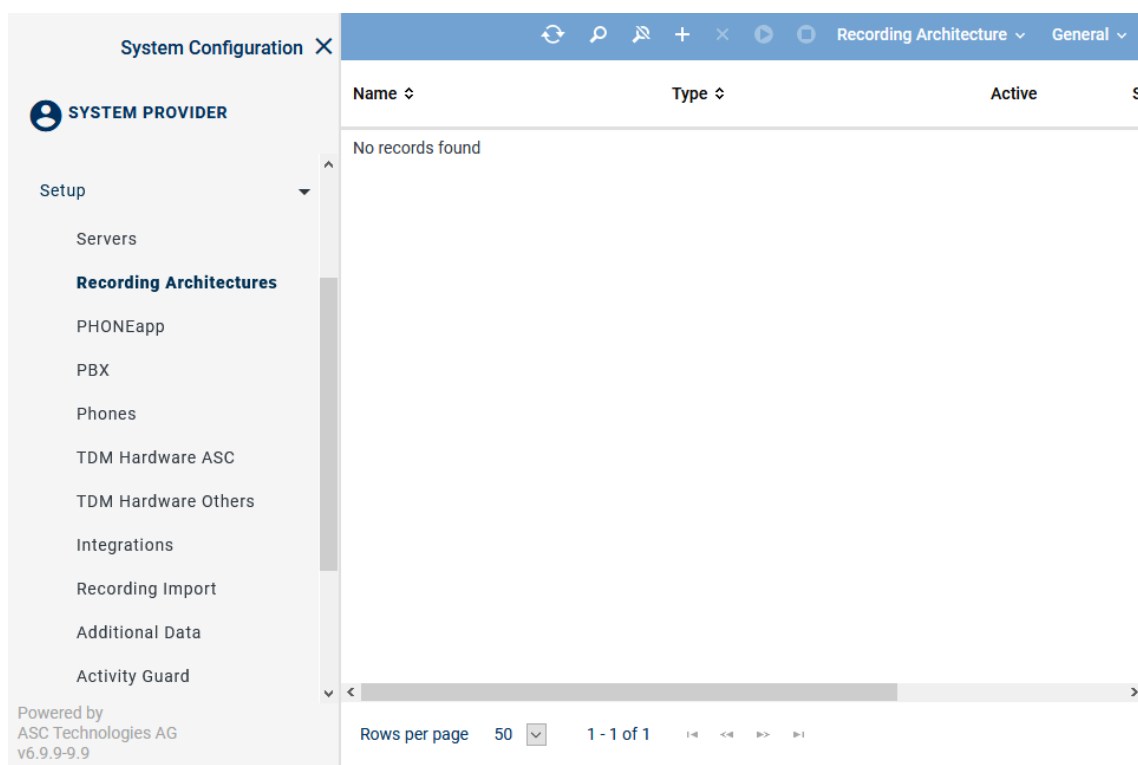





Fig. 264: Recording architectures - main view

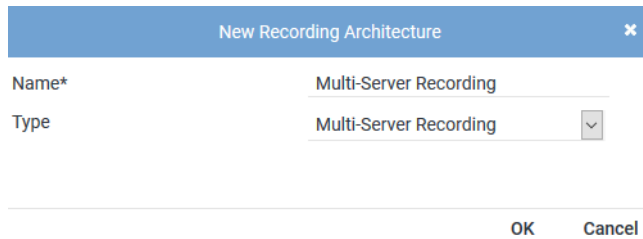
<b>Name</b>	Name of the recording architecture
<b>Type</b>	Type of the recording architecture
<b>Active</b>	Shows whether the recording architecture has been activated and is ready to be used for the recording. <div> <span>✓</span> = Recording architecture is active and ready to be used for recording.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

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

### Create recording architecture Multi-Server Recording

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

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



New Recording Architecture

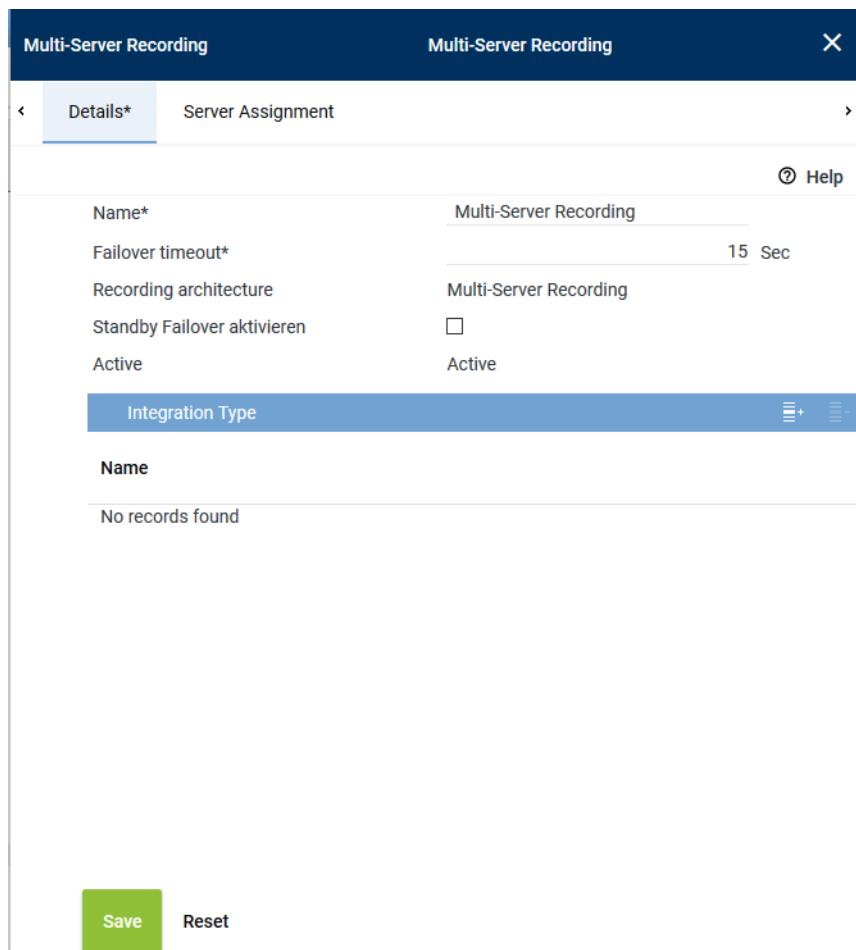
Name\* Multi-Server Recording

Type Multi-Server Recording

OK Cancel

Fig. 265: Create recording architecture - Multi-Server Recording

- In the entry field *Name*, enter a descriptive name for the recording architecture.
  - From the drop-down list *Type*, select the recording architecture type *Multi-Server Recording*.
- NOTICE!** Only the supported recording architecture types are displayed in the drop-down list.
- Click on the button *OK*.
- ⇒ The entries now appear in the detail view.



Multi-Server Recording Multi-Server Recording

< Details\* Server Assignment >

Help

Name\* Multi-Server Recording

Failover timeout\* 15 Sec

Recording architecture Multi-Server Recording

Standby Failover aktivieren ☐

Active Active

Integration Type

Name

No records found

Save Reset


Fig. 266: Recording architecture - tab Details - Multi-Server Recording

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



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

### Add integration type

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

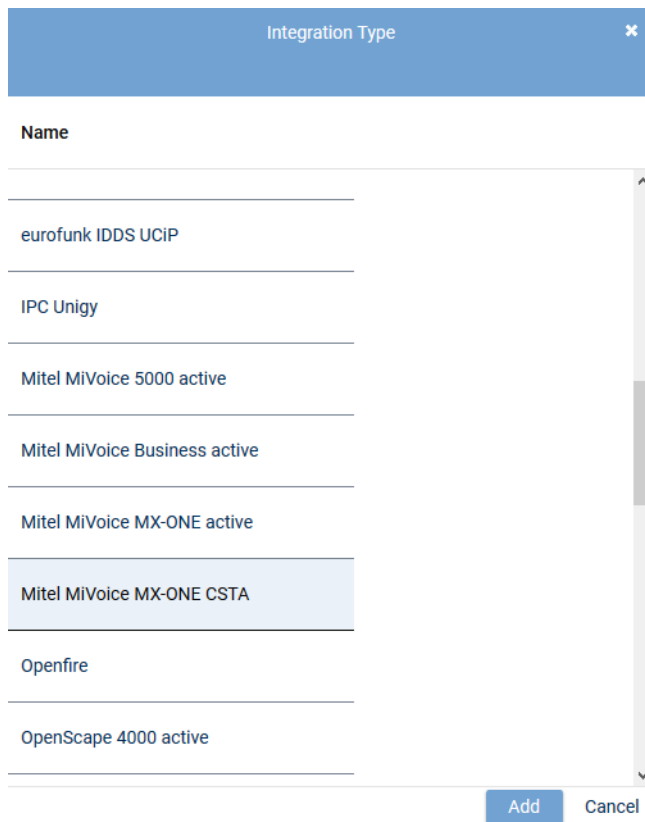


Fig. 267: Select integration type



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 server for Multi-Server Recording

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

### Group field Recording Control and CTIconnect

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

Multi-Server Recording
Multi-Server Recording

Details\*
Server Assignment\*

Recording Control and CTIconnect

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


Recording Server

Recording Server

Server	Standby
REC-01	REC-02

Save
Reset

Fig. 268: Recording architecture - tab Server Assignment

- Click on the button  next to the entry field *Recording Control*.  
⇒ The window *Servers* appears.


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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 269: Recording architecture - assign server - example




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



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

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

### Group field Recording Server

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

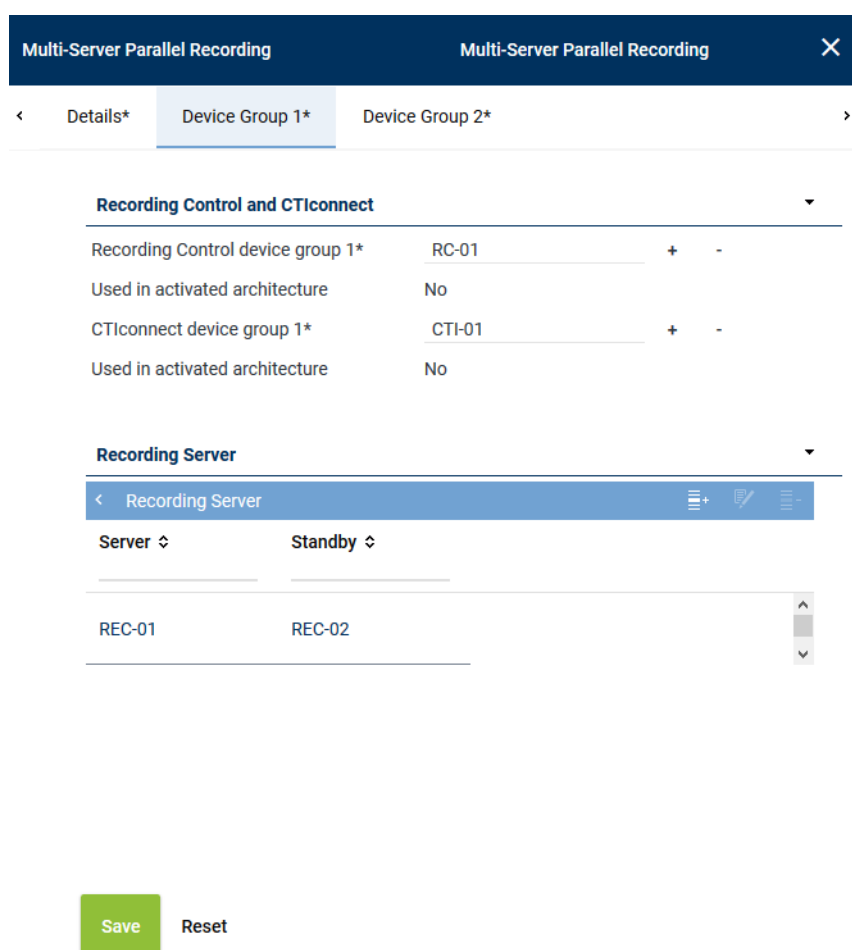









Fig. 270: Add recording server

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

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

### Activate recording architecture

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










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

Fig. 271: Recording architecture - activate recording architecture

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



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



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

#### 7.3.2.4.2 Configure server

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

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

System Configuration X		Servers v General v	
<b>SYSTEM PROVIDER</b>  Setup <b>Servers</b> Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard			
	Name ↕	IP Address ↕	
	CTI-01	192.168.173.177	
	CTI-02	192.168.173.178	
	RC-01	192.168.173.175	
	RC-02	192.168.173.176	
	REC-01	192.168.173.171	
	REC-02	192.168.173.172	
	REC-03	192.168.173.173	
	REC-04	192.168.173.174	

Fig. 272: Servers - main view

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

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

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

### Toolbar of the Servers module

The toolbar offers the following functions.

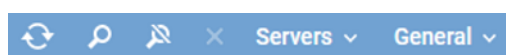







Fig. 273: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.  The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <a href="#">neo</a> system.

<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations"</a> , p. 232.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <a href="#">Administrate NTP server</a> .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Administrate server locations

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

#### Add server locations

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

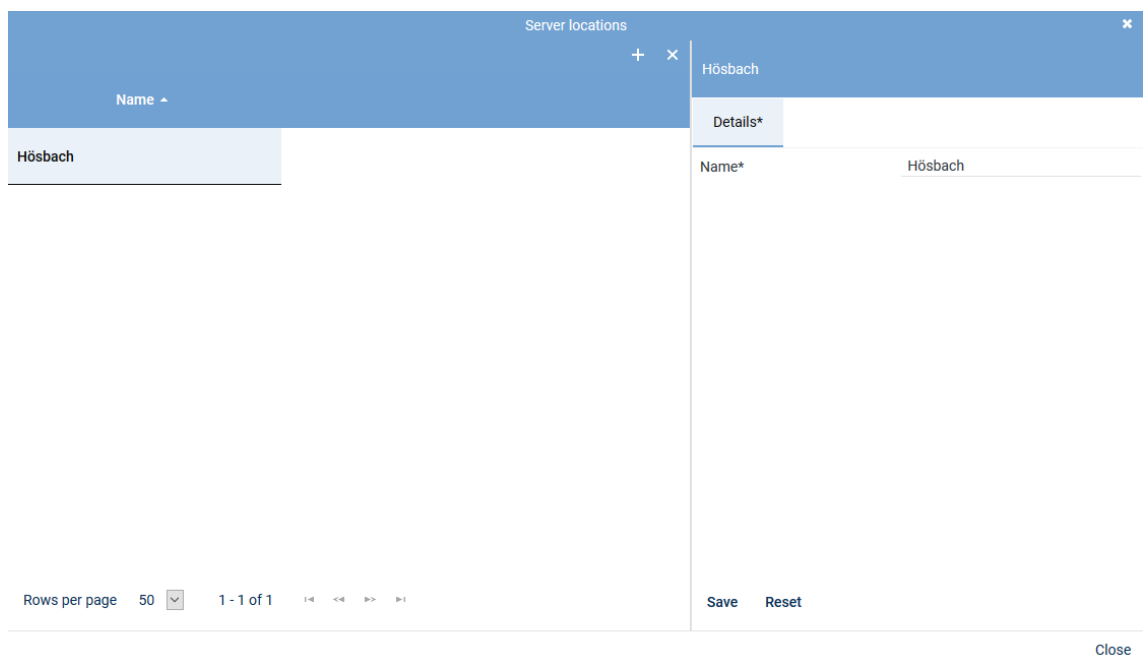



Fig. 274: Add server locations

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

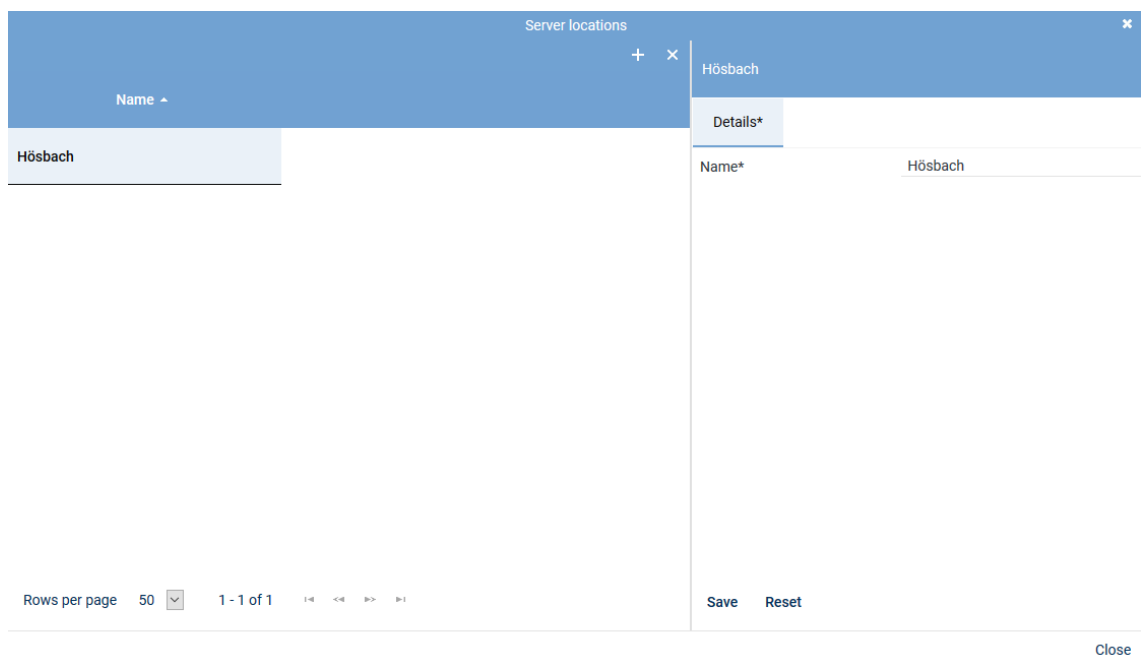
4. To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

### Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a table with a single row containing the text "Hösbach". To the right of the table is a tab labeled "Details\*". Below the table, there is a pagination bar showing "Rows per page 50" and "1 - 1 of 1". At the bottom right of the window, there are buttons for "Save", "Reset", and "Close".

Fig. 275: 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. 276: Servers - tab Details

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

### Tab Usage

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



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

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

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

Fig. 277: Servers - tab usage

### Group field API Server

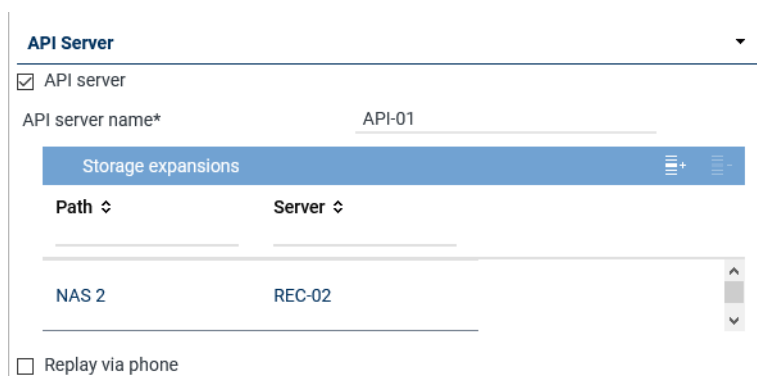




Fig. 278: Group field API Server

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


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

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


Parameter	Value/Description
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping", p. 245</a>.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay", p. 236</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul>

Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.  <input type="checkbox"/> = Function has not been activated.</p> <p><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWER<i>play</i> Pro</li> <li>• Application POWER<i>play</i> Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a <b>PBX</b>, see <a href="#">chapter "Tab Media Streamer", p. 243</a>. To be able to do so, at least 1 <b>PBX</b> must have been configured in the system.</p>

### Add storage expansion for replay

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

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

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

Add Cancel

Fig. 279: Select storage expansion



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

### Group field Audio analysis

**Audio Analysis**

☒ Emotion detection

Stream audio data from\* REC-01 + -

Fig. 280: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> <li>Click on the button <b>+</b> to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 62: Configure audio analysis

**Emotion Detection** ✕

📄

Name ↕

REC-01

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

**Add** **Cancel**

Fig. 281: Select server for emotion detection

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

### Group field Recording Control/Key Management

**Recording Control/Key Management** ▼

☒ Recording control/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 282: Group field Recording Control/Key Management

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

Tab. 63: Configure recording control/key management

### Group field Data Processing

**Data Processing**

☒ Data storage

☐ Transfer data for replay

Target Server

Name

IP Address ↕

No records found

☒ Transfer data for data storage

Target Server

Name

IP Address ↕

No records found

Activate period of time

☒

Start

0:00

▼

End

4:00

▼

Receives data from

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 283: Group field Data Processing

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34


238 / 489

Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 240</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list", p. 240</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b></p> <p>For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>

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

Tab. 64: Data storage

### Add target server to a list

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

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

Fig. 284: 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*

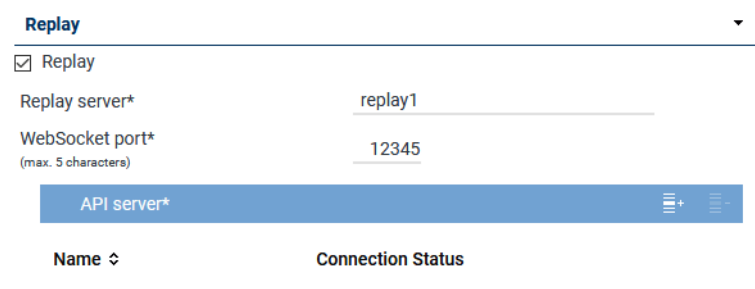




Fig. 285: Group field *Replay*

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API server</a> must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in <a href="#">POWERplay Web</a> are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 242.</li> <li>By clicking on the icon  (Remove), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 65: 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. 286: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 235.

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

### Group field Virtualization

#### Virtualization

☐ VM without Trusted License

Fig. 287: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> <li>• <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 66: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

### Tab Media Streamer

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

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



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

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

PBX +

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

Save
Reset

Fig. 288: Servers module - tab Media Streamer

2. Enter the following parameters:

<b>PBX</b>	<p><b>PBX</b> that the Media Streamer is supposed to be mapped to.</p> <p>Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.</p> <p>If no <b>PBX</b> has been created in the system yet, you can create a <b>PBX</b> via the blue bar <b>PBX</b>, see <a href="#">chapter "Create PBX"</a>, p. 250.</p>
<b>Extension</b>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <b>8000</b>.</p>
<b>Media streamer IP address</b>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <b>SIP</b> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <b>169.254.254.100</b> in the drop-down list.</p>
<b>Minimum port</b>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<b>Maximum port</b>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p>



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

### Tab Replay Server Address Mapping

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

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




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

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

---

**Replay Server Addresses**

 Remove Replay Server Addresses

Internal IP address/ port of the replay server:  :

Internal download URL:

External address/ port of the replay server:  :

External download URL:

Fig. 289: Servers Module - tab Replay Server Address Mapping

### Group field Replay Server Addresses

1. Enter the following parameters

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

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



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

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



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



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

### Tab Key Management

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

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

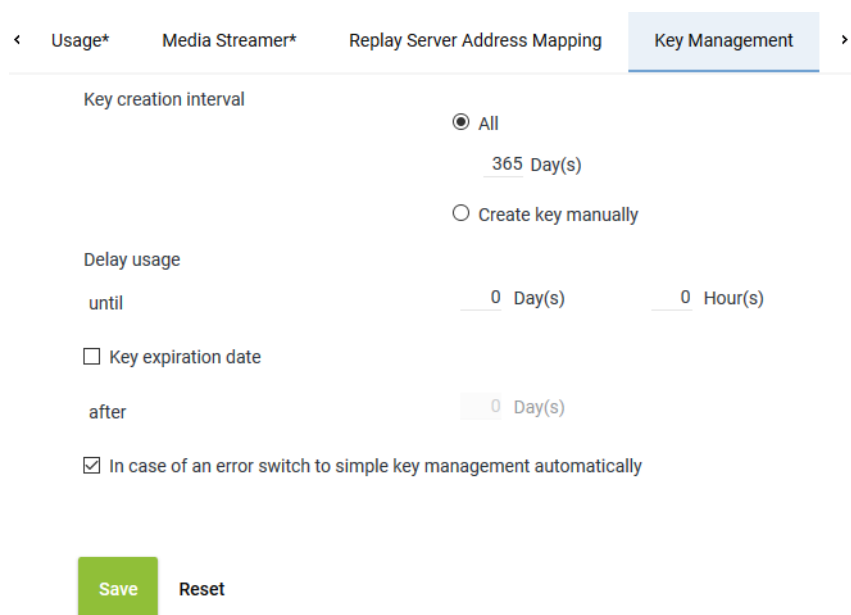


Fig. 290: Servers module - tab Key Management

<b>Key creation interval</b>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually. Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</li> </ul>
<b>Delay usage</b>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption. Possible time interval: 0 to 14 days Default value: 0 days (new keys are immediately used for encryption) A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<b>Key expiration date</b>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p>

	<p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

#### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.  
In this case, no separate configuration is required.  
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*  
In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*  
**NOTICE! License Management does not support encryption.**

#### For licensing, there are the following options:

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on. In this case, no separate configuration is required.

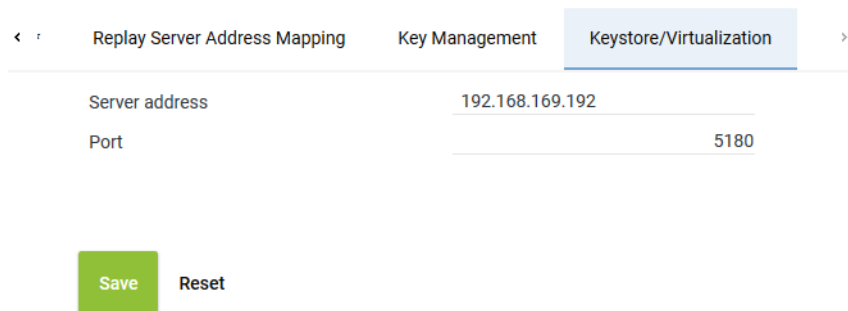
- *Trusted Virtualization License*

Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this. In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



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

Fig. 291: Servers module - tab Keystore/Virtualization

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



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

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

### 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:

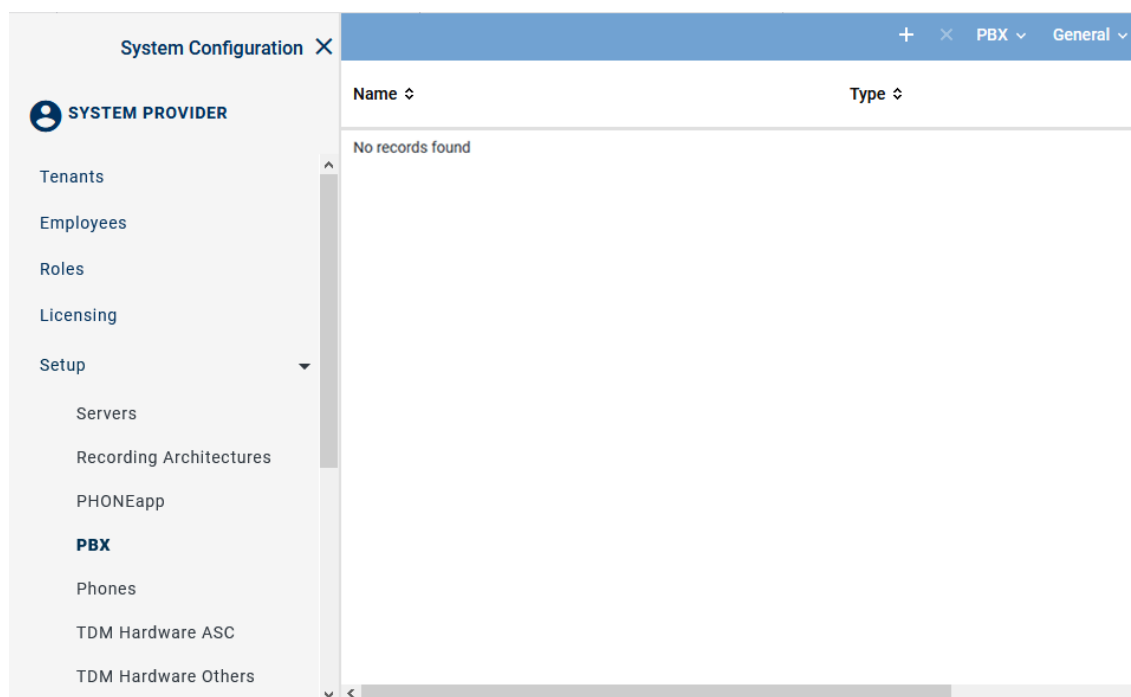


Fig. 292: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

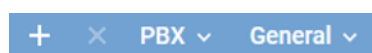




Fig. 293: Toolbar PBX module


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

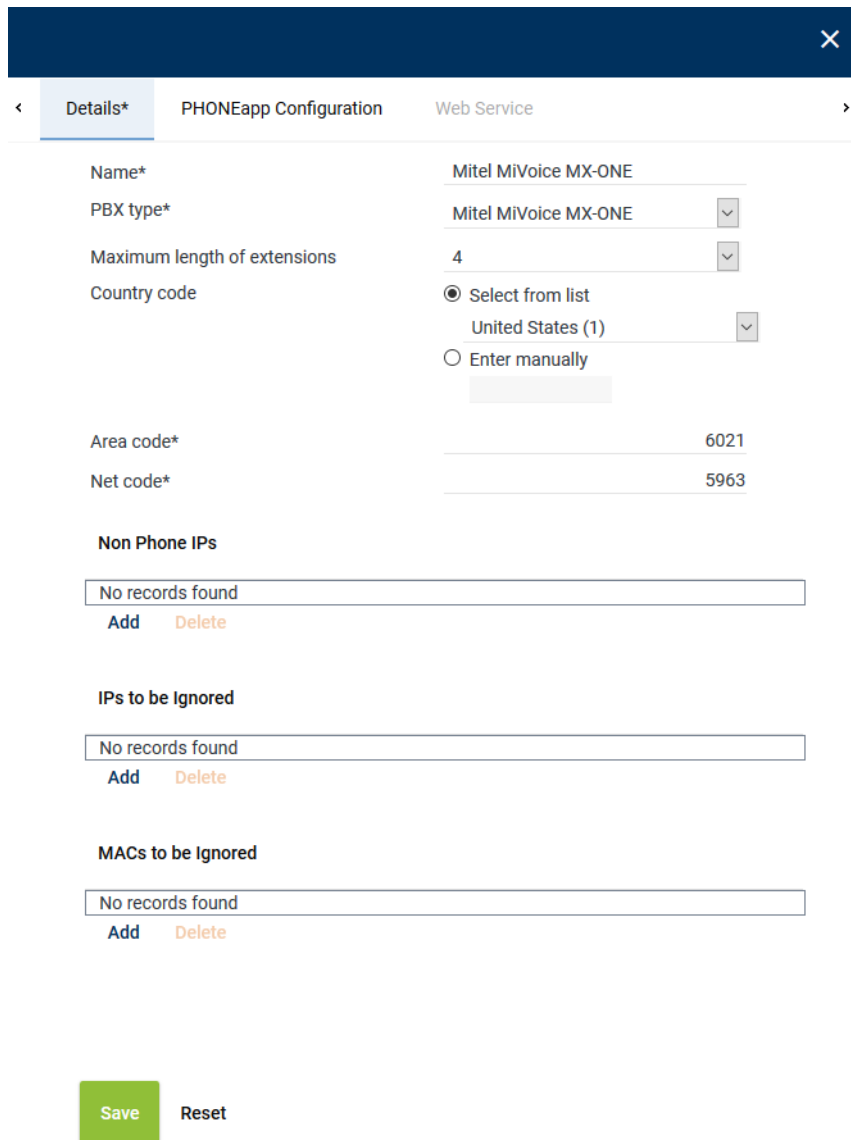
*Module Help* Opens the module-specific online help.



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

### Create new PBX

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



The screenshot shows a web interface for creating a new PBX. At the top, there's a dark blue header bar with a close button (X). Below it, there are three tabs: 'Details\*' (selected), 'PHONEapp Configuration', and 'Web Service'. The 'Details\*' tab contains the following fields:

- Name\***: Mitel MiVoice MX-ONE
- PBX type\***: Mitel MiVoice MX-ONE (dropdown)
- Maximum length of extensions**: 4 (dropdown)
- Country code**: ☒ Select from list (United States (1) dropdown) or ☐ Enter manually
- Area code\***: 6021
- Net code\***: 5963

Below these fields, there are three sections for ignored records:

- Non Phone IPs**: No records found. Buttons: Add, Delete.
- IPs to be Ignored**: No records found. Buttons: Add, Delete.
- MACs to be Ignored**: No records found. Buttons: Add, Delete.

At the bottom, there are two buttons: a green 'Save' button and a 'Reset' button.

Fig. 294: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the <b>PBX</b> from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <li><i>Select from list</i></li> </ul>

Parameter	Value/Description
	Select the country code from the drop-down list. <ul style="list-style-type: none"> <li>• <i>Enter manually</i></li> </ul> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka <i>094</i> .
Area code	Enter the area code without the preceding 0, e. g. 6021.
Net code	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 67: 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

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

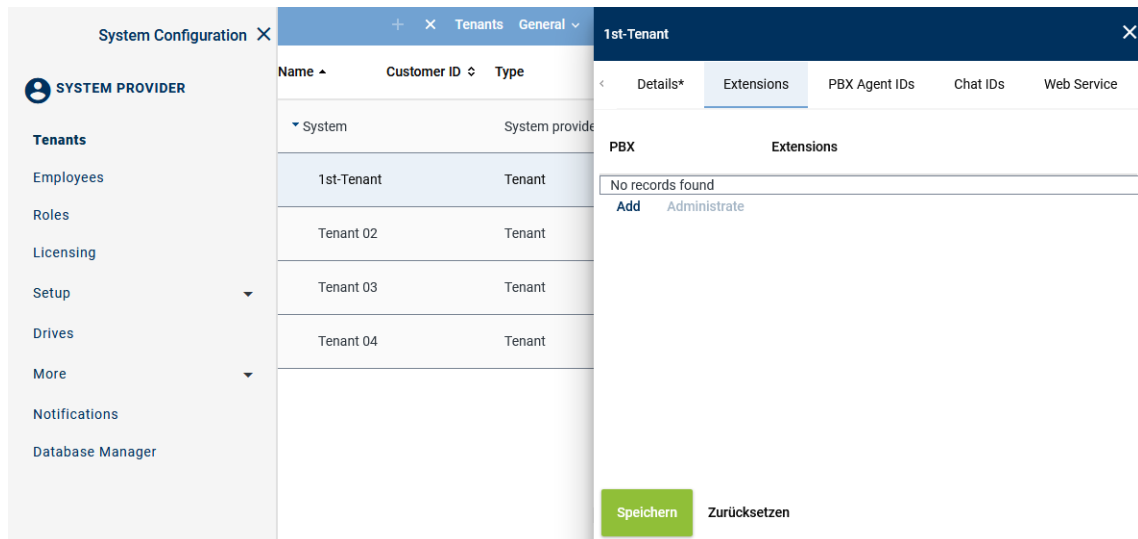


Fig. 295: Tenants - main view - tab Extensions

##### 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. 296: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>• ZIP</li> <li>• TXT</li> <li>• CSV</li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <span style="background-color: #f0f0f0; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <span style="background-color: #4f81bd; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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

Enter country codes as number ranges as follows:  
+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions*

Activate the check box to replace the list of extensions.

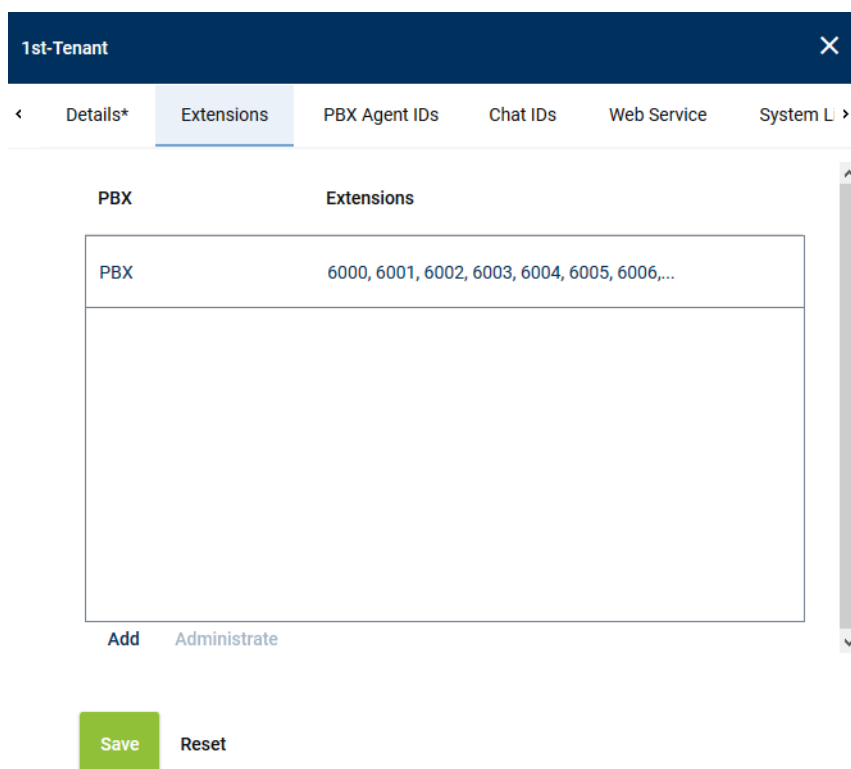
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

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

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

### Remove extensions

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



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

Fig. 297: 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. 298: 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.

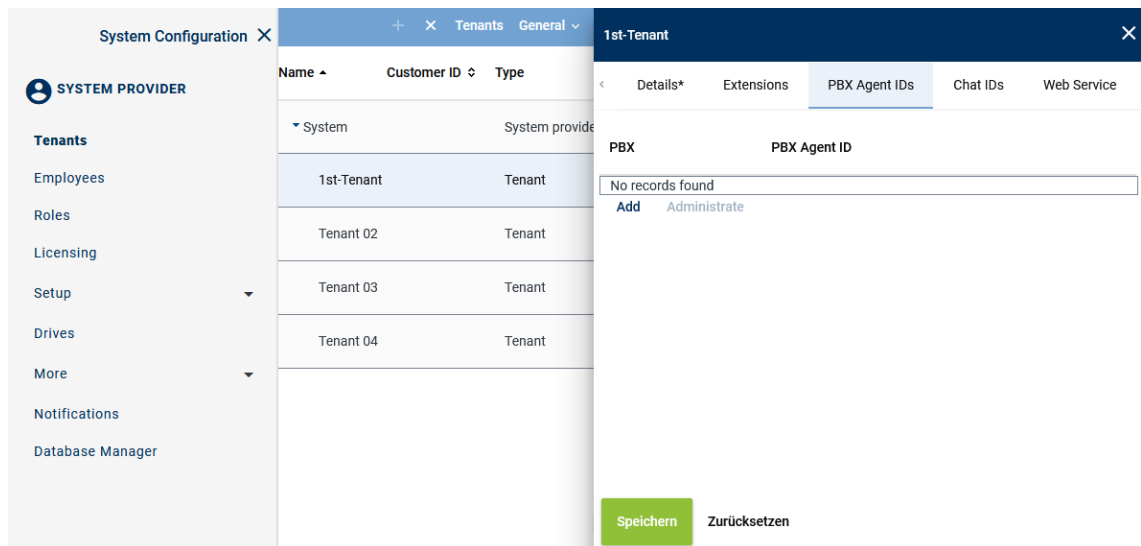


Fig. 299: Tenants - main view - tab PBX Agent ID

### 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:

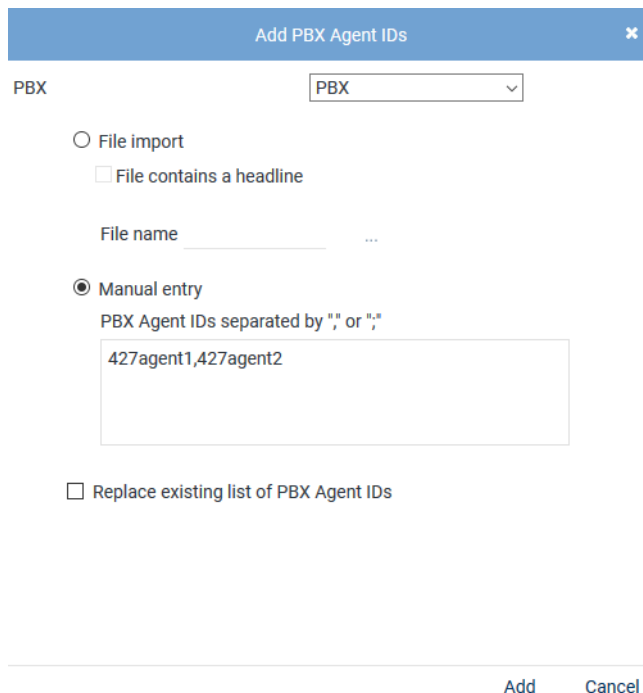


Fig. 300: Assign PBX Agent IDs to tenants

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

**File import** Select the option to import PBX Agent IDs from an existing [CSV](#) file and add them to the table of PBX Agent IDs.

*File contains a headline*

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
	<p><b>File name</b></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>Upload File</b>.</li> </ul>
<b>Manual entry</b>	<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><b>NOTICE! Wildcards cannot be used!</b></p>
<b>Replace existing list of PBX Agent IDs</b>	<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. 301: 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.

**System Configuration** ✕

 **SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 302: 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. 303: 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. 304: 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 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:

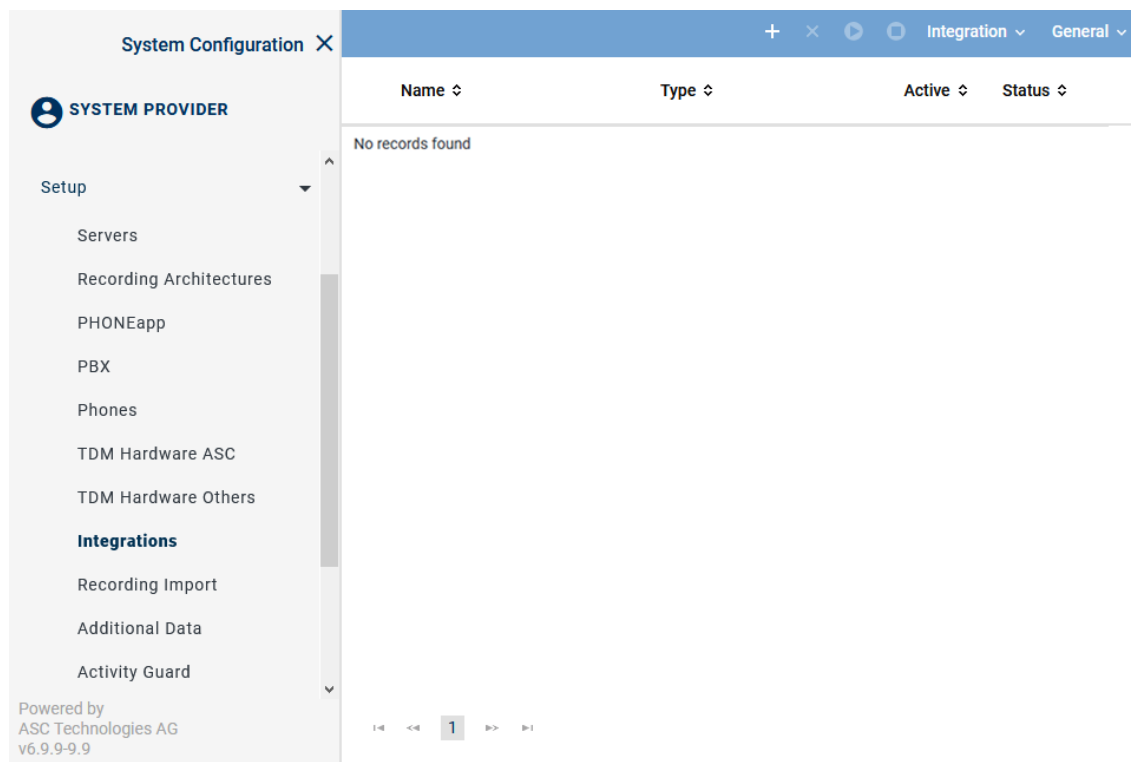




Fig. 305: Integrations - main view

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

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

### Toolbar of the Integrations module

The toolbar offers the following functions.

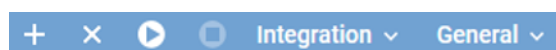






Fig. 306: Toolbar Integrations module

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



	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

- 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.

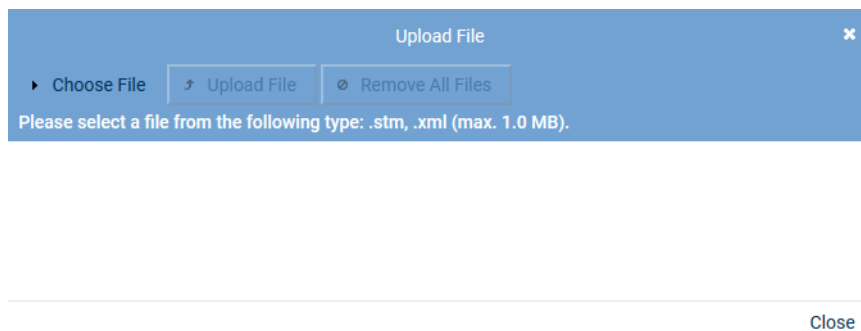


Fig. 307: Choose file

- 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*.

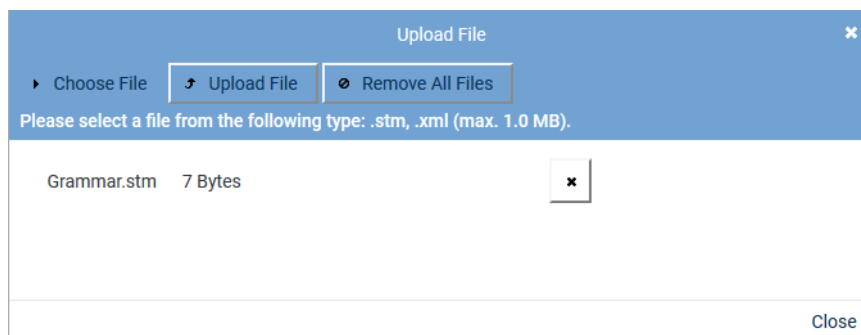



Fig. 308: Upload grammar

- 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. 309: Create integration type

- Enter the following parameters:

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

Tab. 68: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

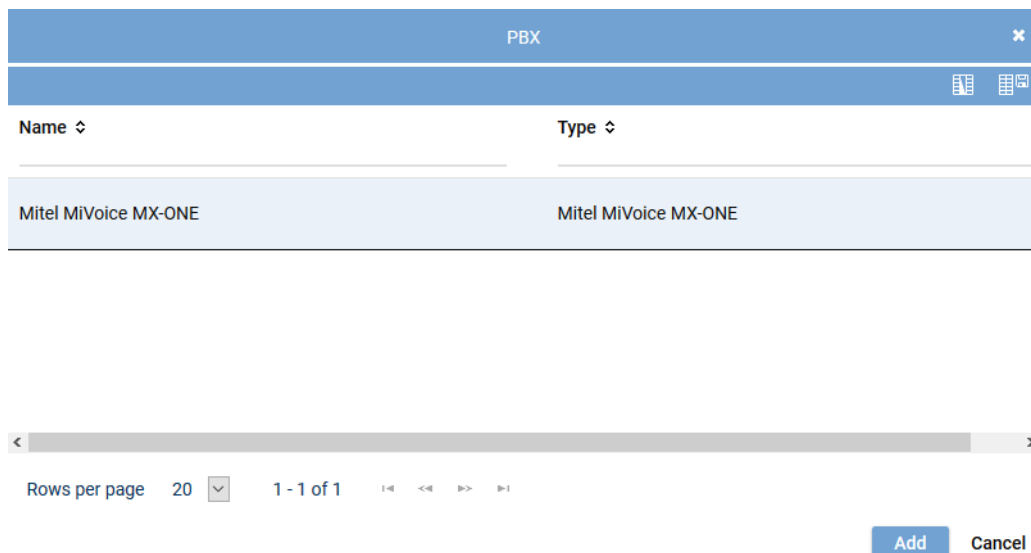


Fig. 310: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

### Assign recording architecture for Multi-Server Recording

- In the detail view on the bottom right, click on the button *Next*.

⇒ The tab *Recording Architecture* appears.

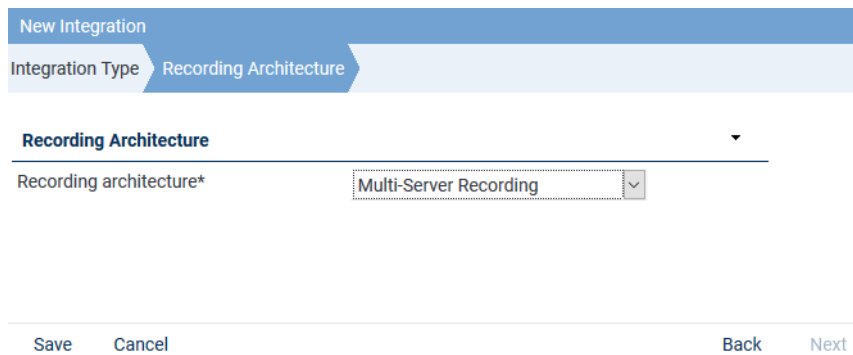


Fig. 311: Assign recording architecture - Multi-Server Recording


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



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

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

### Configuration steps

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









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. 312: 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.

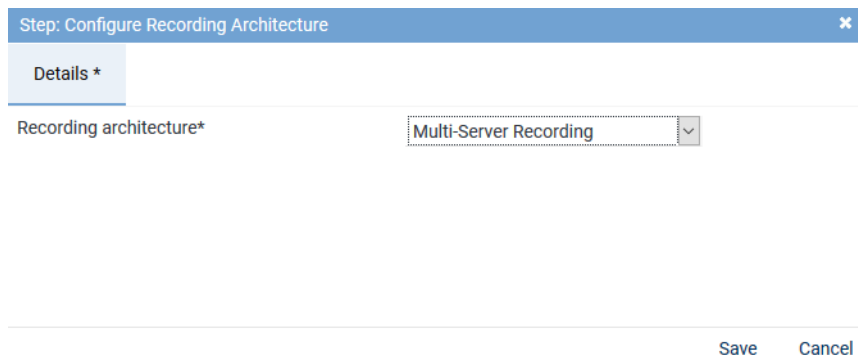



Fig. 313: Configuration step - Configure Recording Architecture

- 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab *MiVoice MX-ONE (CSTA)*

- Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\*
MBG\*

CTIconnect Module

Connection Data

Additional Data

Failover waiting time\*
10

Failover repetitions\*
3

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}\$

Save
Cancel

Fig. 314: CTI connection data - tab MiVoice MX-ONE (CSTA)

By configuring the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

The [CSTA](#) connection is used to monitor the configured monitor points and to start the recording by means of the intrusion feature.



Following an update, you must configure this section 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
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 69: 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 MiVoice MX-ONE (CSTA)

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.

**Connection Data** ▼

---

**PBX IP address**

No records found

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

Fig. 316: 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
✕

PBX IP address\* 192.168.170.219

PBX CSTA port\* 8882

Transport Layer Security (TLS) ☐

☒ Activate authentication

Application ID\* 1234

Password\* ●●●●●●●●●●●●●●●●

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

Fig. 317: Configure connection data

2. Enter the following parameters:

Parameter	Value/Description
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the <a href="#">CSTA</a> connection is supposed to run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate this check box to use the connection with <a href="#">TLS</a> .
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14</a> .
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14</a> .

Parameter	Value/Description
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 70: Configure connection data

- 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.

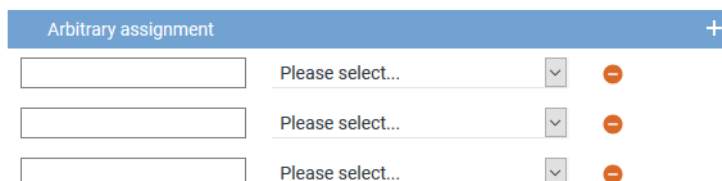



Fig. 318: Arbitrary assignment of the additional data

The following additional data is always available:

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

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

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



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



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

### Configure 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 CTIconnect 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. 319: Configure switching conditions

<b>Failover waiting time</b>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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.
<b>Failover repetitions</b>	Enter how many times the CTI <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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]?$|^\\s[0-9]{4}[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 320: 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.



As parallel recording is only possible via the **MBG**, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

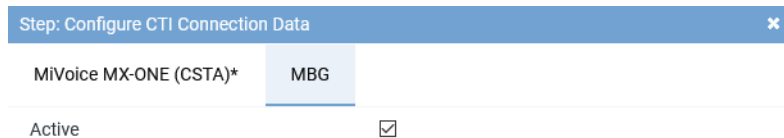


Fig. 321: Activate CTIconnect connection data for [MBG](#)

**Active** Activate the check box to display the configuration parameters and to activate the connection to the [MBG](#).

☒ = Connection has been activated.

☐ = Connection has not been activated.



Following an update, you must configure this section again.

### Group field CTIconnect Module

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

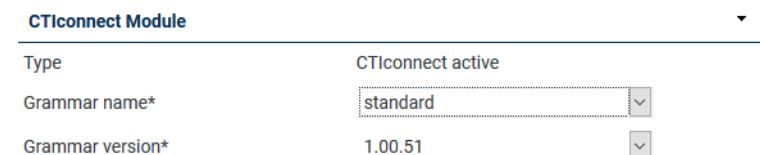


Fig. 322: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 71: 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 MBG

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

**Connection Data** ▼

---

Connection data

No records found

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

Fig. 323: Group field Connection Data

1. In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

Configure Connection
✕

Connection data*	192.168.170.116
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>
<input checked="" type="checkbox"/> Use pre-shared key	
Pre-shared key (PSK)*	●●●●●●●●

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

Fig. 324: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the <a href="#">MBG</a> .
<i>PBX port</i>	Enter the port for the <a href="#">MBG</a> or the <a href="#">SRC</a> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <a href="#">MBG</a> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 72: 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 MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

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.

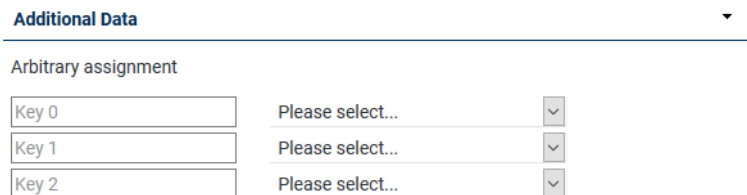


Fig. 325: CTI connection data - additional data module 1

2. Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
3. From the drop-down list, select the entry which is supposed to appear as column headline in the players.
4. Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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.

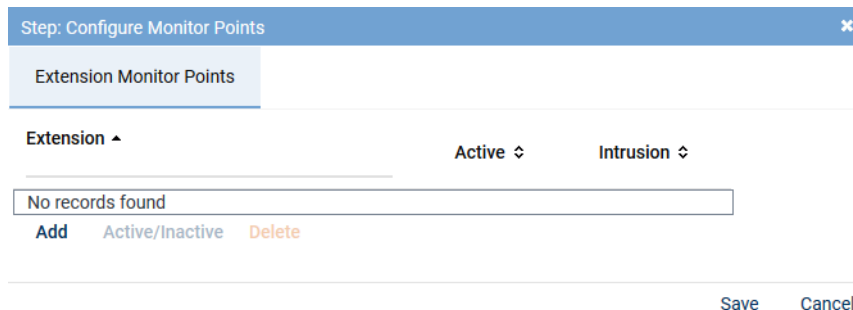


Fig. 326: Configuration step - configure monitor points

### Tab 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.

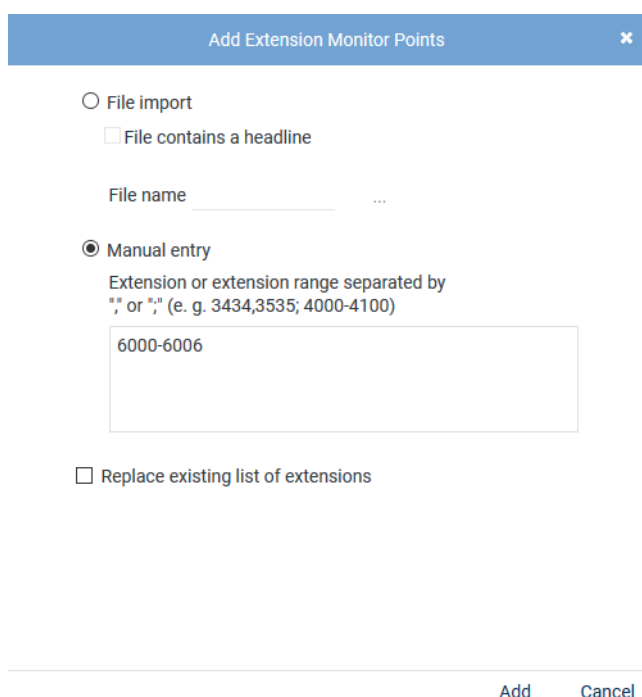



Fig. 327: Add extension monitor points

<b>File import</b>	<p>Select this option to import extensions from an existing <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>↗</b> (<i>Upload file</i>).</li> </ul>
<b>File contains a headline</b>	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
<b>File name</b>	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> </ul>

	<ul style="list-style-type: none"> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button  (<i>Upload file</i>).</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>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><b>NOTICE! Wildcards cannot be used!</b></p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; 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 <span>✕</span>		
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 href="#">Add</a> <a href="#">Active/Inactive</a> <a href="#">Delete</a>		
<div>Save   Cancel</div>		

Fig. 328: Configured extension monitor points

<i>Add</i>	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.
<i>Active/Inactive</i>	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.
<i>Delete</i>	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.
<i>Intrusion</i>	<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<sup>connect</sup> 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. 16](#).

### Global recording settings

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

Step: Global Recording Settings
✕

Details\*

Transport protocol	UDP	▼
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. 329: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i>, the transport protocol applies for the SIP communication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p><b>TCP</b> = unencrypted</p> <p><b>UDP</b> = unencrypted</p> <p><b>TLS</b> = encrypted</p>
<i>Port SIP signaling</i>	Enter the port for <b>SIP</b> signaling that is opened on the recording server for incoming <b>SIP</b> communication and that has been selected in the outgoing <b>SIP</b> notifications as the port of the recording server. Default <b>5060</b> .
<i>Remote SIP port</i>	Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by <b>SIP</b> to start <i>active-stream recording</i> . Default <b>7300</b> .
<i>Activate SIP authentication</i>	Activate the check box if <b>SIP</b> 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 <b>SIP</b> registration of extensions recorded with intrusion feature. The user name is configured in the <b>PBX</b> and applies for all extensions to be registered.



Parameter	Value/Description
<i>Password of the SIP registration</i>	Enter the password for <a href="#">SIP</a> registration of extensions recorded with intrusion feature. The password is configured in the <a href="#">PBX</a> 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 <a href="#">PBX</a> .
<i>PBX port</i>	Enter the port for the communication with the <a href="#">PBX</a> , default 5060.


Tab. 73: Global recording settings

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



Following an update, you must configure this section 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.

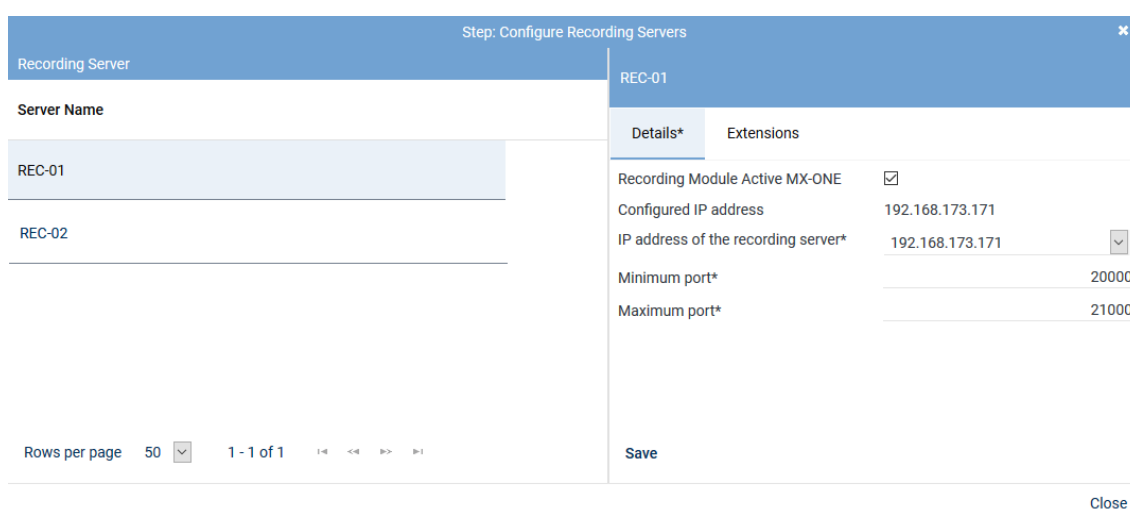


Fig. 330: Configuration step - Configure recording servers

- 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 <a href="#">RTP</a> 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 <b>RTP</b> data from the recording server, e. g. 21000.

Tab. 74: 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.



Following an update, you must configure this section 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*.

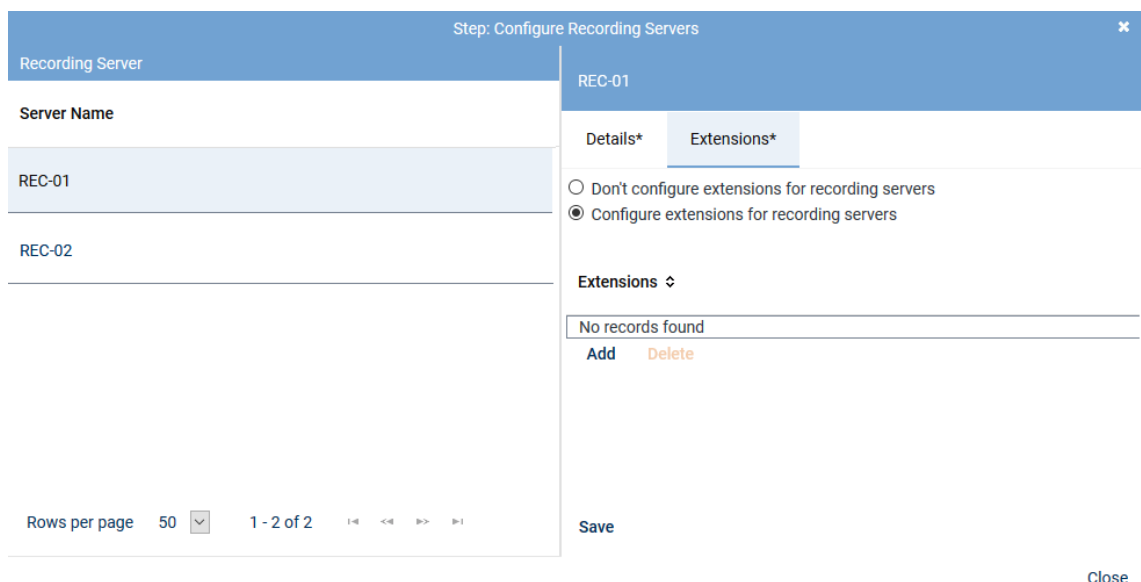


Fig. 331: Tab Extensions

**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. 332: 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.

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;"> <p>9999</p> </div> <p style="text-align: center;"> <a href="#">Add</a>   <a href="#">Delete</a> </p> <p style="text-align: center; margin-top: 10px;"><a href="#">Save</a></p>

Rows per page 50 ▼   1 - 2 of 2   << < > >>

[Close](#)

Fig. 333: 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.



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

### 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. 334: 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	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 75: 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. 76: 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.

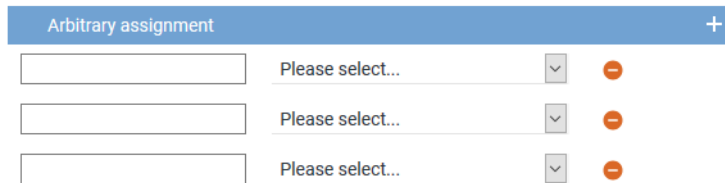



Fig. 335: Arbitrary assignment of the additional data

The following additional data is always available:

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

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



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



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

### **Configure add-on for 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<sup>connect</sup> 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

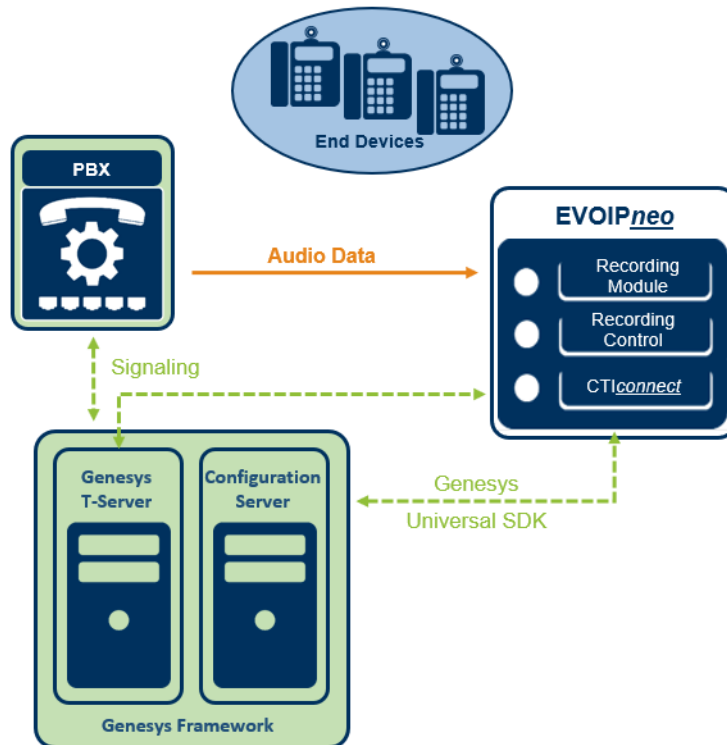


Fig. 336: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

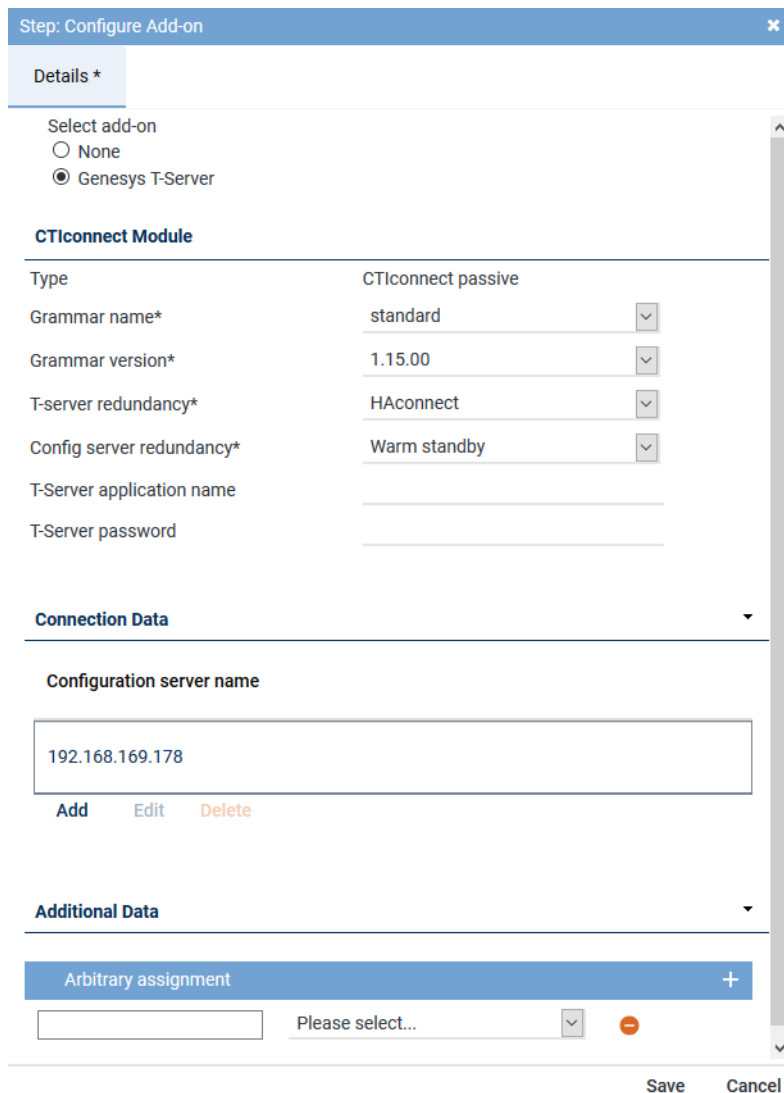


Fig. 337: Configure add-on for Genesys T-Server

### 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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. 77: 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:

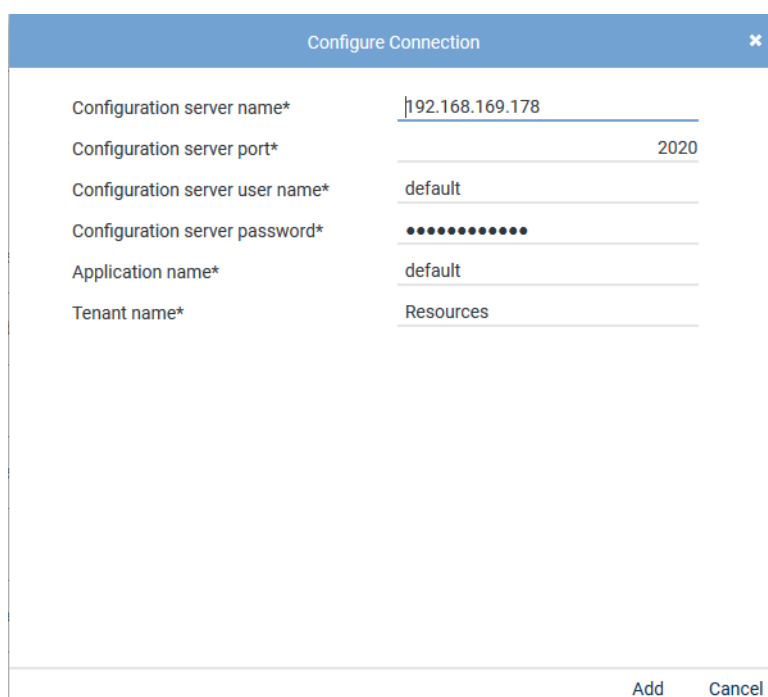


Fig. 338: Configure connection data

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. 78: 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. 339: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

### Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

▼

Save

Cancel

Fig. 340: 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. 341: 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. 342: 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. 343: Deactivate integration

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

## 7.3.2.5 Configure recording solution Multi-Server Failover

### 7.3.2.5.1 Create recording architecture

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

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

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

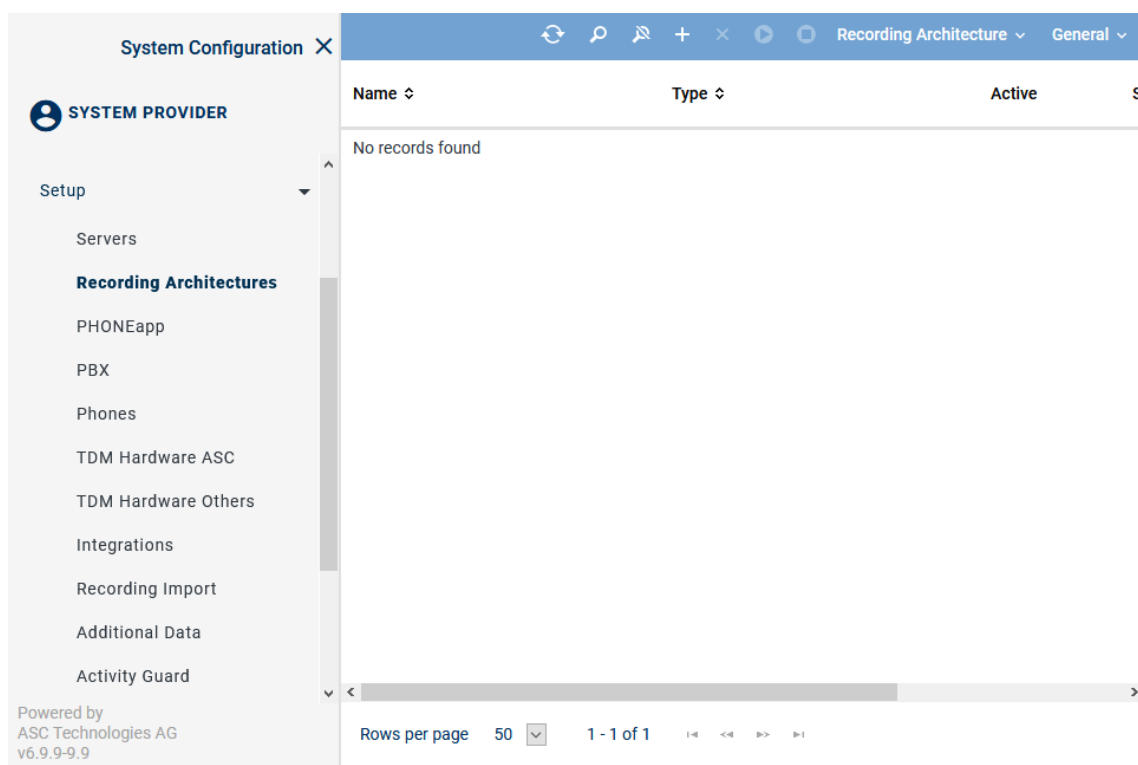




Fig. 344: Recording architectures - main view

<b>Name</b>	Name of the recording architecture
<b>Type</b>	Type of the recording architecture
<b>Active</b>	Shows whether the recording architecture has been activated and is ready to be used for the recording. ✓ = 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.
<b>Standby Active</b>	Shows whether the standby server is active for one or several recording components in the recording architecture. ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined.
<b>Creation Date</b>	Date on which the recording architecture was installed.
<b>Updated</b>	Date on which the settings of the recording architecture were updated for the last time.



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








### Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 345: Toolbar Recording Architectures module

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


		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. <b>NOTICE!</b> You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	Deactivates the selected recording architecture. <b>NOTICE!</b> You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
<i>Recording Architecture</i>	<i>Standby Management</i>	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Create recording architecture 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.

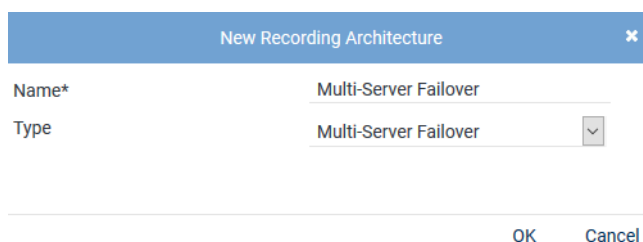


Fig. 346: Create recording architecture - Multi-Server Failover

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

3. From the drop-down list *Type*, select the recording architecture type *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.

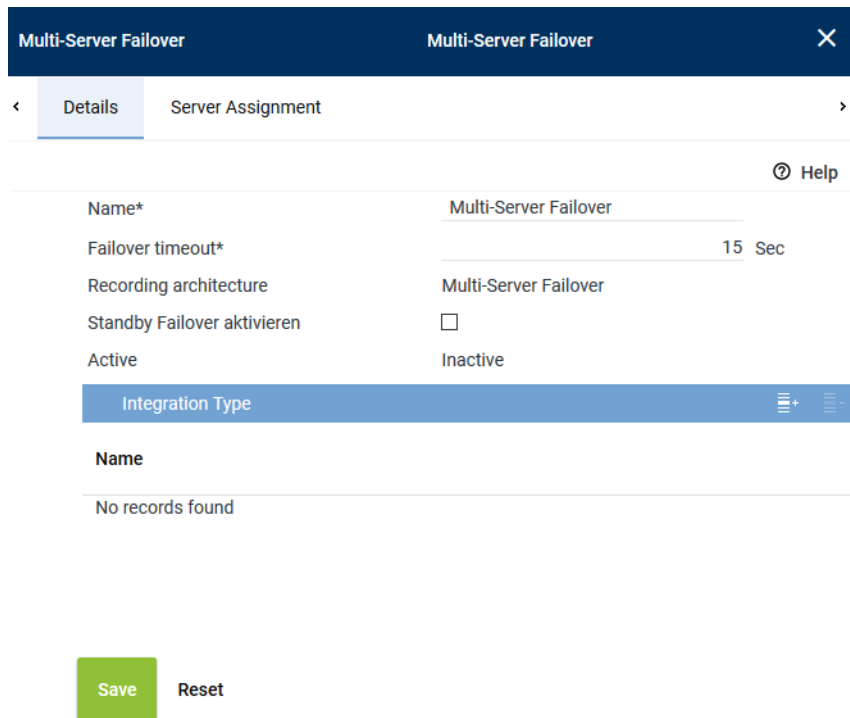


Fig. 347: Recording architecture - tab Details - Multi-Server Failover

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. 450](#).

<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><b>NOTICE!</b> 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><b>NOTICE!</b> 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><b>NOTICE!</b> 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

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



⇒ The window *Integration Type* appears.

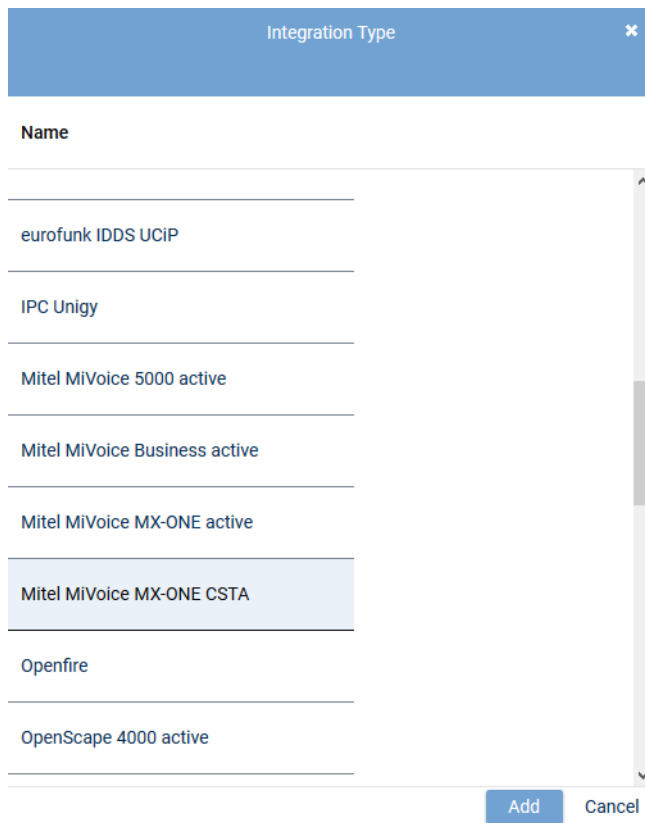


Fig. 348: Select integration type



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 Multi-Server Failover**

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

### **Group field Recording Control and CTIconnect**

In this group field, you can configure recording control. You can configure two different 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*	RC-01	+	-
Used in activated architecture	No		

Standby Server

▼

Recording Control standby*	RC-02	+	-
Used in activated architecture	No		
CTIconnect standby*	RC-02	+	-
Used in activated architecture	No		

Recording Server

▼

< Recording Server

+

✎

⋮

Server ↕	Standby ↕
REC-01	REC-02

↑

↓

Save

Reset

Fig. 349: 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. 350: 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. 351: 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. 352: Recording architecture - activate recording architecture

- To deactivate the recording architecture, if required, click on the icon  (Deactivate).

⇒ In the column *Active*, the icon  (*Inactive*) appears.



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



For all recording architectures with failover components, you can manage to the standby components via standby management. This holds true for Multi-Server Recording and Multi-Server Parallel Recording systems if redundancy options are available for these systems. See [chapter "Standby management for failover architectures", p. 450](#).



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

### 7.3.2.5.2 Configure server

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

- In the navigation bar, select the menu item *Setup > Servers*.

⇒ The following window appears:

System Configuration X		Servers ▾ General ▾	
SYSTEM PROVIDER		Name ▾	IP Address ▾
Setup		CTI-01	192.168.173.177
Servers		CTI-02	192.168.173.178
Recording Architectures		RC-01	192.168.173.175
PHONEapp		RC-02	192.168.173.176
PBX		REC-01	192.168.173.171
Phones		REC-02	192.168.173.172
TDM Hardware ASC		REC-03	192.168.173.173
TDM Hardware Others		REC-04	192.168.173.174
Integrations			
Recording Import			
Additional Data			
Activity Guard			

Fig. 353: 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. 354: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.  The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <i>neo</i> system.
<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 298</a> .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <i>Administrate NTP server</i> .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Administrate server locations

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

### Add server locations

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

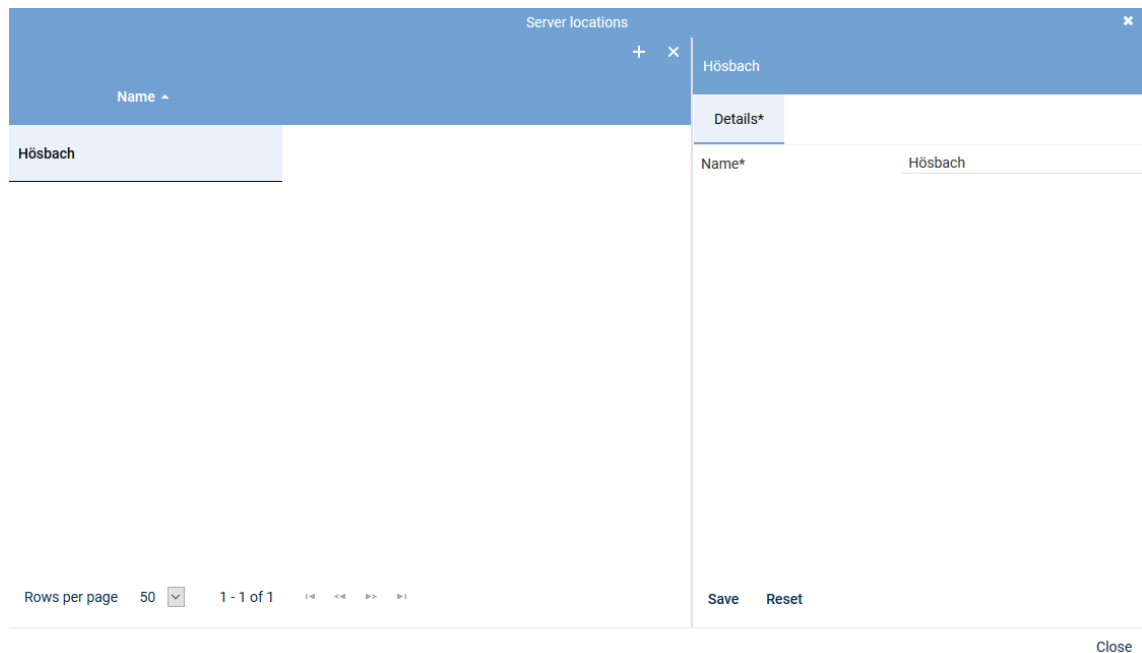



Fig. 355: Add server locations

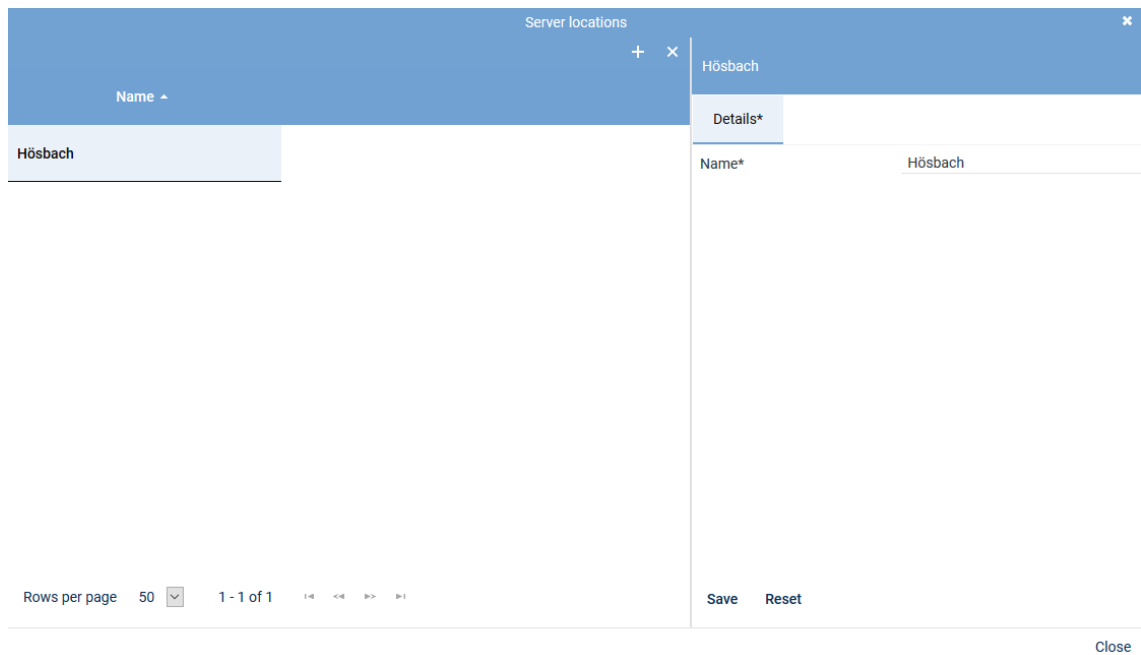
- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.
- To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
- To add further locations, repeat the last 3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

### Delete server location




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

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



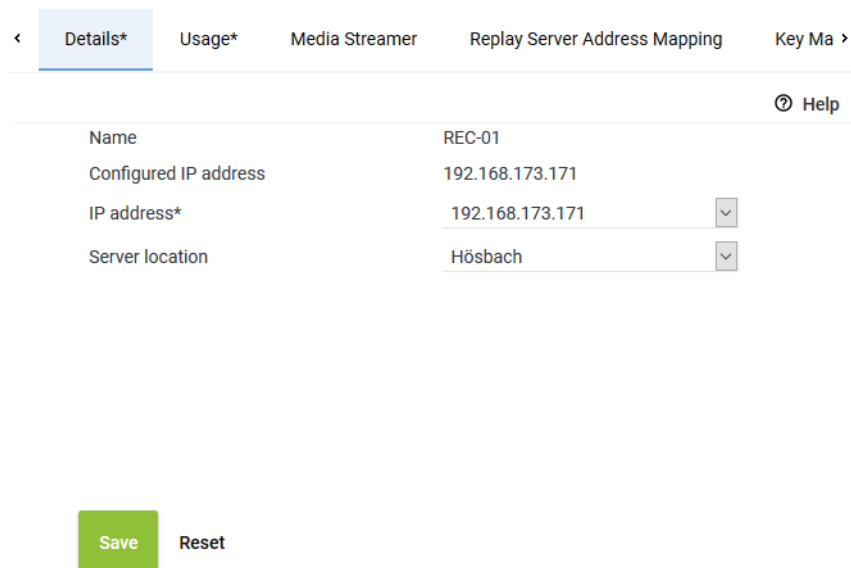
The screenshot shows a window titled "Server locations" with a close button (x) in the top right. Inside, there's a table with a header "Name" and one row containing "Hörsbach". To the right of the table is a "Details\*" tab. Below the table, there's a pagination bar showing "Rows per page 50" and "1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

Fig. 356: Delete server location



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

### Tab Details

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



The screenshot shows a window titled "Servers - tab Details" with a close button (x) in the top right. The window has a tabbed interface with "Details\*" selected. Below the tabs, there's a "Help" icon. The main content area contains a table with the following fields:

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

At the bottom left, there are "Save" and "Reset" buttons.

Fig. 357: Servers - tab Details

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



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

### Tab Usage

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



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

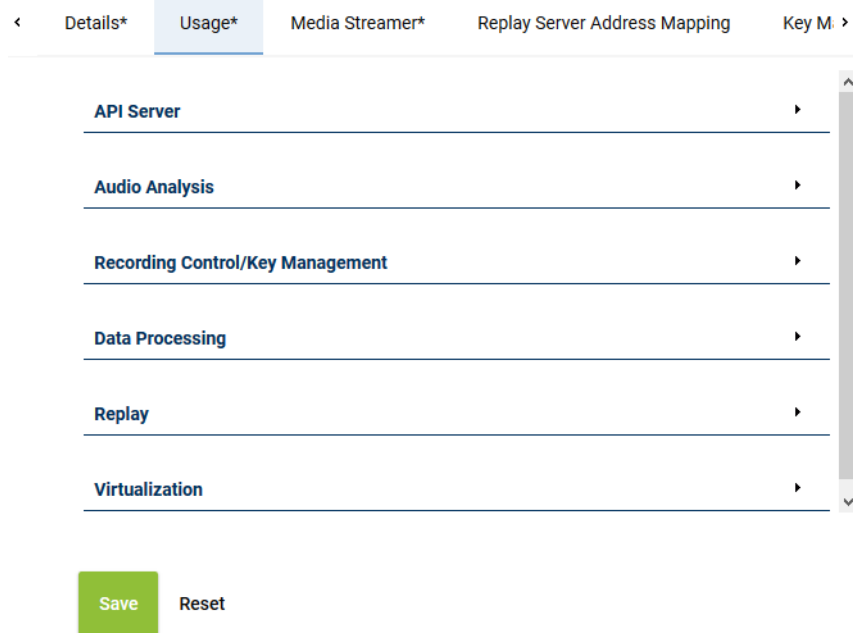


Fig. 358: Servers - tab usage

### Group field API Server

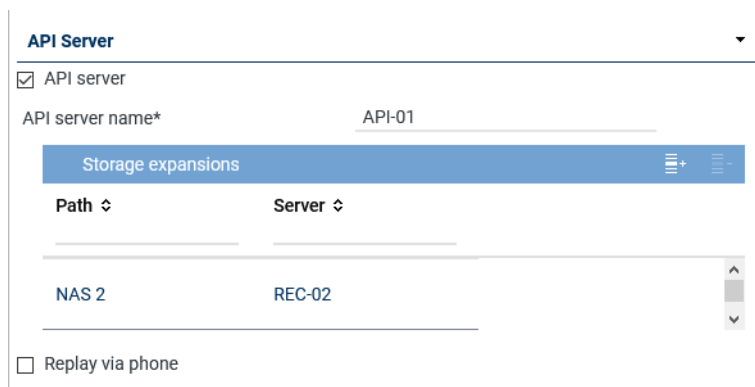




Fig. 359: Group field API Server

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


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

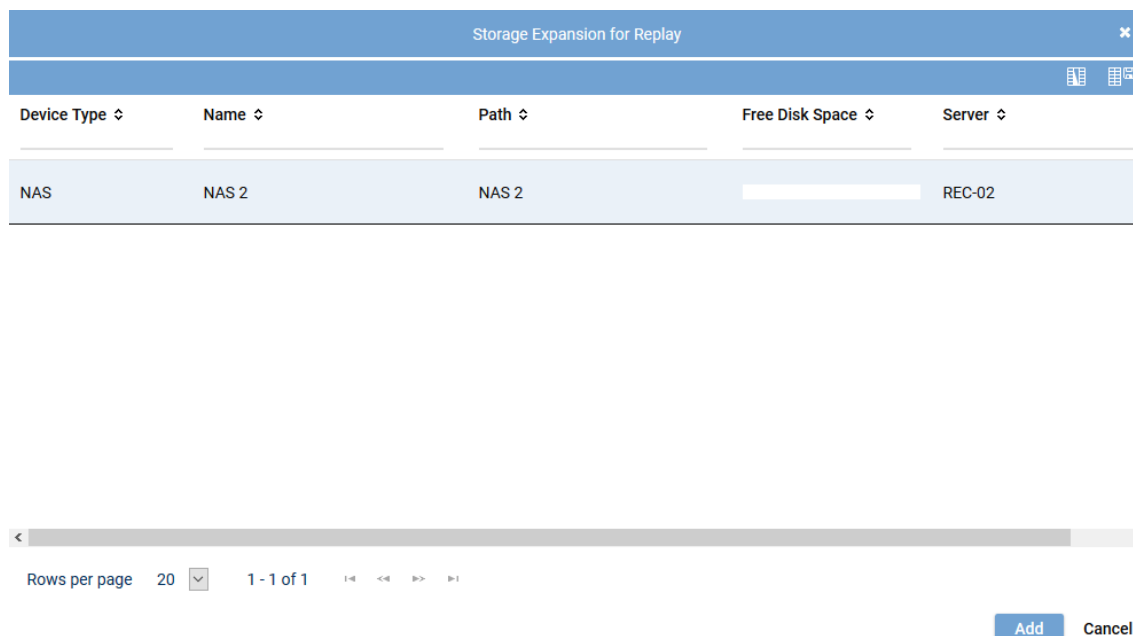
Furthermore, the ASC API Server is responsible for replay by means of the web applications. Not until the ASC API Server has started, can the replay server be activated and the corresponding ASC API Server assigned for replay in the web applications.

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

Parameter	Value/Description
	<p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping"</a>, p. 312.</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"> <li>• By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay"</a>, p. 303.</li> <li>• By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul> <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><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWER<i>play</i> Pro</li> <li>• Application POWER<i>play</i> Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a <i>PBX</i>, see <a href="#">chapter "Tab Media Streamer"</a>, p. 310. To be able to do so, at least 1 <i>PBX</i> must have been configured in the system.</p>

### Add storage expansion for replay

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



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

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 360: Select storage expansion

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

### Group field Audio analysis




**Audio Analysis**

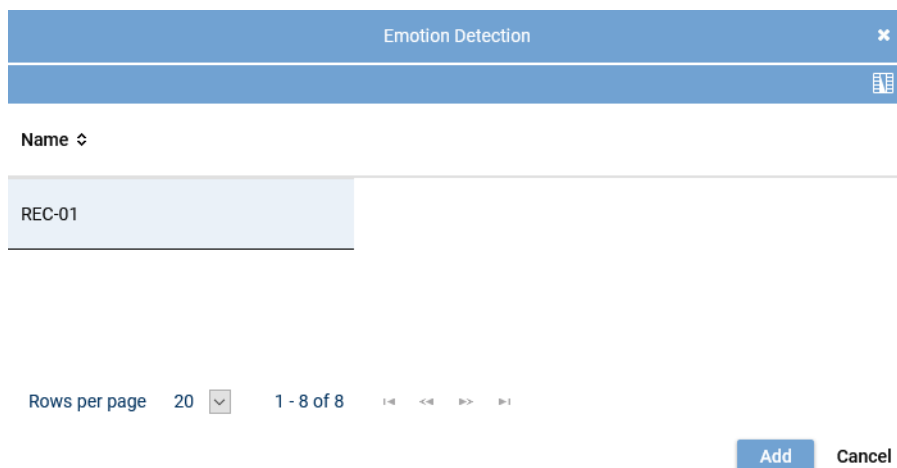
☒ Emotion detection

Stream audio data from\* REC-01 +

Fig. 361: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	Activate this check box to activate emotion detection for audio analysis.  <input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.  <input type="checkbox"/> = Function has not been activated.
<i>Stream audio data from</i>	If the function emotion detection has been activated, the parameter to select the respective server becomes active. <ul style="list-style-type: none"> <li>Click on the button  to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 79: Configure audio analysis



Emotion Detection

Name ↕

REC-01
--------

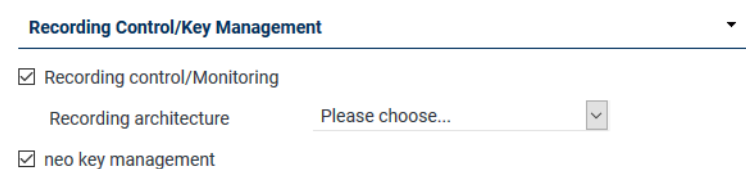
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 362: Select server for emotion detection

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

### Group field Recording Control/Key Management



Recording Control/Key Management

☒ Recording control/Monitoring

Recording architecture Please choose...

☒ neo key management

Fig. 363: Group field Recording Control/Key Management

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

Tab. 80: Configure recording control/key management

### Group field Data Processing

**Data Processing** ▼

☒ Data storage

☐ Transfer data for replay

Target Server

Name	IP Address ↕
No records found	

☒ Transfer data for data storage

Target Server

Name	IP Address ↕
No records found	

Activate period of time ☒

Start

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server

☒ Import

Recording architecture

Fig. 364: Group field Data Processing


Parameter	Value/Description
<i>Data storage</i>	Activate the check box to make additional functions of data processing available for editing.
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 307</a>.</li> <li>By clicking on the icon  (Remove), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be trans-</p>

Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list"</a>, p. 307.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b> For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>
<i>Archiving</i>	<p>Activate the check box <i>Archiving</i> if you would like to use the server for archiving purposes.</p>
<i>Export</i>	<p>Activate the check box <i>Export</i> to allow the export from this server.</p> <ul style="list-style-type: none"> <li><i>Replay server</i> From the drop-down list, select the replay server where the exported recordings are supposed to be replayed after export. The drop-down list displays all servers which have been configured as replay servers.</li> </ul> <p><b>NOTICE!</b> For the export from <i>neo</i> to <i>neo</i>, you do not have to select a replay server.</p>
<i>Import</i>	<p>Activate the check box <i>Import</i> so that the imported data can be saved on this server.</p> <ul style="list-style-type: none"> <li><i>Recording architecture</i> From the drop-down list, select the recording architecture which is supposed to serve this function. The drop-down list displays all recording architectures which enable this function.</li> </ul>

Parameter	Value/Description
	<b>NOTICE!</b> If you would like to use a server for the import where no recording is supposed to take place, you can create an architecture for the import only.

Tab. 81: Data storage

### Add target server to a list

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



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

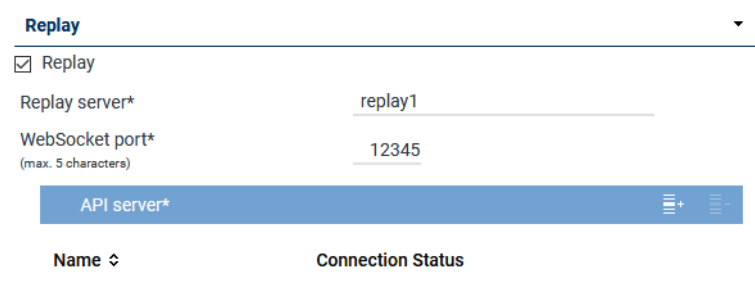
Fig. 365: Select server



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

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

### Group field Replay





**Replay**

☒ Replay

Replay server\*



WebSocket port\*   
(max. 5 characters)

API server\*  

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

Fig. 366: Group field Replay

Parameter	Value/Description
<i>Replay</i>	A replay server can replay recordings via the integrated <i>Replay Feature</i> . Only data which has either been recorded directly on this server or which has been transferred to this server for data stor-

Parameter	Value/Description
	<p>age or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API</a> 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 <a href="#">POWERplay</a> Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 308.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 82: 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.

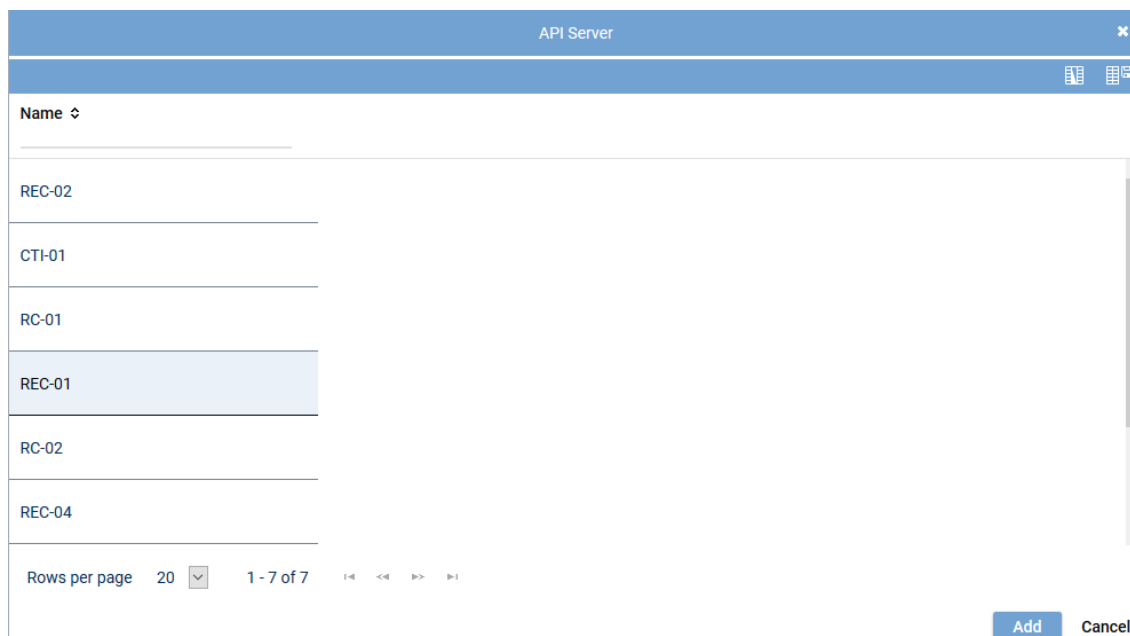


Fig. 367: Select server



Only those servers are available on which the **API** service has been installed and activated.  
See [chapter "Group field API Server", p. 301](#).

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. 368: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> </ul>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li><i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 83: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

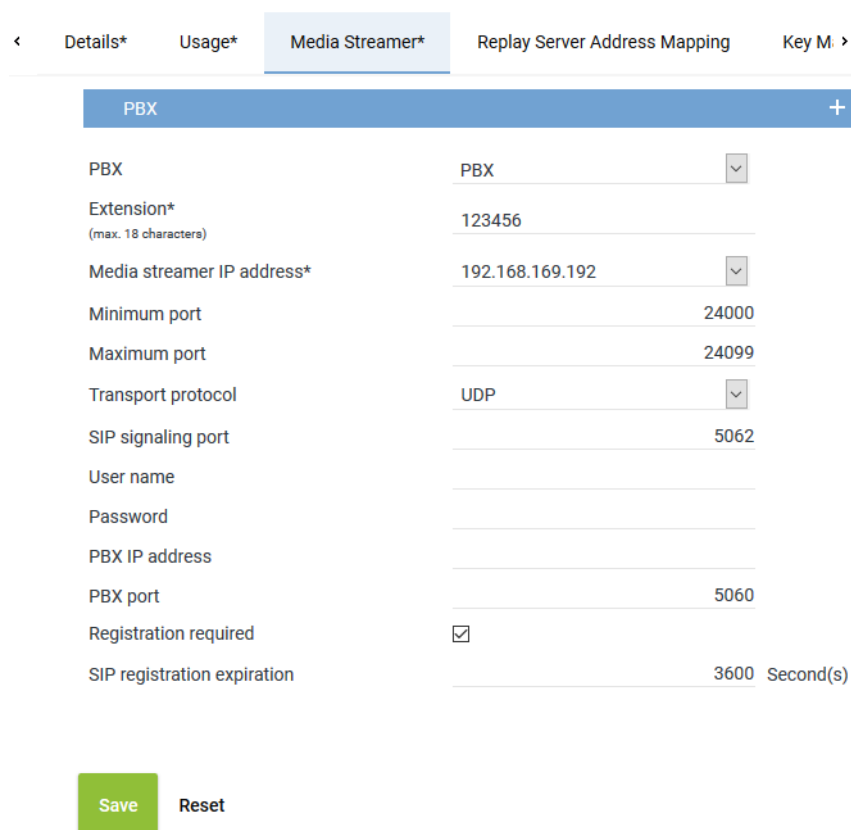
### Tab Media Streamer

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

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



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



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

PBX +

PBX	PBX	▼
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. 369: Servers module - tab Media Streamer

- Enter the following parameters:

<b>PBX</b>	<b>PBX</b> that the Media Streamer is supposed to be mapped to. Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.
------------	--

	<p>If no PBX has been created in the system yet, you can create a <a href="#">PBX</a> via the blue bar <i>PBX</i>, see <a href="#">chapter "Create PBX"</a>, p. 316.</p>
<i>Extension</i>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <i>8000</i>.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <a href="#">SIP</a> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <i>169.254.254.100</i> in the drop-down list.</p>
<i>Minimum port</i>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<i>Maximum port</i>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p> <p>A port range of 100 (e. g. 24000-24099) is sufficient for 50 licenses. The port range should be twice as wide as the number of available licenses.</p> <p><b>NOTICE! The port range must not have less than 64 ports.</b></p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the <a href="#">SIP</a> communication.</p> <p><a href="#">TCP</a> = unencrypted  <a href="#">UDP</a> = unencrypted  <a href="#">TLS</a> = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the <a href="#">SIP</a> communication.</p> <p>Port for data exchange: <i>5062</i></p>
<i>User name</i>	Enter the user name for the authentication on the <a href="#">SIP</a> server.
<i>Password</i>	Enter the password for the authentication on the <a href="#">SIP</a> server.
<i>PBX IP address</i>	<p>Enter the IP address of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the IP address <i>169.254.254.101</i>.</p>
<i>PBX port</i>	<p>Enter the port of the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p>If an external analog gateway has been integrated, enter the value <i>5060</i>.</p>
<i>Registration required</i>	<p>Select whether the <a href="#">SIP</a> extension has to be registered with the <a href="#">SIP</a> registrar of the <a href="#">PBX</a>.</p> <p><input checked="" type="checkbox"/> = <a href="#">SIP</a> extension has to be registered.  <input type="checkbox"/> = <a href="#">SIP</a> extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <i>Registration required</i>.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

### Tab Replay Server Address Mapping

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

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



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

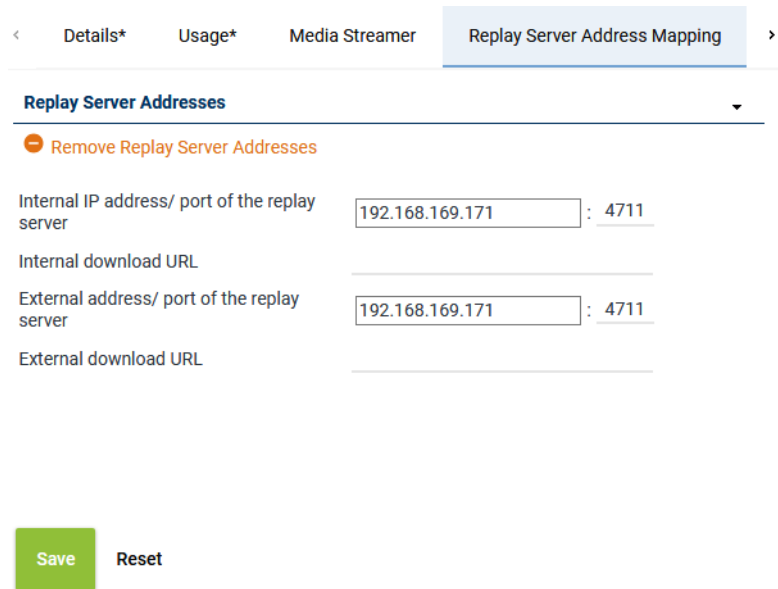


Fig. 370: Servers Module - tab Replay Server Address Mapping

### Group field Replay Server Addresses

1. Enter the following parameters

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

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



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

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



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

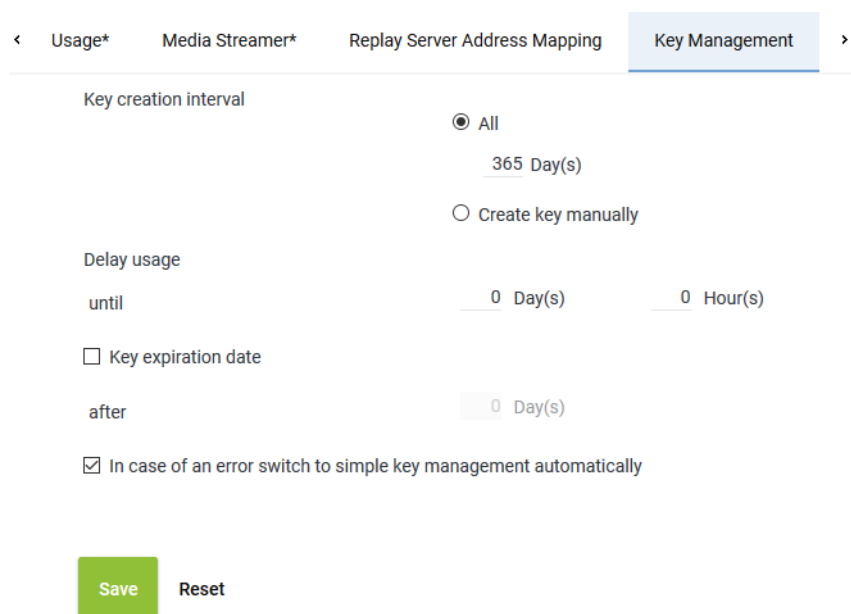


For information about the configuration refer to the administration manual for tenants *User management tenant*.

### Tab Key Management

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

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



< 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. 371: Servers module - tab Key Management

<b>Key creation interval</b>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually.</li> </ul> <p>Old keys which are no longer used for encryption become inactive for the time being. They remain in the database, though, since they are still required for the decryption of old recordings.</p>
------------------------------	--

<i>Delay usage</i>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</p> <p>Possible time interval: 0 to 14 days</p> <p>Default value: 0 days (new keys are immediately used for encryption)</p> <p>A delay guarantees that the key has been captured by a database backup before it will actually be used.</p>
<i>Key expiration date</i>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p> <p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.

In this case, no separate configuration is required.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.

- *Dongle Manager*

In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.

- *ASC License Management System*

**NOTICE! License Management does not support encryption.**

**For licensing, there are the following options:**

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes.

In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on.

In this case, no separate configuration is required.

- *Trusted Virtualization License*

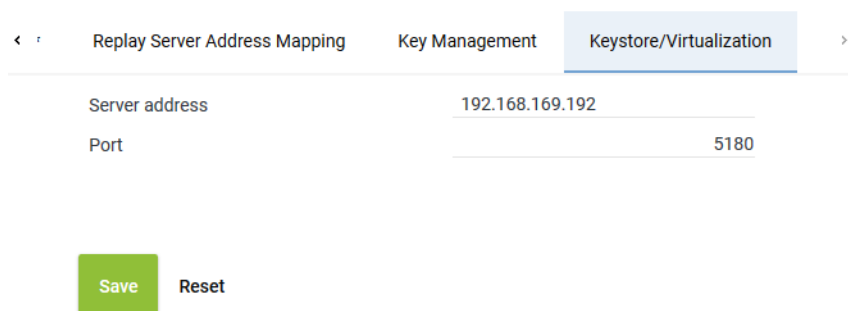
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



The screenshot shows a web interface for configuring the Keystore/Virtualization tab. It has three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization'. The 'Keystore/Virtualization' tab is active. Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom, there are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 372: Servers module - tab Keystore/Virtualization

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

	IP address of the server where the service <i>DongleMan</i> has been installed.
<i>Port</i>	Enter the port for the connection. 5180 = Dongle Manager 8181 = ASC License Management System



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

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

### 7.3.2.5.3 Create PBX

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

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

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

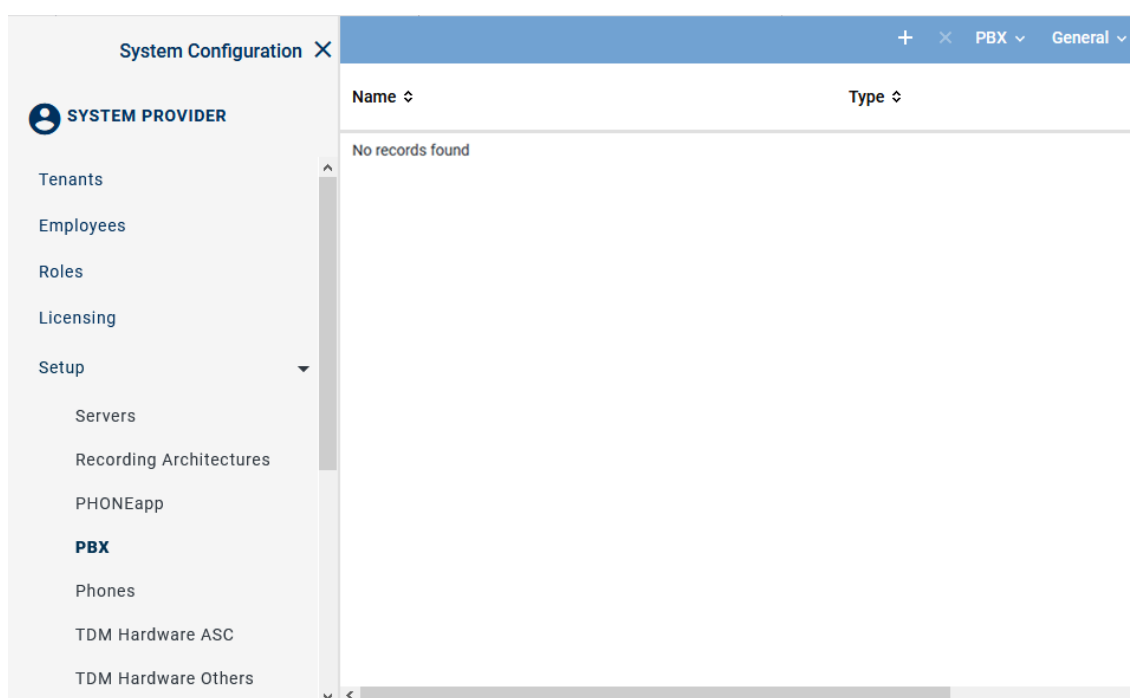


Fig. 373: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.

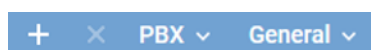




Fig. 374: Toolbar PBX module

	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.




<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	<i>Administrate Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Create new PBX

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

×

< 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. 375: 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 <span style="color: blue;">PBX</span> from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <li><i>Select from list</i> Select the country code from the drop-down list.</li> <li><i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka 094.</li> </ul>
<i>Area code</i>	Enter the area code without the preceding 0, e. g. 6021.
<i>Net code</i>	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 84: Create PBX

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

#### 7.3.2.5.4 Assign recording resources

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

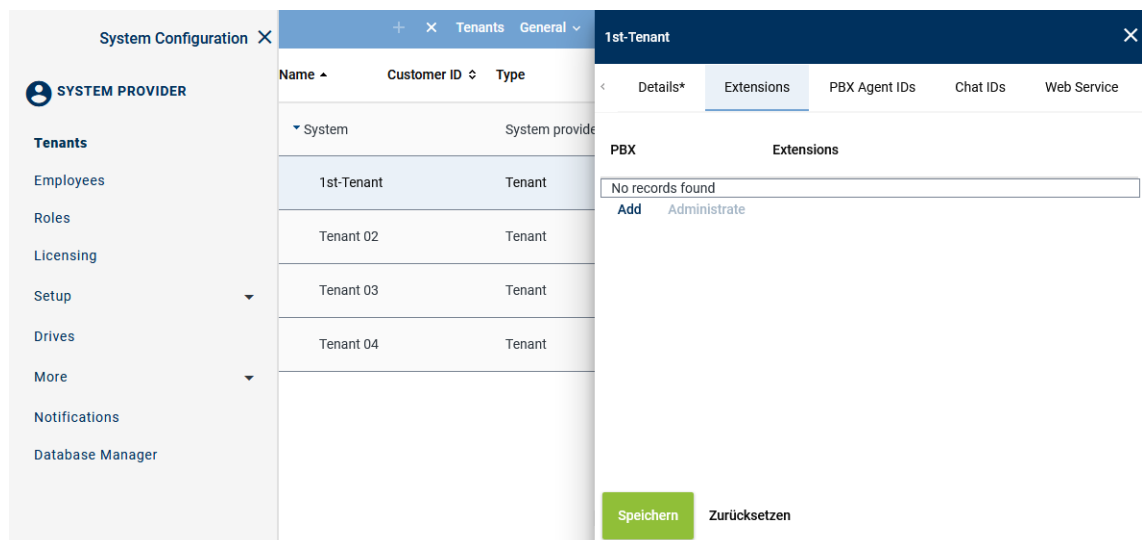


Fig. 376: Tenants - main view - tab Extensions

##### 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. 377: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>• <i>ZIP</i></li> <li>• <i>TXT</i></li> <li>• <i>CSV</i></li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <span style="border: 1px solid #ccc; padding: 2px 5px;">...</span> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <span style="background-color: #4f81bd; color: white; padding: 2px 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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

Enter country codes as number ranges as follows:  
+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions* Activate the check box to replace the list of extensions.

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

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

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

### Remove extensions

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

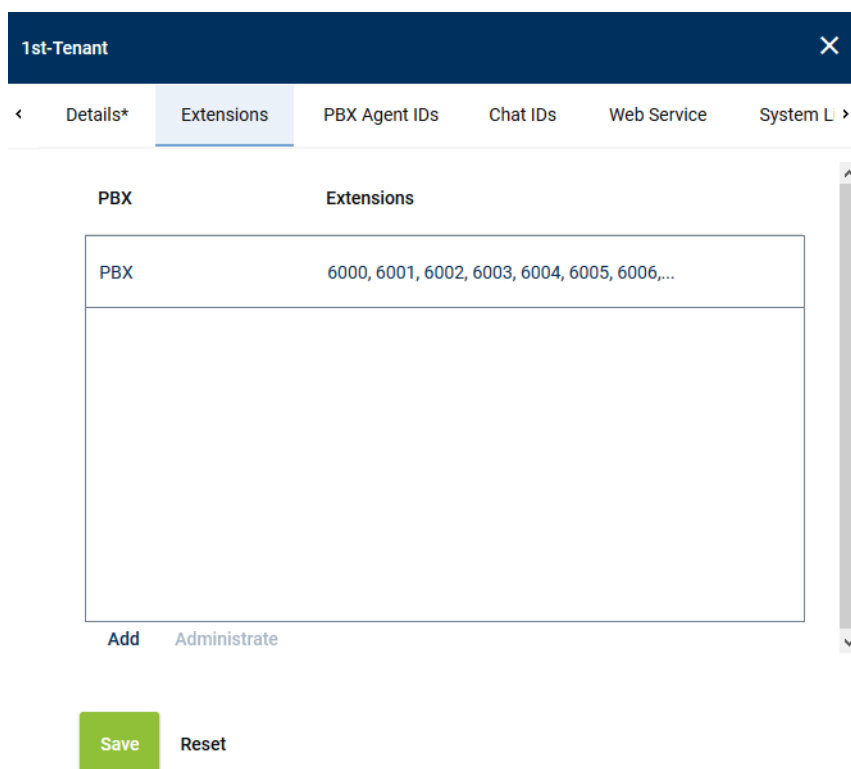


Fig. 378: Remove extensions

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. 379: 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.

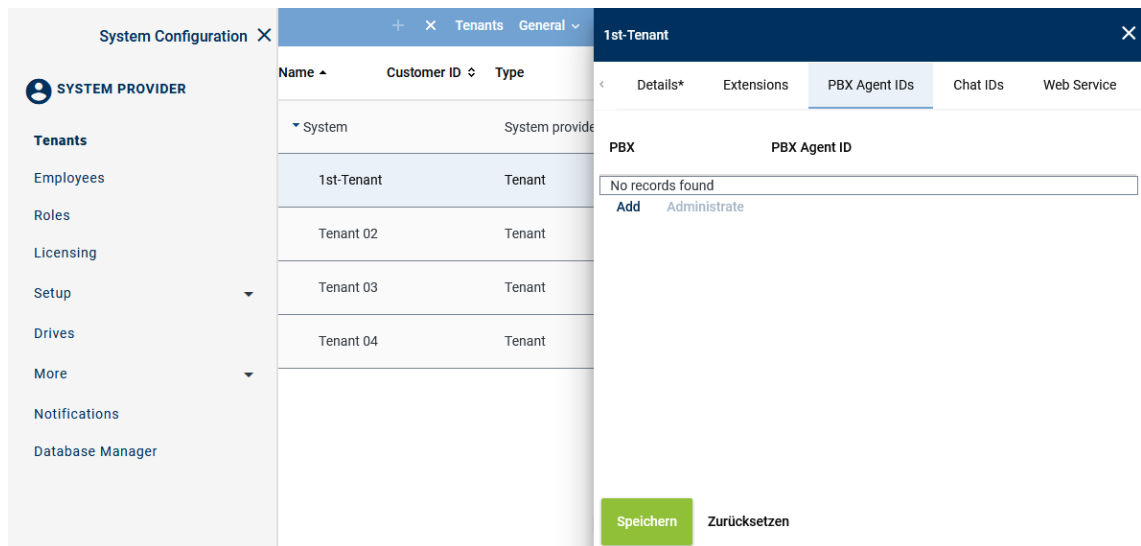
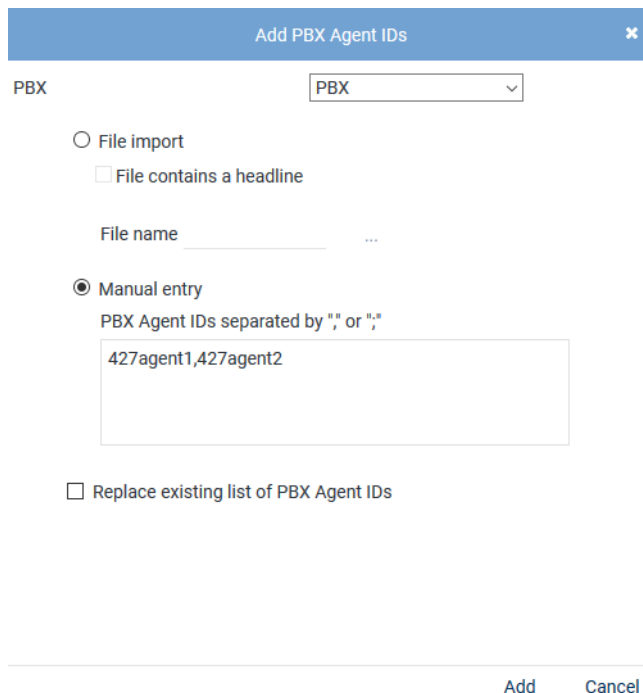


Fig. 380: Tenants - main view - tab PBX Agent ID

### 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:



The 'Add PBX Agent IDs' dialog box is shown. It has a title bar with the text 'Add PBX Agent IDs' and a close button. The main content area includes a dropdown menu for 'PBX' with 'PBX' selected. Below this, there are two radio buttons: 'File import' and 'Manual entry'. The 'Manual entry' option is selected. Under 'Manual entry', there is a text input field containing '427agent1,427agent2'. A checkbox labeled 'File contains a headline' is also present. At the bottom, there is a checkbox labeled 'Replace existing list of PBX Agent IDs'. The dialog box has 'Add' and 'Cancel' buttons at the bottom right.

Fig. 381: 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 the option to import PBX Agent IDs from an existing <a href="#">CSV</a> 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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>Upload File</b>.</li> </ul>
<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><b>NOTICE! Wildcards cannot be used!</b></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. 382: 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*.

### 7.3.2.5.5 Configure additional data

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

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

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

**System Configuration** ✕

**SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 383: 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. 384: 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. 385: 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.

### 7.3.2.5.6 Create integration for Multi-Server Failover

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

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

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

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

⇒ The following window appears:

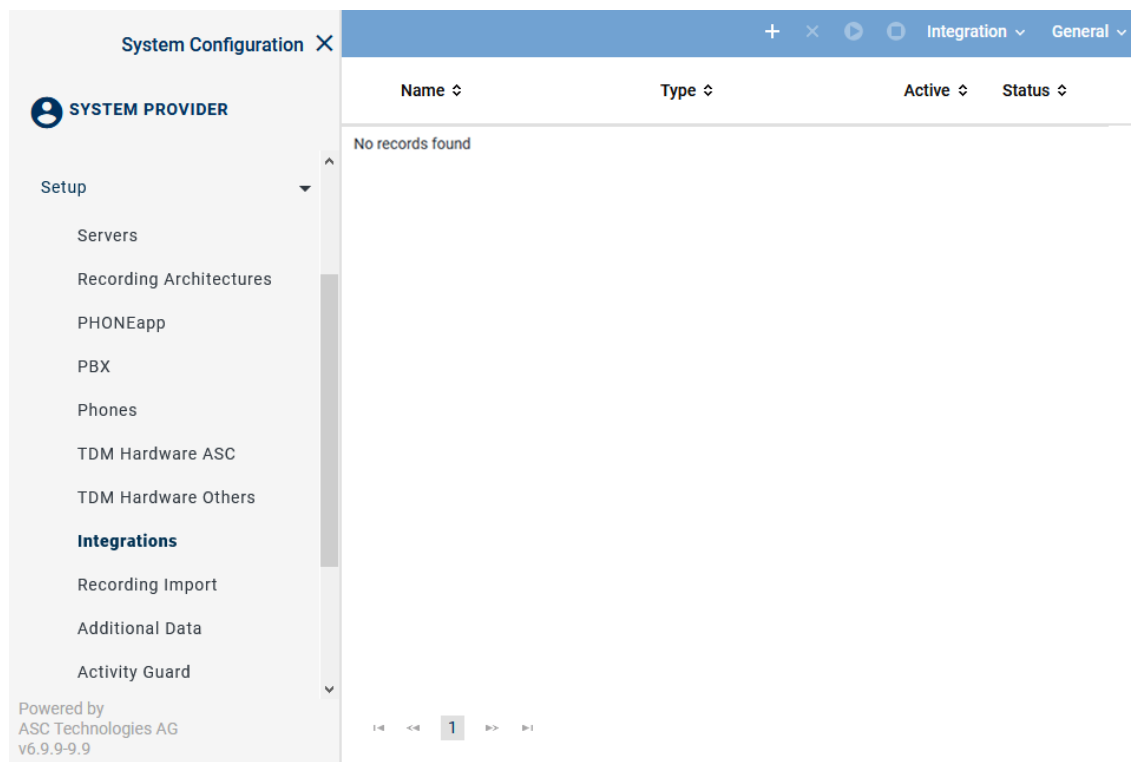




Fig. 386: Integrations - main view

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



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



### Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 387: Toolbar Integrations module

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

	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

- 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.

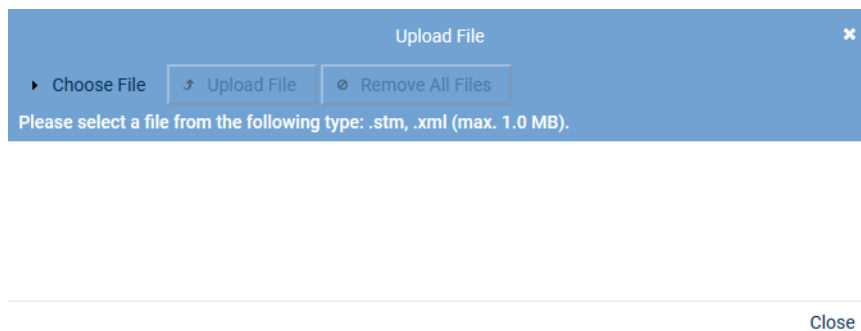


Fig. 388: Choose file

- 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*.

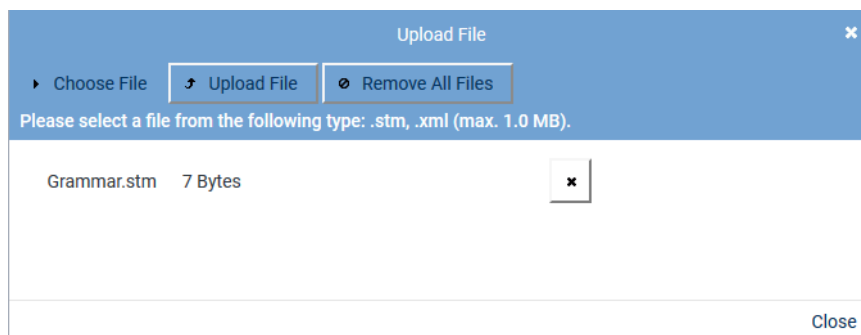



Fig. 389: Upload grammar

- 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. 390: Create integration type

- Enter the following parameters:

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

Tab. 85: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

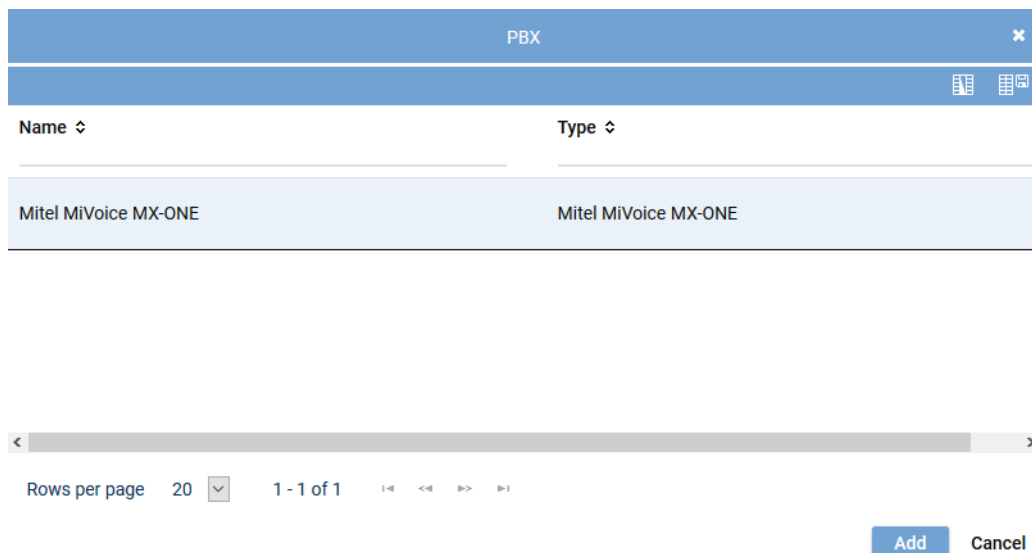


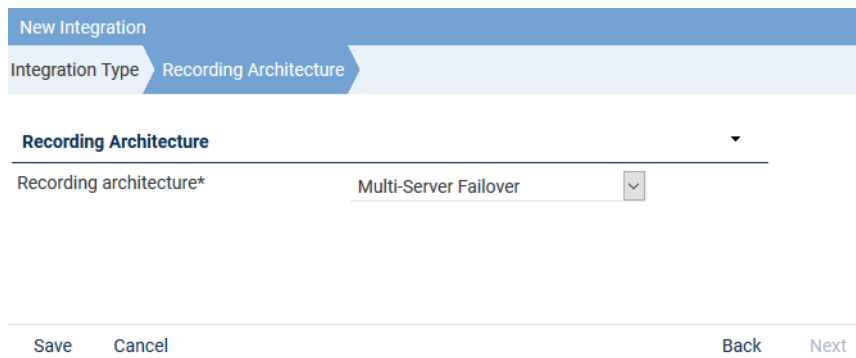
Fig. 391: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

### Assign recording architecture for Multi-Server Failover

- 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. 392: 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. 393: 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.

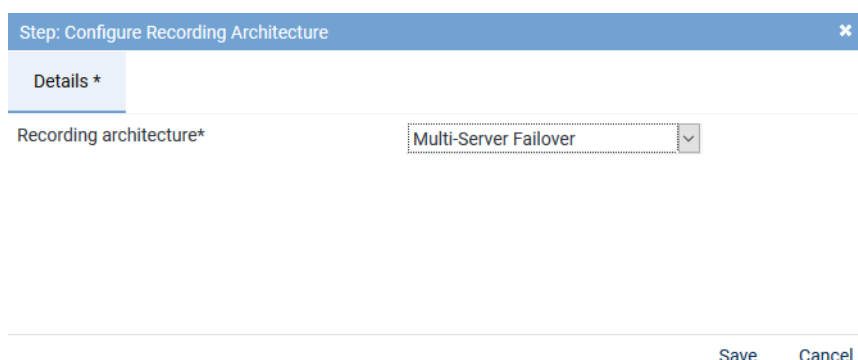



Fig. 394: Configuration step - Configure Recording Architecture

- 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab *MiVoice MX-ONE (CSTA)*

By configuring the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

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

- Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\*
MBG\*

CTIconnect Module

Connection Data

Additional Data

Failover waiting time*	10
Failover repetitions*	3
Regular expression for phone type identification*	<code>^[A-Za-z]*\s[0-9]{4}[a-zA-Z]?\$ ^[0-9]{4}[a-zA-Z]?\$ ^DBC[0-9]{5}\$</code>

Save
Cancel

Fig. 395: CTI connection data - tab MiVoice MX-ONE (CSTA)



Following an update, you must configure this section 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. 396: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 86: 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 MiVoice MX-ONE (CSTA)

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



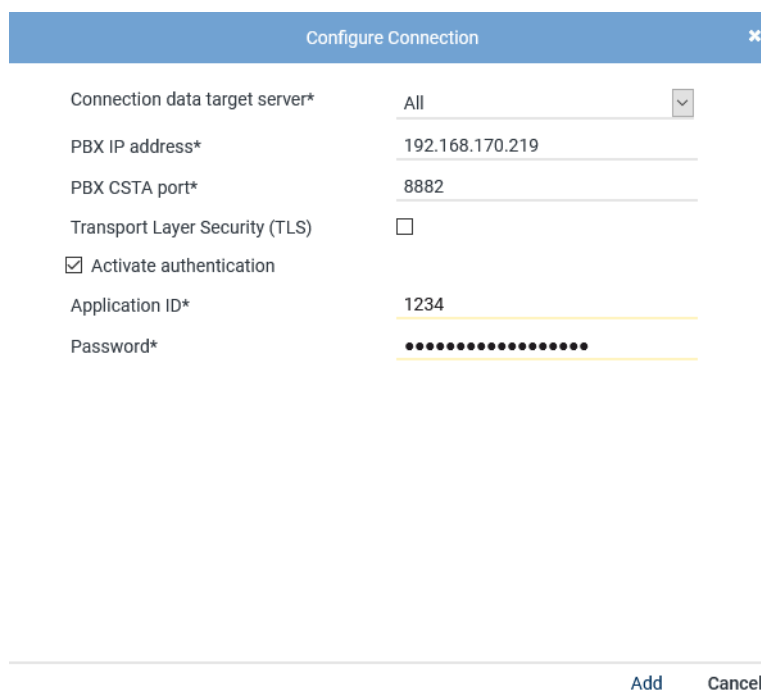
In case, the connection to the CTI<sup>connect</sup> module fails, the recording with the recording variant via the MBG continues with restricted additional data. Phone numbers and direction continue to be available.



Connection Data
<div>PBX IP address</div> <div>No records found</div> <div> <a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> </div>

Fig. 397: 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 target server\*

All

PBX IP address\*

192.168.170.219

PBX CSTA port\*

8882

Transport Layer Security (TLS)

☐

☒ Activate authentication

Application ID\*

1234

Password\*

.....

Add

Cancel

Fig. 398: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<i>PBX IP address</i>	Enter the IP address of the PBX.
<i>PBX CSTA port</i>	Enter the port via which the <a href="#">CSTA</a> connection is supposed to run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .
<i>Transport Layer Security</i>	Activate this check box to use the connection with <a href="#">TLS</a> .
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14</a> .
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14</a> .

Parameter	Value/Description
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 87: Configure connection data

- 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.

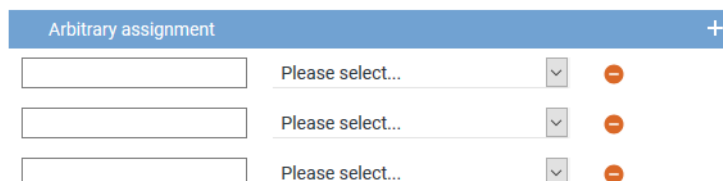



Fig. 399: Arbitrary assignment of the additional data

The following additional data is always available:

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

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

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



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



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

### Configure 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 CTIconnect 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. 400: Configure switching conditions

<b>Failover waiting time</b>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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.
<b>Failover repetitions</b>	Enter how many times the CTI <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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]?$|^\\s[0-9]{4}[a-zA-Z]?$|^DBC[0-9]{5}$
```

Fig. 401: 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.



As parallel recording is only possible via the **MBG**, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

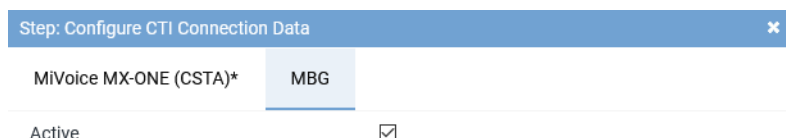


Fig. 402: Activate CTIconnect connection data for [MBG](#)

**Active** Activate the check box to display the configuration parameters and to activate the connection to the [MBG](#).

☒ = Connection has been activated.

☐ = Connection has not been activated.



Following an update, you must configure this section again.

### Group field CTIconnect Module

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

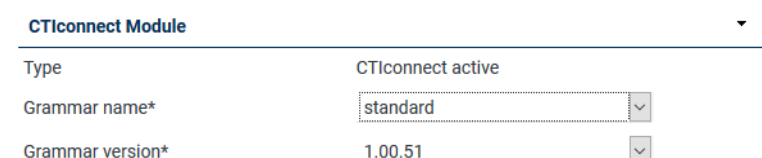


Fig. 403: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 88: 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 MBG

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

**Connection Data** ▼

---

Connection data

No records found

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

Fig. 404: Group field Connection Data

- In the group field *Connection Data* in the table, click on the button *Add*.

⇒ The following window appears:

Configure Connection
✕

Connection data*	192.168.170.116
PBX port*	6810
Activate indirect recording	<input type="checkbox"/>
<input checked="" type="checkbox"/> Use pre-shared key	
Pre-shared key (PSK)*	●●●●●●●●

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

Fig. 405: Configure connection

- Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the <a href="#">MBG</a> .
<i>PBX port</i>	Enter the port for the <a href="#">MBG</a> or the <a href="#">SRC</a> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <a href="#">MBG</a> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 89: 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.

### Group field Additional Data MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

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.

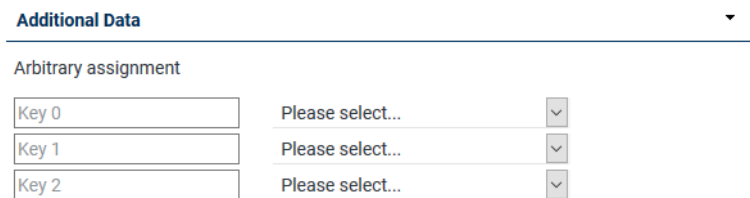



Fig. 406: CTI connection data - additional data module 1

2. Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
3. From the drop-down list, select the entry which is supposed to appear as column headline in the players.
4. Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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.

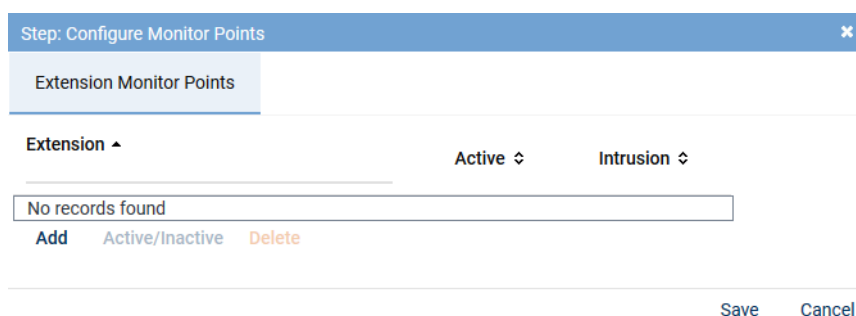


Fig. 407: Configuration step - configure monitor points

### Tab 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.

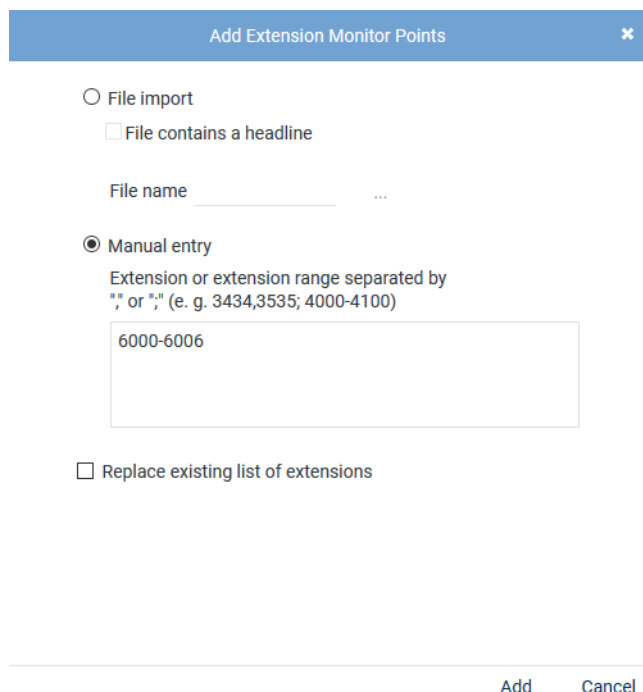


Fig. 408: Add extension monitor points

<b>File import</b>	<p>Select this option to import extensions from an existing <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>↗</b> (<i>Upload file</i>).</li> </ul>
<b>File contains a headline</b>	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
<b>File name</b>	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>↗</b> (<i>Upload file</i>).</li> </ul>
<b>Manual entry</b>	<p>Select this option to enter extensions or extension ranges manually.</p>



Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumeric entries with a hyphen are not detected as a range, they must be entered individually. You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.

**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 <span>✕</span>		
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 href="#">Add</a> <a href="#">Active/Inactive</a> <a href="#">Delete</a>		
<a href="#">Save</a> <a href="#">Cancel</a>		

Fig. 409: Configured extension monitor points

<b>Add</b>	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.
<b>Active/Inactive</b>	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.
<i>Delete</i>	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.
<i>Intrusion</i>	<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. 16](#).

### Global recording settings

- Click on the button  (*Edit configuration step*) in the line *Global recording settings* in the main view.
 

⇒ The window *Step: Global Recording Settings* appears.

Step: Global Recording Settings

Details\*

Transport protocol

UDP

Port SIP signaling\*

5060

Remote SIP port\*

7300

Activate SIP authentication

☒

User name for the SIP registration

#extension

Password for the SIP registration

.....

Activate PBX connection

☒

SIP registration expiration\*

3600

PBX IP address\*

192.168.170.219

PBX port\*

5060

Save

Cancel

Fig. 410: Configuration step - Global Recording Settings

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

Parameter	Value/Description
<i>Transport protocol</i>	<p>Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i>, the transport protocol applies for the SIP communication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
<i>Port SIP signaling</i>	Enter the port for SIP signaling that is opened on the recording server for incoming SIP communication and that has been selected in the outgoing SIP notifications as the port of the recording server. Default 5060.
<i>Remote SIP port</i>	Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by SIP to start <i>active-stream recording</i> . Default 7300.
<i>Activate SIP authentication</i>	Activate the check box if 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 SIP registration of extensions recorded with 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 SIP registration of extensions recorded with 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. 90: Global recording settings

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



Following an update, you must configure this section 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	REC-01
Server Name	<div>Details*</div> <div>Extensions</div>
REC-01	<div>Recording Module Active MX-ONE <input checked="" type="checkbox"/></div> <div>Configured IP address 192.168.173.171</div> <div>IP address of the recording server* 192.168.173.171</div> <div>Minimum port* 20000</div> <div>Maximum port* 21000</div>
REC-02	

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 411: 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 <b>RTP</b> data from the recording server, e. g. <b>20000</b> .
<i>Maximum port</i>	Enter the highest port configured on the PBX that is used to receive the <b>RTP</b> data from the recording server, e. g. <b>21000</b> .

Tab. 91: 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.



Following an update, you must configure this section 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*.

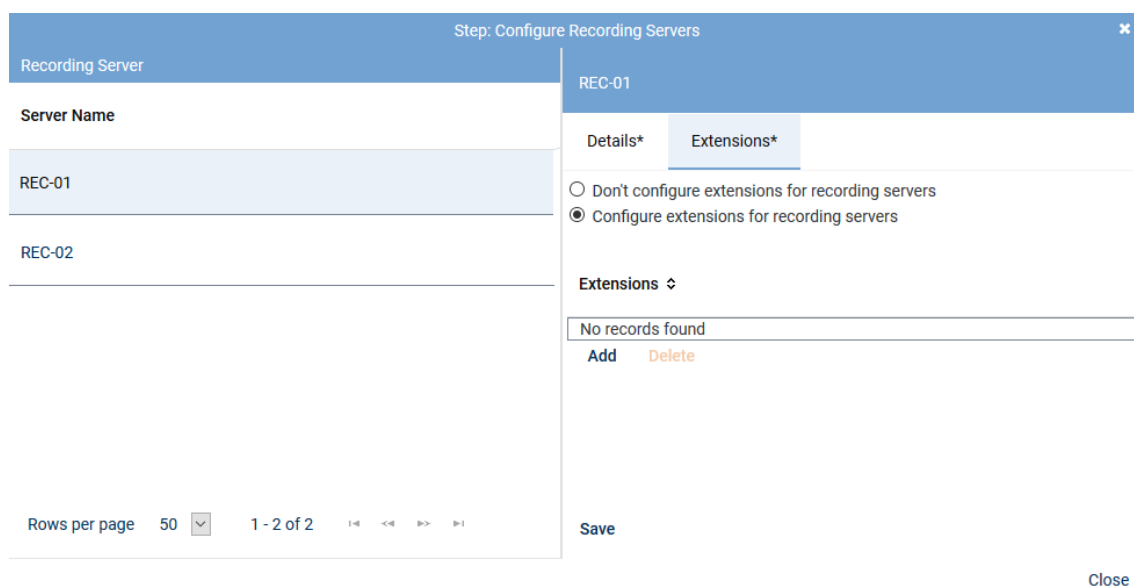


Fig. 412: Tab Extensions

**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.

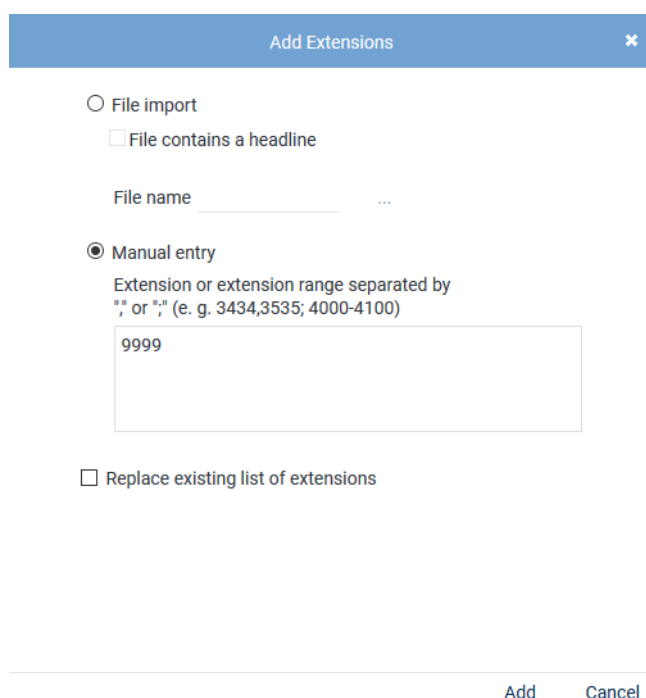


Fig. 413: Add extensions

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.

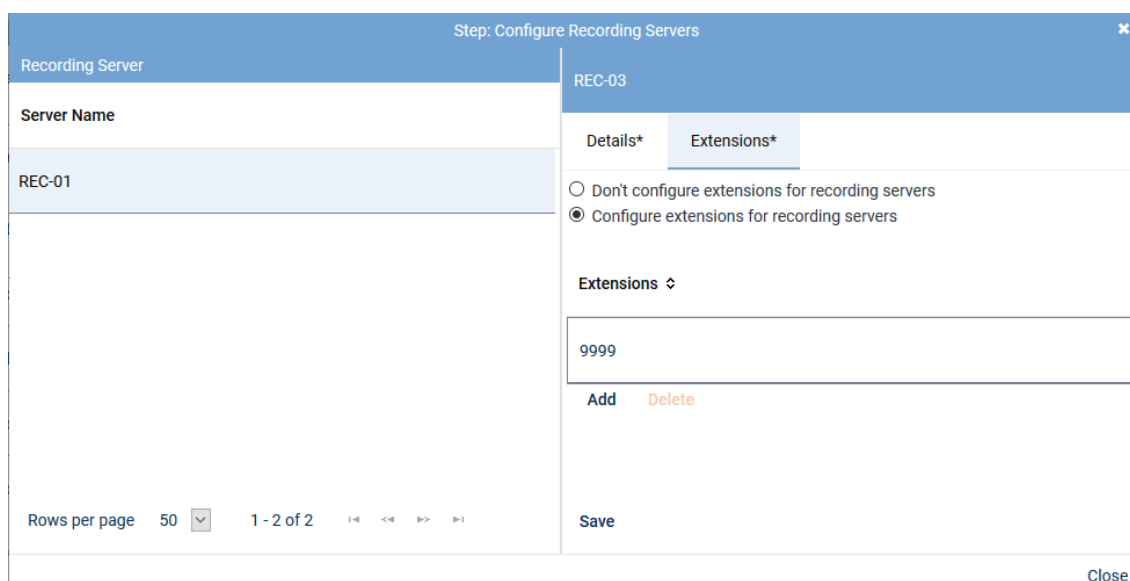


Fig. 414: Added extensions

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.



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

### 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	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
PRIVATEDATA	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
SERVICEGROUPID	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
SERVICEGROUPLIST	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA1	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL1	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA2	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL2	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRDATA3	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
IVRLABEL3	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>
OASID	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>

Arbitrary assignment
+

	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>	
	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>	
	Please select...	<span style="border: 1px solid #ccc; padding: 2px 5px;">▼</span>	<span style="color: red;">-</span>	

Save Cancel

Fig. 415: 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	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 92: Configure CTIconnect module

### Group field Connection Data

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. 93: 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.

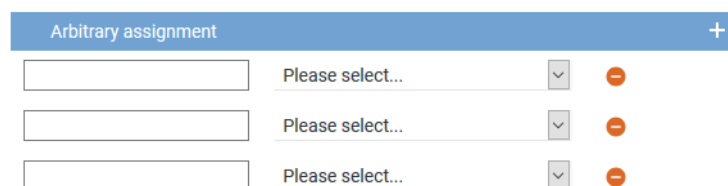



Fig. 416: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
- *End time*



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

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



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



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

### **Configure add-on for 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<sup>connect</sup> 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

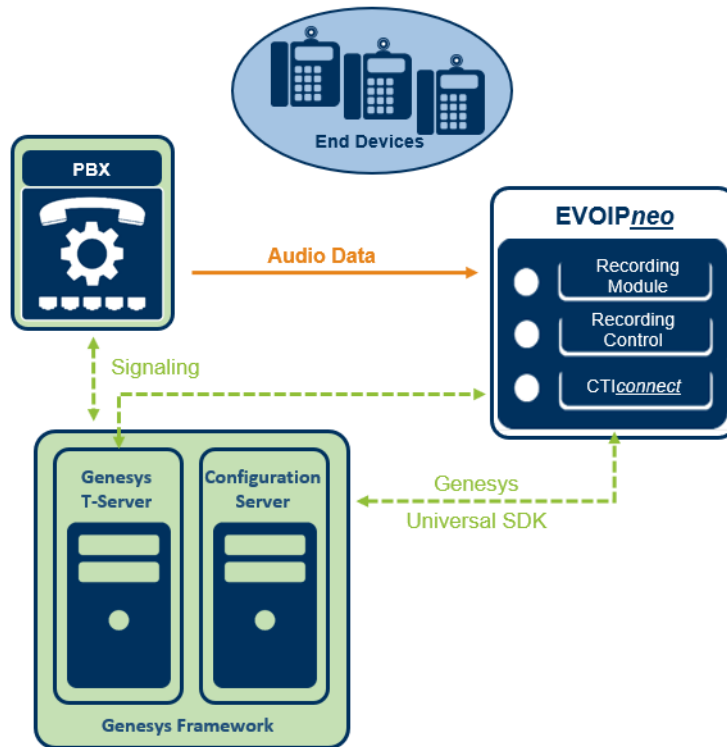


Fig. 417: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

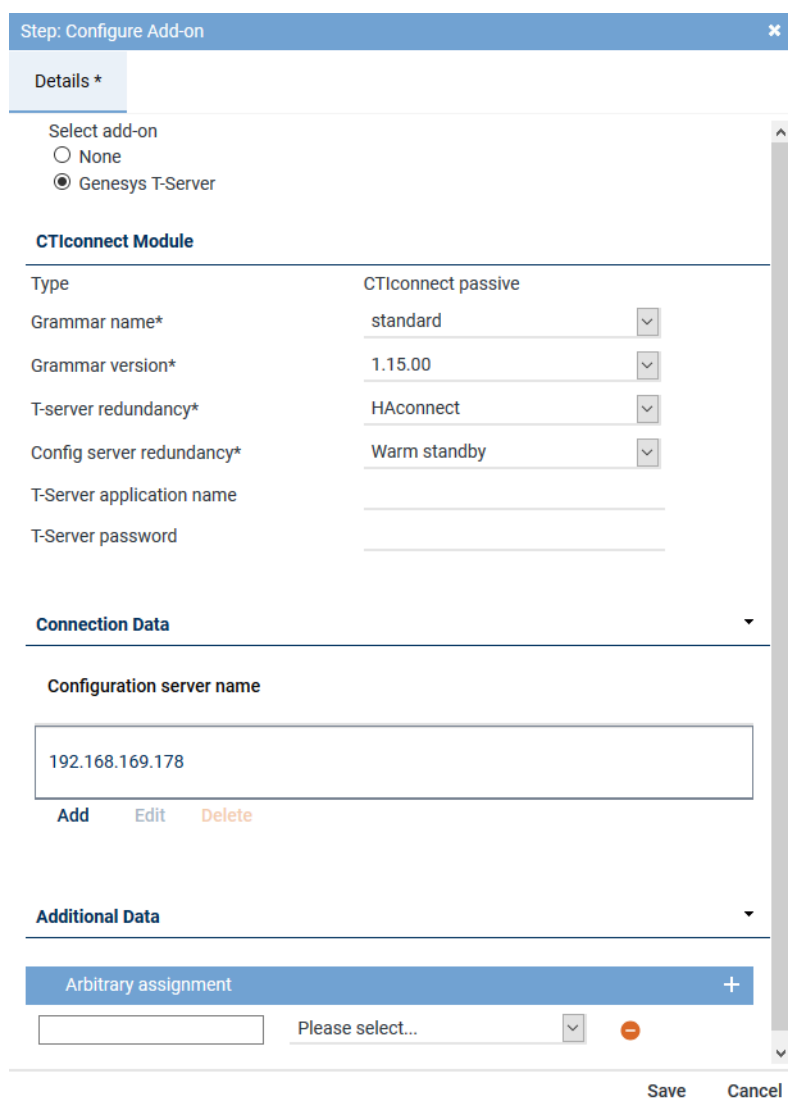
### Adjust configuration file for Genesys add-on

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. 418: 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<i>T-Server application name</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the application name that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>
<i>T-Server password</i>	<p>This parameter must only be entered, if authentication on the Genesys T-Server is required.</p> <p>Enter the password that the CTI<u>connect</u> module is supposed to use to log in to the Genesys T-Server.</p> <p>If you use several Genesys T-Servers, the login data must be identical for all servers.</p>

Tab. 94: Configure add-on for Genesys T-Server

### Group field Connection Data

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

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

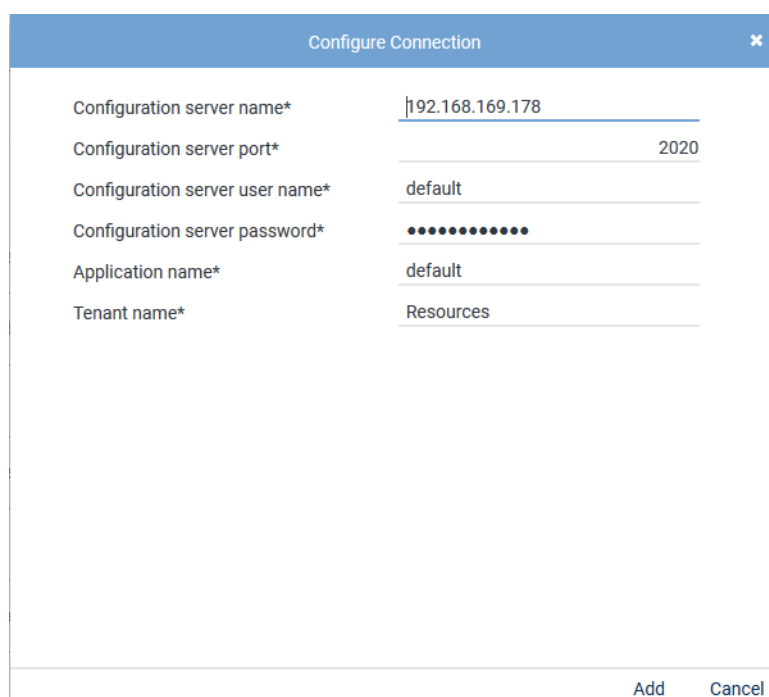


Fig. 419: Configure connection data

2. Enter the following parameters:

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

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

Tab. 95: Configure connection data

### Group field Additional Data

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

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



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

### Arbitrary assignment

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



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

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



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


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

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

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

Fig. 420: Arbitrary assignment of the additional data

The following additional data is always available:

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

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




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



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

### Configure miscellaneous settings

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

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select... ▼

Save

Cancel

Fig. 421: 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. 422: 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. 423: 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. 424: Deactivate integration

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

## 7.3.2.6 Configure recording solution Multi-Server Parallel Recording

### 7.3.2.6.1 Create recording architecture

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

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

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



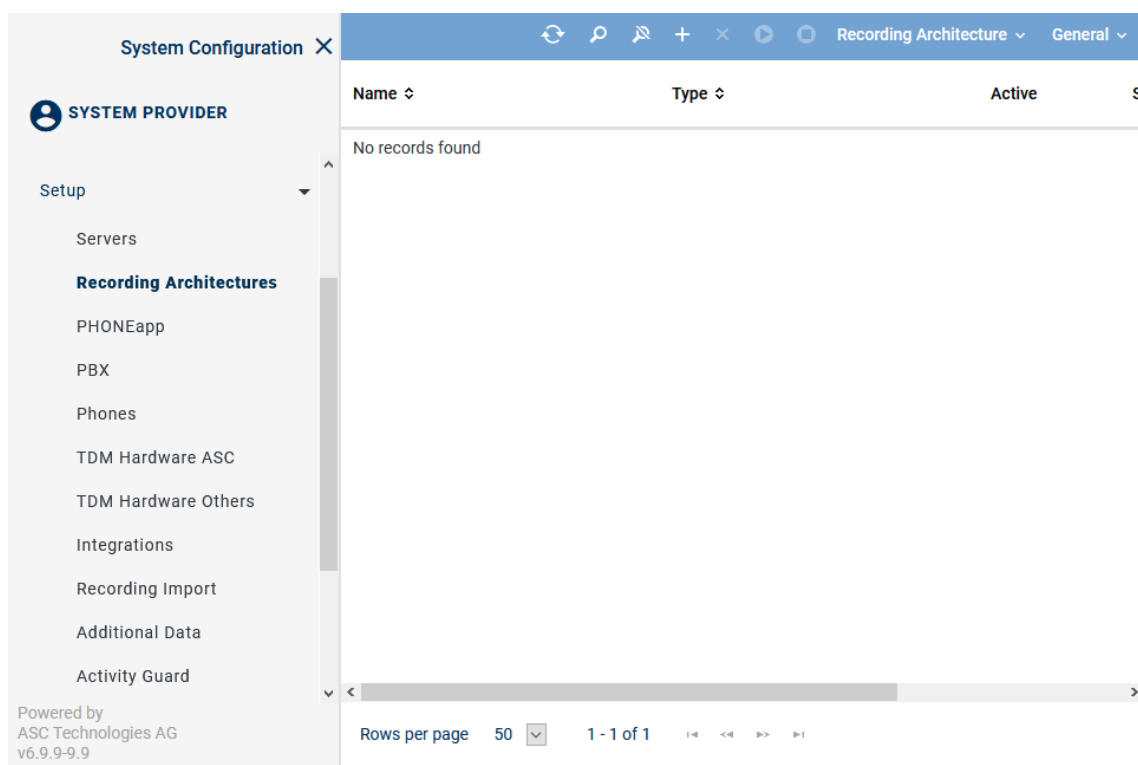




Fig. 425: Recording architectures - main view

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



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








### Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 426: Toolbar Recording Architectures module

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


		The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Create</i>	Creates a new recording architecture.
	<i>Delete</i>	Deletes the selected recording architecture. The recording architecture is removed from the list of the main view. <b>NOTICE!</b> You can only delete recording architectures which are inactive and have not been assigned to an integration or server for the import.
	<i>Activate</i>	Activates the selected recording architecture.
	<i>Deactivate</i>	Deactivates the selected recording architecture. <b>NOTICE!</b> You can only deactivate recording architectures which have neither been assigned to an active integration nor to an active import.
<i>Recording Architecture</i>	<i>Standby Management</i>	The menu item is only available for recording architectures with failover possibilities. By clicking on the menu item Standby Management, you can open a window in which you can manually define the active server in architectures with failover concepts.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.




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

### Create recording architecture Multi-Server Parallel Recording

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


- 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 Parallel Recording

Type

Multi-Server Parallel Recording 

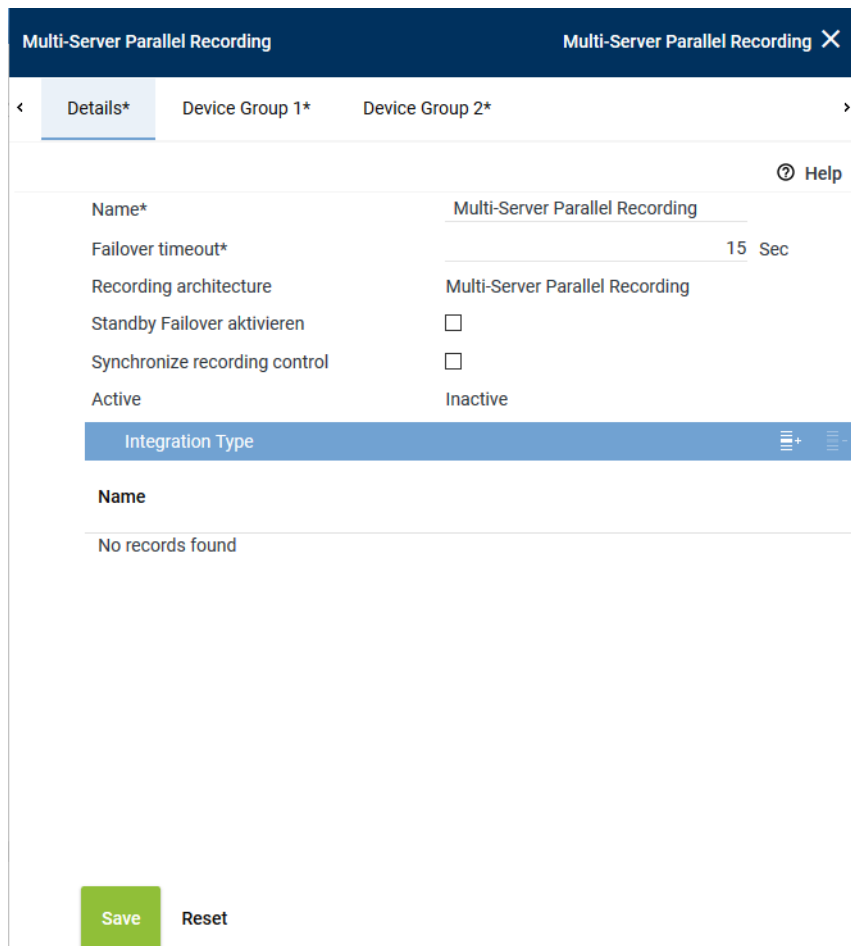
OK

Cancel

Fig. 427: Create recording architecture - Multi-Server Parallel Recording

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

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



Multi-Server Parallel Recording

Multi-Server Parallel Recording X

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

ⓘ Help

Name\* Multi-Server Parallel Recording

Failover timeout\* 15 Sec

Recording architecture Multi-Server Parallel Recording

Standby Failover aktivieren ☐

Synchronize recording control ☐

Active Inactive

Integration Type

Name

No records found

Save Reset

Fig. 428: Recording architecture - tab Details - Multi-Server Parallel Recording

Since additional standby components may have been configured for the different active recording servers, a failover timeout may be configured in this recording architecture. For more information about the configuration of failover architectures, see [chapter "Standby management for failover architectures", p. 450](#).




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

5. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers, see [chapter "Synchronization of recording control", p. 442](#).

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

If you do not want to synchronize recording control, you can configure duplicate detection, see [chapter "Duplicates in parallel recording architectures"](#), p. 445.

### Add integration type

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

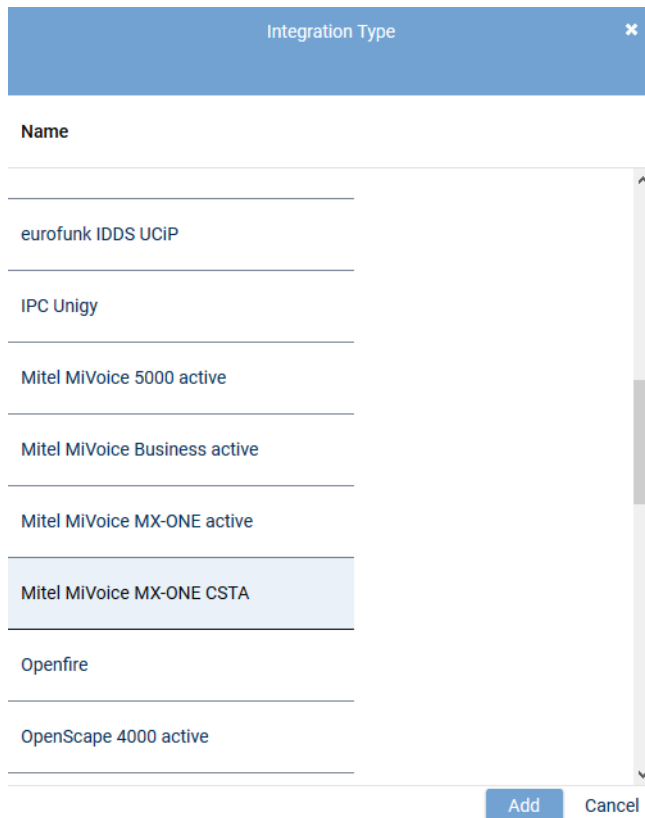


Fig. 429: Select integration type



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 server for Multi-Server Parallel Recording

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

#### Tab Device Group 1

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

#### Group field Recording Control and CTIconnect

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

Multi-Server Parallel Recording
Multi-Server Parallel Recording
×

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

Recording Control and CTIconnect

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

Recording Server

< Recording Server
⌵ ⌵ ⌵

Server ⌵	Standby ⌵	
REC-01	REC-02	⌵

Save

Reset

Fig. 430: Recording architecture - server assignment device group 1

- Click on the button **+** next to the entry field *Recording Control* to assign a server.  
⇒ The window *Servers* appears.

Servers

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

Rows per page


20

1 - 8 of 8

Add

Cancel

Fig. 431: Recording architecture - assign server - example


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



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

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

### Group field Recording Server

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

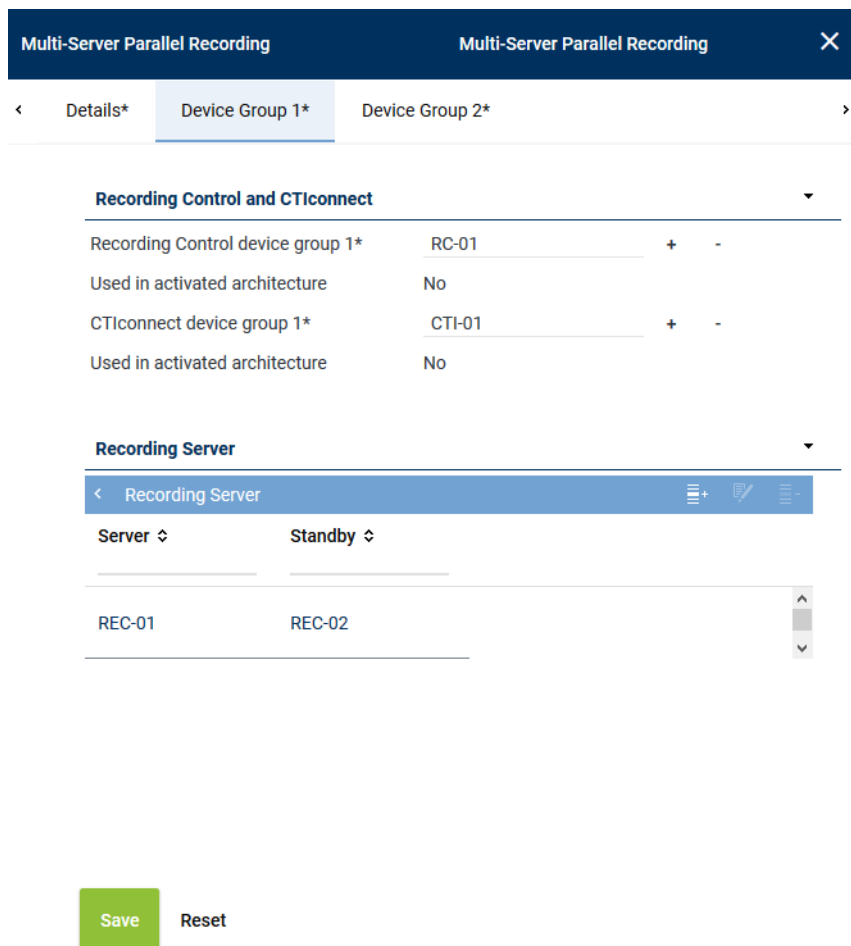






Fig. 432: Add recording server

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

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




### Tab Device Group 2

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



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

### Activate recording architecture

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










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

Fig. 433: Recording architecture - activate recording architecture - example

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



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



Parallel recording results in redundant recording data in the system. To make sure that this data does not remain in the system permanently, you can configure duplicate detection so that duplicate sets of data are deleted, see [chapter "Configure duplicate detection", p. 446](#).

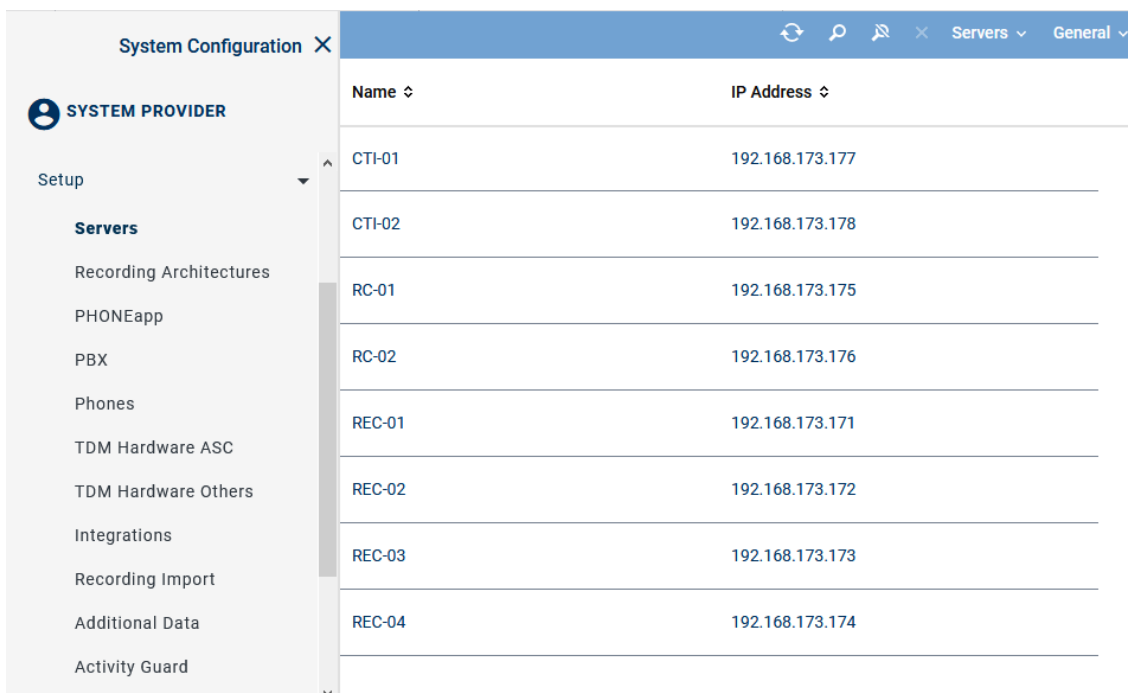


If you install an add-on for the integration subsequently, you must deactivate the recording architecture and activate it again after having installed the license.

### 7.3.2.6.2 Configure server

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

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



Name	IP Address
CTI-01	192.168.173.177
CTI-02	192.168.173.178
RC-01	192.168.173.175
RC-02	192.168.173.176
REC-01	192.168.173.171
REC-02	192.168.173.172
REC-03	192.168.173.173
REC-04	192.168.173.174

Fig. 434: Servers - main view

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

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

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

### Toolbar of the Servers module

The toolbar offers the following functions.

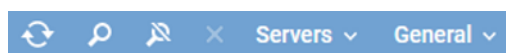







Fig. 435: Toolbar Servers module

	<i>Refresh</i>	Refreshes the main view.
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria.  The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that all sets of data are displayed in the main view again.
	<i>Delete</i>	Deletes the selected server configuration.  This function is meant to delete the server configuration if the hardware of a server has been removed and there is no connection to the <a href="#">neo</a> system.



<i>Servers</i>	<i>Administrate Server Locations</i>	Opens a window in which you can create and administrate locations of the servers, see <a href="#">chapter "Administrate server locations", p. 365</a> .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for the time synchronization, see <a href="#">Administrate NTP server</a> .
	<i>Manage Synchronization Configurations</i>	Opens a window in which you can manage the synchronization configurations.
<i>General</i>	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• <i>Displayed information</i></li> <li>• <i>Order of the displayed columns</i></li> <li>• <i>Number of rows per page</i></li> </ul>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



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

### Administrate server locations

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

#### Add server locations

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

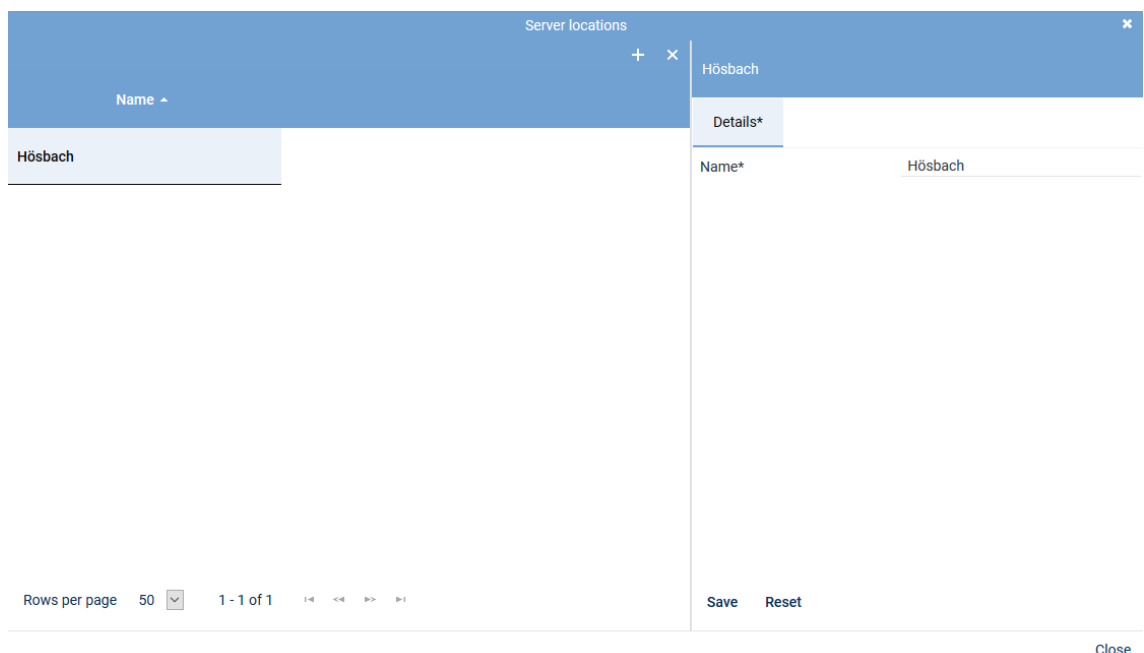



Fig. 436: Add server locations

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

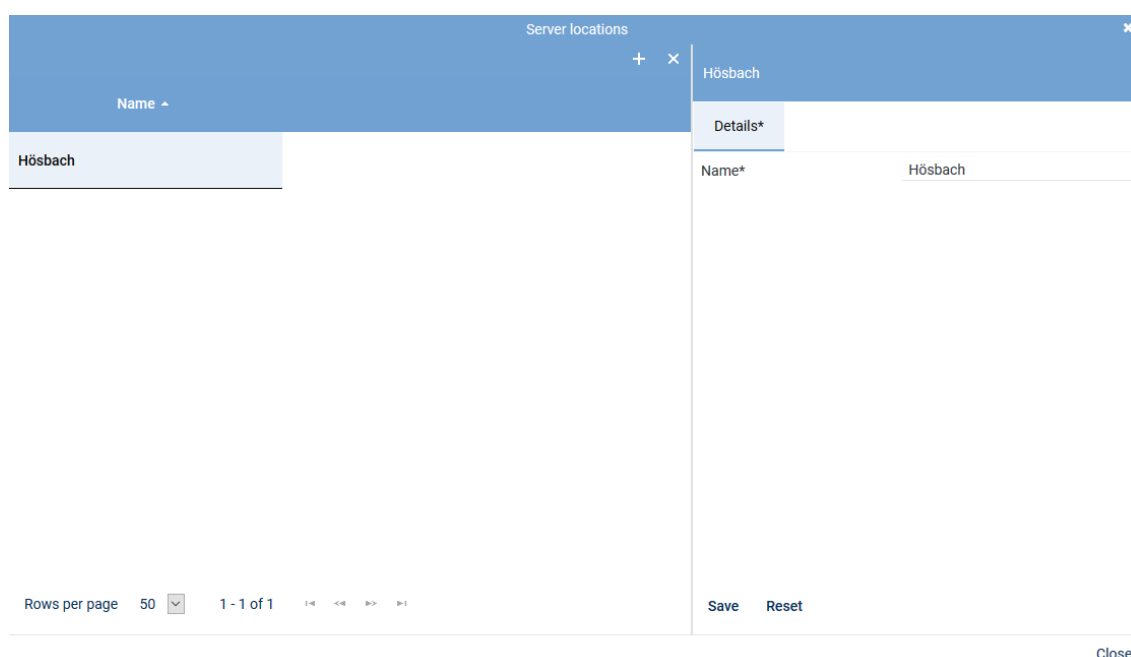
4. To save the entry, click on the button *Save*.  
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

### Delete server location




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

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



The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Inside the window, there is a table with a header "Name" and a single row containing "Hösbach". To the right of the table is a "Details\*" panel. The "Details\*" panel has a label "Name\*" and a text field containing "Hösbach". At the bottom of the window, there are buttons for "Save" and "Reset", and a "Close" button at the very bottom right. The bottom of the window also displays "Rows per page 50" and "1 - 1 of 1".

Fig. 437: 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. 438: Servers - tab Details

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

### Tab Usage

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



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

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

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

Fig. 439: Servers - tab usage

### Group field API Server

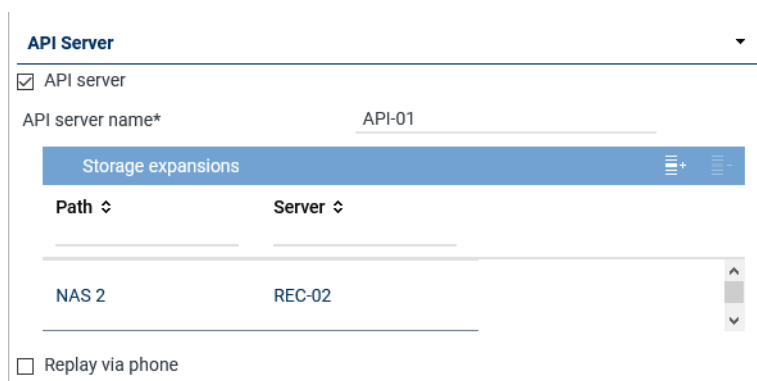




Fig. 440: Group field API Server

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


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

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


Parameter	Value/Description
<i>API server</i>	<p>Activate the check box to start the ASC API Server.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>API server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>To be able to reach the ASC API Server from a public network and with configured port forwarding, too, you have to adjust the settings in the tab <i>Replay Server Address Mapping</i>, see <a href="#">chapter "Tab Replay Server Address Mapping", p. 378</a>.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add storage expansions, see <a href="#">chapter "Add storage expansion for replay", p. 369</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.</li> </ul>

Parameter	Value/Description
	If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.  <input type="checkbox"/> = Function has not been activated.</p> <p><b>NOTICE!</b> The function <i>Replay via phone</i> has been implemented in the following <i>neo</i> components:</p> <ul style="list-style-type: none"> <li>• Application POWERplay Pro</li> <li>• Application POWERplay Instant</li> <li>• Replay module</li> </ul> <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p><b>NOTICE!</b> In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see <a href="#">chapter "Tab Media Streamer", p. 376</a>. To be able to do so, at least 1 PBX must have been configured in the system.</p>

### Add storage expansion for replay

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

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

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

Add Cancel

Fig. 441: Select storage expansion

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

### Group field Audio analysis

**Audio Analysis**

☒ Emotion detection

Stream audio data from\* REC-01 + -

Fig. 442: Group field Audio Analysis

Parameter	Value/Description
<i>Emotion detection</i>	<p>Activate this check box to activate emotion detection for audio analysis.</p> <p><input checked="" type="checkbox"/> = Function has been activated. Tenants can use the emotion detection function.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Stream audio data from</i>	<p>If the function emotion detection has been activated, the parameter to select the respective server becomes active.</p> <ul style="list-style-type: none"> <li>Click on the button <b>+</b> to select the server from which the audio data is supposed to be streamed for emotion detection from the list of available servers.</li> </ul>

Tab. 96: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

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

Add Cancel

Fig. 443: Select server for emotion detection

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

### Group field Recording Control/Key Management

**Recording Control/Key Management** ▼

☒ Recording control/Monitoring

Recording architecture Please choose... ▼

☒ neo key management

Fig. 444: Group field Recording Control/Key Management

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

Tab. 97: Configure recording control/key management

### Group field Data Processing

**Data Processing**

☒ Data storage

☐ Transfer data for replay

Target Server

Name

IP Address ↕

No records found

☒ Transfer data for data storage

Target Server

Name

IP Address ↕

No records found

Activate period of time

☒

Start

0:00

▼

End

4:00

▼

Receives data from

Name

Only Replay

No records found

☐ Archiving

☒ Export

Replay server

Please choose... ▼

☒ Import







Recording architecture

All-in-one Basic ▼

Fig. 445: Group field Data Processing

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - *neo* 6.x Rev. 34

371 / 489


Parameter	Value/Description
<i>Data storage</i>	<p>Activate the check box to make additional functions of data processing available for editing.</p>
<i>Transfer data for replay</i>	<p>Activate the check box if you would like to transfer the data to another server for replay purposes only.</p> <p>If the function has been activated, you can add a server to the list <i>Target Server</i> to which the recorded data is supposed to be transferred for replay purposes. The data is not saved on the target server but only buffered in a cache for replay purposes.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target server, see <a href="#">chapter "Add target server to a list", p. 373</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which an API server and a replay server have been configured.</p>
<i>Transfer data for data storage</i>	<p>Activate the check box if you would like to transfer the data to be saved on another server.</p> <p>If the function has been activated, you can select a server in the list <i>Target Server</i> to which the recorded data is supposed to be transferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> <li>By clicking on the icon  (<i>Add</i>), you can add the target servers, see <a href="#">chapter "Add target server to a list", p. 373</a>.</li> <li>By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list.</li> </ul> <p><b>NOTICE!</b> Only those servers are displayed for which the function <i>data storage</i> has been activated.</p> <p>If the function has been activated, you can activate the transfer for a certain period of time.</p> <ul style="list-style-type: none"> <li><i>Activate period of time</i> <input checked="" type="checkbox"/> = Function activated. The fields to enter a time become active. Select the time for from – to by means of the rotating field.</li> <li><i>Activate period of time</i> <input type="checkbox"/> = Function not activated.</li> </ul> <p><b>NOTICE!</b> Once the function has been configured, the data can be replayed on the target server. If replay is requested, the data is buffered in the working memory of the target server even if the transfer for data storage has not been completed.</p> <p><b>NOTICE!</b></p> <p>For distributed systems with a slower network connection, the storage interval for data transfer may be adjusted. The storage interval for data transfer must be configured by an ASC service technician or by an authorized partner.</p>
<i>Receive data from</i>	<p>This table displays servers which transfer data to this server.</p> <p>The column <i>Name</i> displays the server name from which data is transferred.</p> <p>The column <i>Only Replay</i> displays the purpose of the transfer:</p> <p> = Data is transferred for replay only.</p> <p> = Data is transferred for data storage.</p>



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

Tab. 98: Data storage

### Add target server to a list

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

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

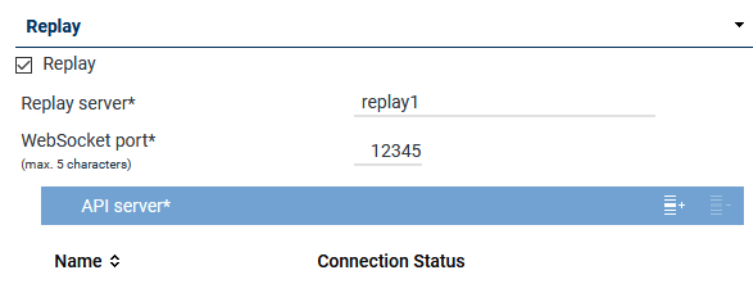
Fig. 446: Select server



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

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

### Group field *Replay*



**Replay** ▾

☒ Replay

Replay server\*



WebSocket port\*   
(max. 5 characters)

API server\* ⋮

Name ⚡ Connection Status

Fig. 447: Group field *Replay*

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the <a href="#">API server</a> must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in <a href="#">POWERplay Web</a> are supposed to be transmitted.
<i>List API server</i>	<p>Here, you can add <a href="#">API servers</a> that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the <a href="#">API servers</a> which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p>

Parameter	Value/Description
	<ul style="list-style-type: none"> <li>By clicking on the icon  (Add), you can add the <a href="#">API server</a>, see <a href="#">chapter "Add API server to a list"</a>, p. 375.</li> <li>By clicking on the icon  (Remove), you can remove selected <a href="#">API servers</a> from the list.</li> </ul>

Tab. 99: Configure replay


### Search and replay functions



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

### Add API server to a list

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

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

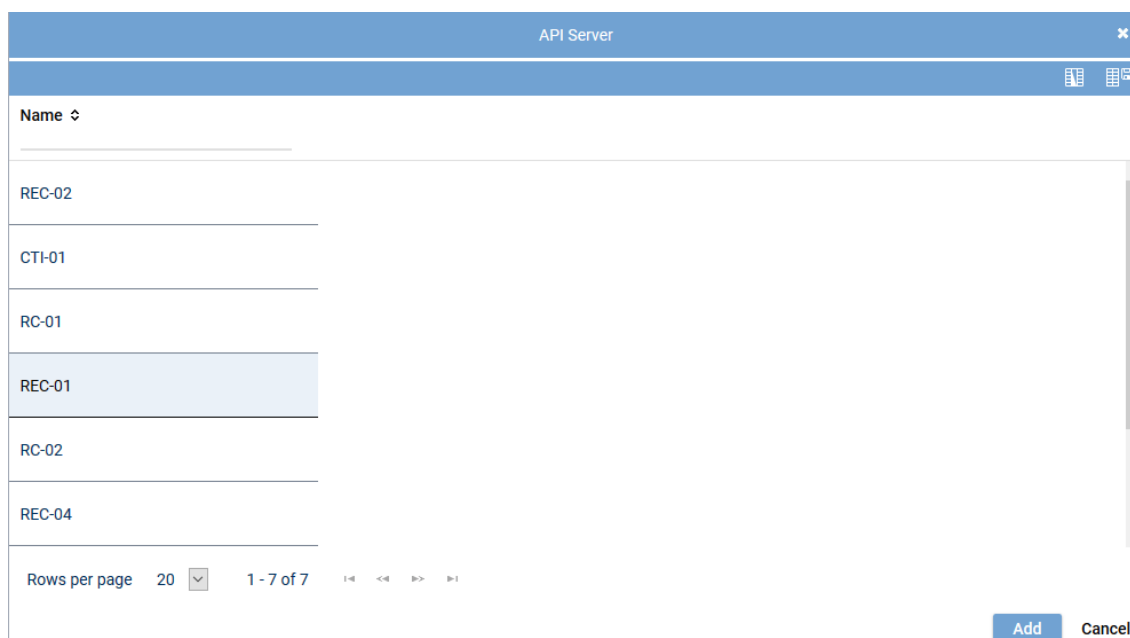


Fig. 448: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server"](#), p. 368.

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

### Group field Virtualization

#### Virtualization

☐ VM without Trusted License

Fig. 449: Group field Virtualization

Parameter	Value/Description
<i>VM without Trusted License</i>	<p>This functionality can only be activated if the system runs in a virtual environment and if no <i>TRUSTED_VIRTUALIZATION</i> license has been installed.</p> <p>When you tick the check box <i>VM without Trusted License</i>, the tab <i>Keystore/Virtualization</i> becomes active and must be completed.</p> <p>There, you can configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>licensing.asc.de</i> If you enter this domain, there is no key management.</li> <li>• <i>IP address of the DongleMan</i> If you enter the IP address of the Dongle Manager, you can activate key management.</li> </ul>

Tab. 100: Configure virtualization



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



For *virtualization* without an Internet connection, a Trusted License is required.

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

### Tab Media Streamer

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

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



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

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

PBX +

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

Save
Reset

Fig. 450: Servers module - tab Media Streamer

2. Enter the following parameters:

<b>PBX</b>	<p><b>PBX</b> that the Media Streamer is supposed to be mapped to.</p> <p>Select a <b>PBX</b> from the drop-down list. The drop-down list displays all <b>PBXs</b> which have been created in the system.</p> <p>If no <b>PBX</b> has been created in the system yet, you can create a <b>PBX</b> via the blue bar <b>PBX</b>, see <a href="#">chapter "Create PBX"</a>, p. 383.</p>
<b>Extension</b>	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value <b>8000</b>.</p>
<b>Media streamer IP address</b>	<p>IP address which is supposed to be used for the exchange of the audio data and for the <b>SIP</b> communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p> <p>If an external analog gateway has been integrated, select the IP address <b>169.254.254.100</b> in the drop-down list.</p>
<b>Minimum port</b>	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
<b>Maximum port</b>	<p>Enter the maximum port which is supposed to be used for the audio data exchange.</p> <p>Enter an uneven number.</p>

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

### Tab Replay Server Address Mapping

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

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



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

<

Details\*

Usage\*

Media Streamer

Replay Server Address Mapping

>

Replay Server Addresses

Remove Replay Server Addresses

Internal IP address/ port of the replay server

192.168.169.171

:

4711

Internal download URL

External address/ port of the replay server

192.168.169.171

:

4711

External download URL

Save

Reset

Fig. 451: Servers Module - tab Replay Server Address Mapping

Group field **Replay Server Addresses**

1. Enter the following parameters

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

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



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



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



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

### Tab Key Management

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

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

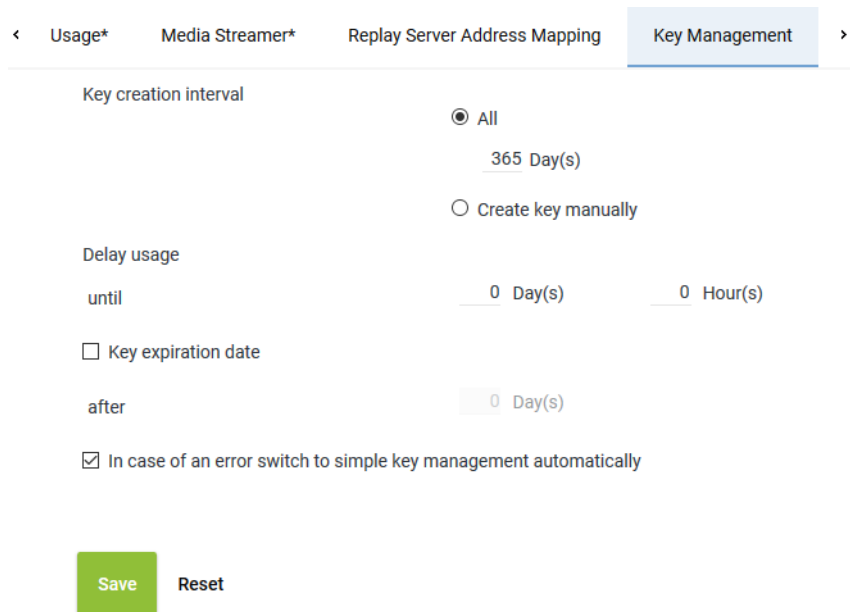


Fig. 452: Servers module - tab Key Management

<b>Key creation interval</b>	<p>Select whether a key is supposed to be generated automatically or manually. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>All</i> Select the intervals in which a new key is supposed to be generated automatically. Possible time interval: 1 to 365 days Default value: 365 days</li> <li>• <i>Create key manually</i> Select that a key is supposed to be generated manually.</li> </ul> <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>
<b>Delay usage</b>	<p>If required, enter a time interval during which the new key is not supposed to be used yet after having been created. Not until after this time interval has passed can the key be actually used for encryption.</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>
<b>Key expiration date</b>	<p>Select whether an inactive key is supposed to become invalid after the expiration of the time interval defined here.</p> <p><input type="checkbox"/> = Key never becomes invalid.</p>



	<p><input checked="" type="checkbox"/> = Key becomes invalid. In the entry field, enter the time interval after which the key loses its validity. Once this time interval has passed, the key cannot be used anymore. If recording data must be deleted after a certain period of time, this option offers additional security on top of the configured date of deletion. This especially applies to the case when recording data has been transferred manually to a storage location where the deletion mechanism of the system cannot find it.</p> <p><b>CAUTION!</b> All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the <u>neo</u> key management does not work (e. g. if the service <i>DongleMan</i> fails). If you have not activated the option, no recording takes place as long as the <u>neo</u> key management has been activated but does not work.</p> <p><input checked="" type="checkbox"/> = In case of an error, simple key management is used as replacement.</p> <p><input type="checkbox"/> = In case of an error, no recording takes place as long as the <u>neo</u> key management has been activated. In this case, disable key management in the tab <i>Usage</i>.</p>



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



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

### Tab Keystore/Virtualization

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

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

The tab *Keystore/Virtualization* is not active unless you have activated the function *VM without Trusted License* in the tab *Usage*. I. e. that you have not installed the licenses locally but would like to manage the licenses via an Internet connection by means of ASC license management.

#### For key management there are the following options:

- *Dongle*  
You can continue to use your existing dongle. The Dongle Manager reads out the encryption password from the dongle.  
In this case, no separate configuration is required.  
In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the Dongle Manager runs on.
- *Dongle Manager*  
In the current version, the Dongle Manager reads out the encryption password directly from the database. To enable this, you must enter the connection data to the server that the Dongle Manager runs on.
- *ASC License Management System*  
**NOTICE! License Management does not support encryption.**

#### For licensing, there are the following options:

*Without Internet access:*

- *Dongle*

Without Internet access you can continue to use your dongle for authentication purposes. In a virtualized environment, the USB port that the dongle has been plugged in to must have been assigned to the server that the VMware has been installed on. In this case, no separate configuration is required.

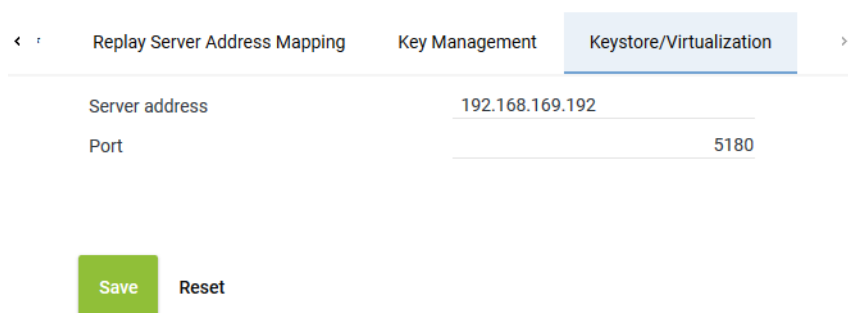
- *Trusted Virtualization License*

Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this. In this case, no separate configuration is required.

*With Internet access:*

- *ASC License Management System*

You can establish a connection to ASC's license management via the Internet. To do so, you must enter the connection data *licensing.asc.de* in this tab.



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

Fig. 453: Servers module - tab Keystore/Virtualization

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



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

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

### 7.3.2.6.3 Create PBX

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

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

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

⇒ The following window appears:

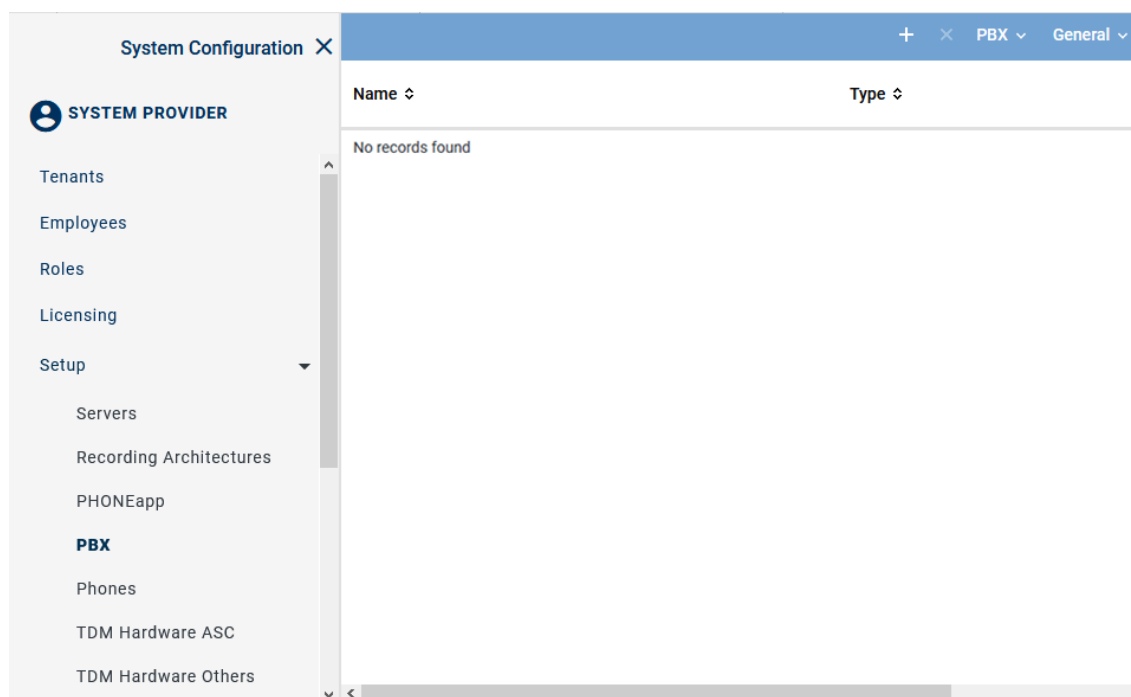




Fig. 454: PBX module - main view

### Toolbar of the PBX module

The toolbar offers the following functions.



Fig. 455: Toolbar PBX module


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

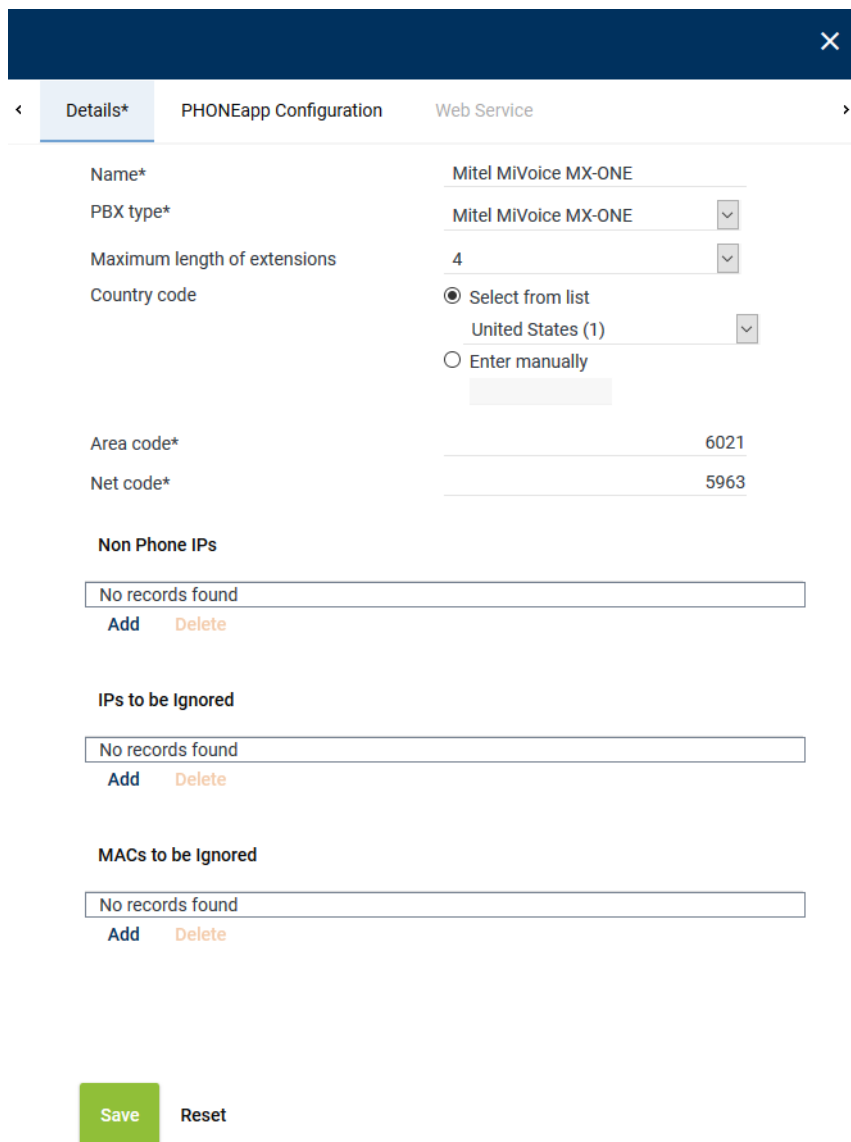
*Module Help* Opens the module-specific online help.



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

### Create new PBX

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



The screenshot shows a web form for creating a new PBX. At the top, there's a dark blue header bar with a close button (X). Below it, there are three tabs: 'Details\*' (selected), 'PHONEapp Configuration', and 'Web Service'. The 'Details\*' tab contains the following fields:

- Name\***: Mitel MiVoice MX-ONE
- PBX type\***: Mitel MiVoice MX-ONE (dropdown)
- Maximum length of extensions**: 4 (dropdown)
- Country code**: ☒ Select from list (United States (1) dropdown) or ☐ Enter manually
- Area code\***: 6021
- Net code\***: 5963

Below these fields, there are three sections for ignored records:

- Non Phone IPs**: No records found. Buttons: Add, Delete.
- IPs to be Ignored**: No records found. Buttons: Add, Delete.
- MACs to be Ignored**: No records found. Buttons: Add, Delete.

At the bottom, there are two buttons: a green 'Save' button and a 'Reset' button.

Fig. 456: Create new PBX - tab Details

- Set the following parameters in the detail view:

Parameter	Value/Description
<i>Name</i>	This <i>name</i> serves as the identifier of this PBX.
<i>PBX type</i>	Select the type of the <b>PBX</b> from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <li><i>Select from list</i></li> </ul>

Parameter	Value/Description
	Select the country code from the drop-down list. <ul style="list-style-type: none"> <li>• <i>Enter manually</i></li> </ul> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka <i>094</i> .
Area code	Enter the area code without the preceding 0, e. g. 6021.
Net code	Enter the net code, e. g. 5963. Do not enter an extension here.

Tab. 101: Create PBX

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

#### 7.3.2.6.4 Assign recording resources

##### Resources for tenants

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

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

##### Assign extensions to tenants

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

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

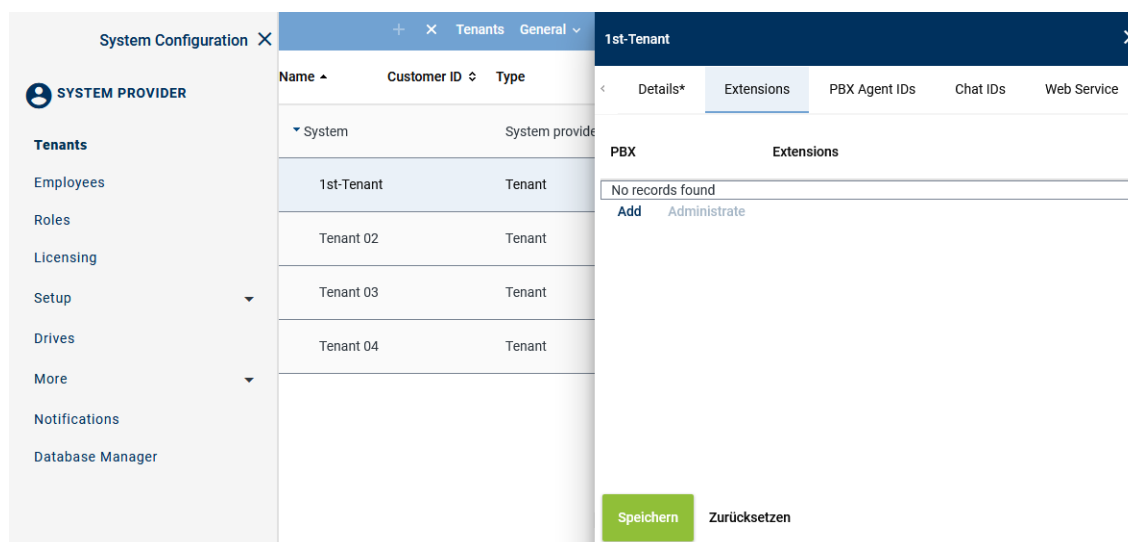


Fig. 457: Tenants - main view - tab Extensions

##### 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. 458: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>ZIP</li> <li>TXT</li> <li>CSV</li> </ul> <p><b>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>Click on the button <span style="background-color: #f1f3f4; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>Click on the button <i>Choose File</i>.</li> <li>Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>Click on the button <span style="background-color: #4285f4; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP<sub>neo</sub> active for Mitel MiVoice MX-ONE (CSTA3) - neo 6.x Rev. 34

386 / 489

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

Enter country codes as number ranges as follows:  
+4984496800-+4984496810

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

**NOTICE! Wildcards cannot be used!**

*Replace existing list of extensions*

Activate the check box to replace the list of extensions.

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

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

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

### Remove extensions

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

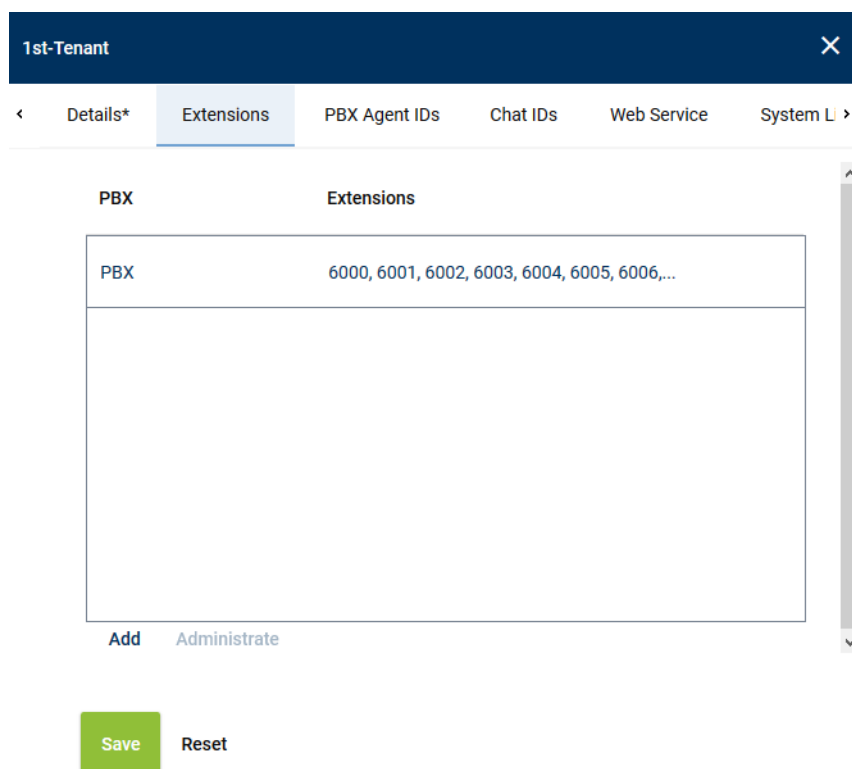


Fig. 459: Remove extensions

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. 460: 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.



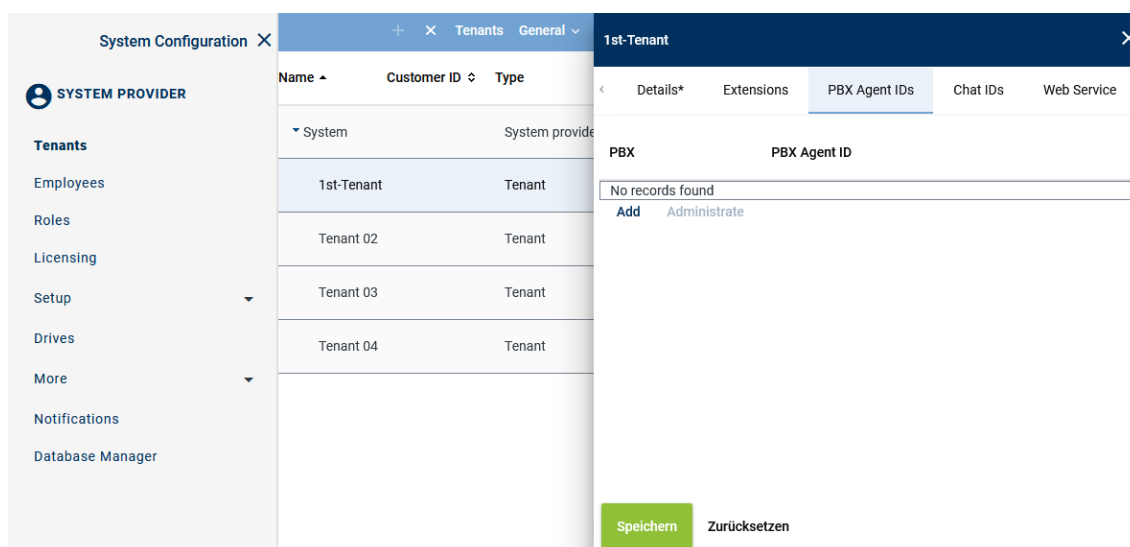
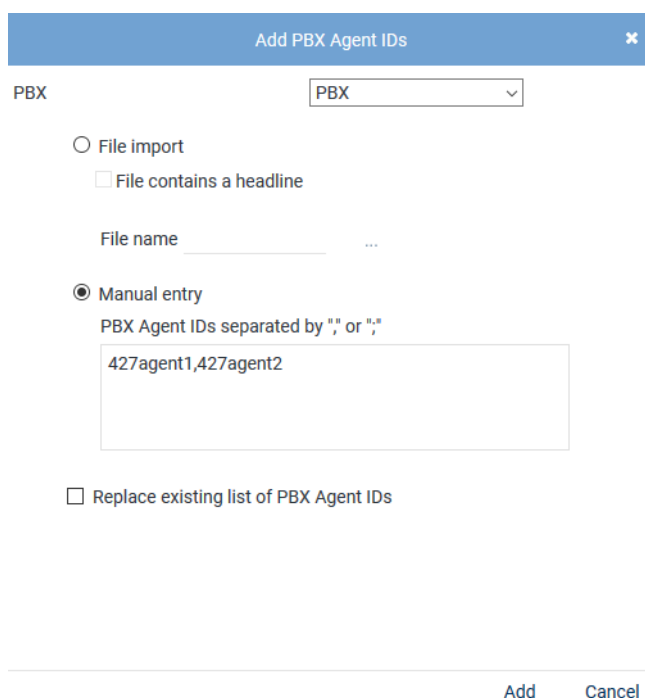


Fig. 461: Tenants - main view - tab PBX Agent ID

### 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:



The 'Add PBX Agent IDs' dialog box shows a dropdown menu for 'PBX' with 'PBX' selected. There are two radio buttons: 'File import' and 'Manual entry'. The 'Manual entry' option is selected. Below it, a text box contains '427agent1,427agent2'. There is a checkbox for 'File contains a headline' and another for 'Replace existing list of PBX Agent IDs'. At the bottom, there are 'Add' and 'Cancel' buttons.

Fig. 462: 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 the option to import PBX Agent IDs from an existing <a href="#">CSV</a> 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 <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> 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"> <li>• Click on the button <b>...</b> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <b>Upload File</b>.</li> </ul>
<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><b>NOTICE! Wildcards cannot be used!</b></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. 463: 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*.

### 7.3.2.6.5 Configure additional data

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

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

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

**System Configuration** ✕

**SYSTEM PROVIDER**

Setup ▾

- Servers
- Recording Architectures
- PHONEapp
- PBX
- Phones
- TDM Hardware ASC
- TDM Hardware Others
- Integrations
- Recording Import
- Additional Data**
- Activity Guard

Additional Data
↻ Additional Data
General ▾

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

Fig. 464: 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. 465: 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. 466: 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.

### 7.3.2.6.6 Create integration for Multi-Server Parallel Recording

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

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

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

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

⇒ The following window appears:

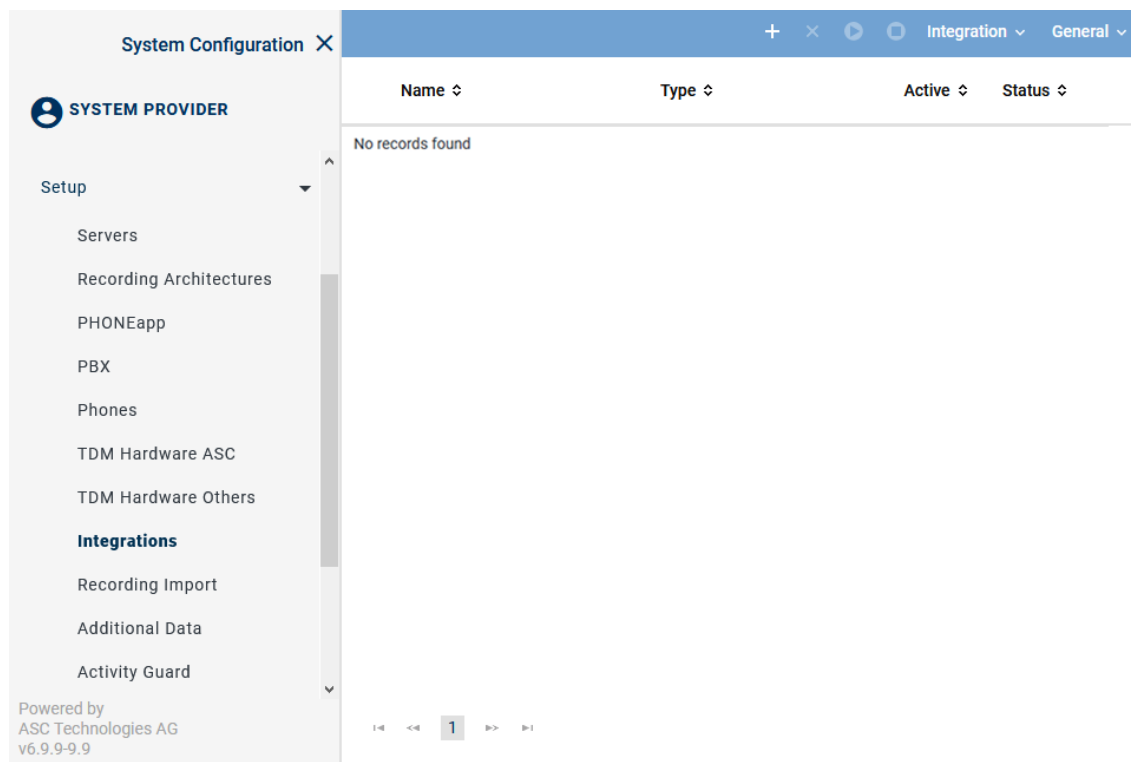




Fig. 467: Integrations - main view

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



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



### Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 468: Toolbar Integrations module

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

	<i>Activate</i>	Activates the selected integration. The integration can only be activated if it has been configured completely.
	<i>Deactivate</i>	Deactivates the selected integration. This stops running recordings.
<i>Integration</i>	<i>Import Grammar</i>	By clicking on this menu item, you can import a customized grammar which you can then configure in the configuration step for the CTI connection data.
<i>General</i>	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

### Import grammar

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

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

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

⇒ The window *Upload File* appears.

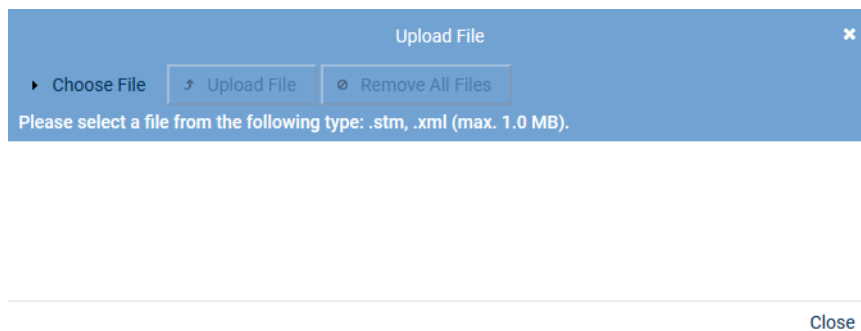


Fig. 469: Choose file

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*.

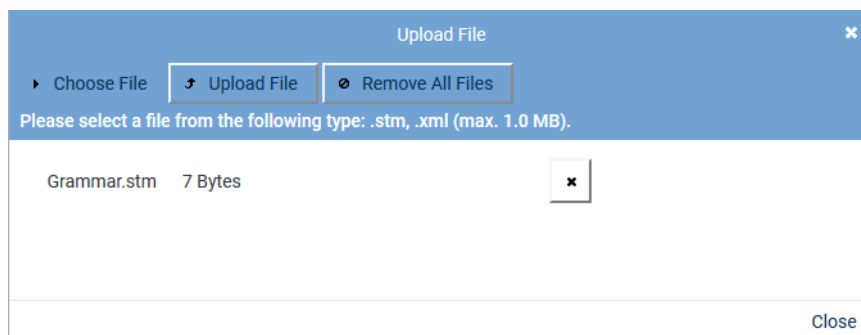



Fig. 470: Upload grammar

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


- 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. 471: Create integration type

- Enter the following parameters:

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

Tab. 102: Create integration type

- Click on the button  next to the field *PBX* to assign the [PBX](#).  
⇒ The window *PBX* appears.

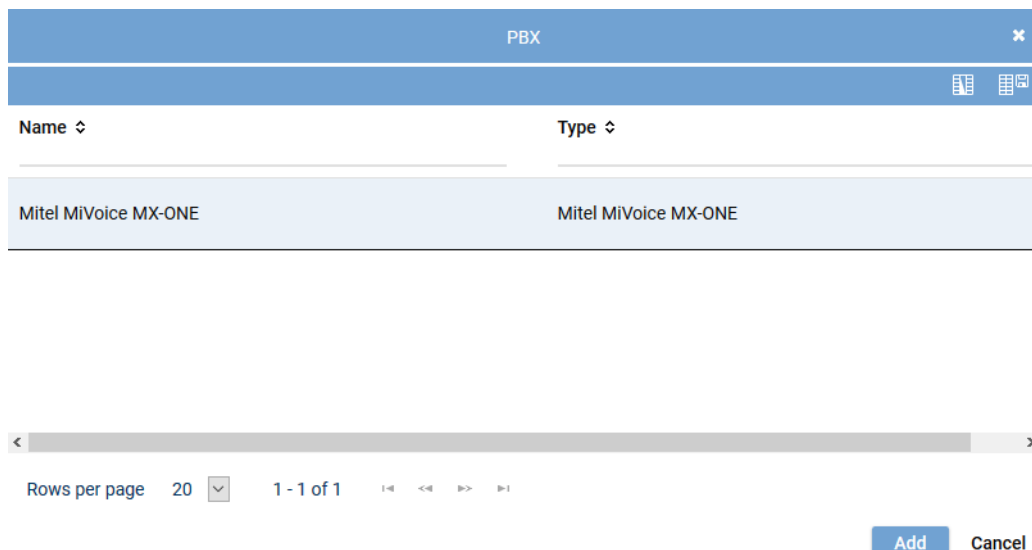


Fig. 472: Integrations - select PBX

- Select the respective [PBX](#) from the list of available PBXs.
- Click on the button *Add*.

### Assign recording architecture for Multi-Server Parallel Recording

- In the detail view on the bottom right, click on the button *Next*.

⇒ The tab *Recording Architecture* appears.

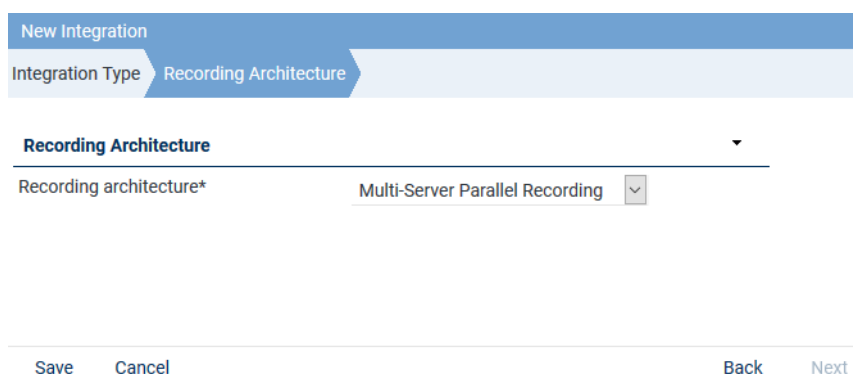


Fig. 473: Assign recording architecture - Multi-Server Parallel

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



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


3. Click on the button *Save*.

⇒ The integration now appears in the main view.



When using a recording architecture with parallel recording, the tab *Parallel Recording* appears in the detail view. In this tab, you can adjust the settings for the duplicate detection of parallel configured servers, see [chapter "Duplicates in parallel recording architectures", p. 445](#).

### 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. 474: 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.

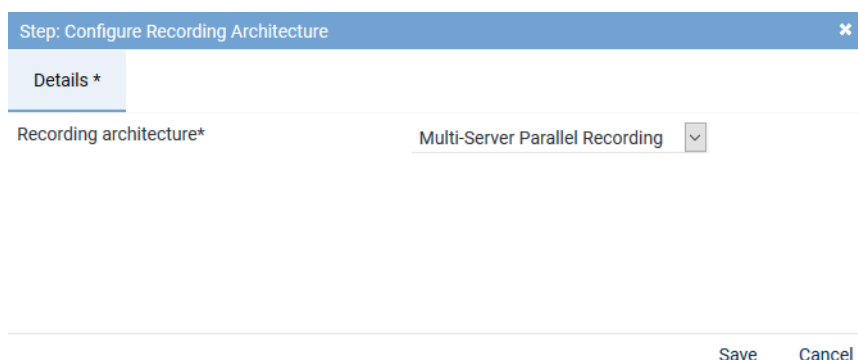



Fig. 475: Configuration step - Configure Recording Architecture

- 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 additional data if applicable.



In case of a missing or an inoperative **CTI** connection or if the end devices are not monitored, **SIP** and **RTP** data may still arrive at the recording server for end devices configured as *Automatic Call Recording Enabled*. As long as a recording profile has been configured in the Recording Planner module, the recording server can receive this **SIP** and **RTP** information from the **BIB** or from the gateway and process and record it accordingly. But as a result of missing **CTI**, only the minimum of information is tagged via **SIP**.



Following an update, you must configure this section again.

### Tab MiVoice MX-ONE (CSTA)

In the tab *MiVoice MX-ONE (CSTA)*, you configure the recording variants *Active Stream Recording* and/or *Intrusion* and/or *Trunk-side Recording*.

The **CSTA** connection is used to monitor the configured monitor points and to start the recording via the intrusion feature.

- Select the tab *MiVoice MX-ONE (CSTA)* to configure the **CSTA** connection to the PBX.

Step: Configure CTI Connection Data

MiVoice MX-ONE (CSTA)\* MBG

**CTIconnect Module**

Type CTIconnect active

Grammar name\* standard

Grammar version\* 1.00.12

**Connection Data Device Group 1**

**Connection Data Device Group 2**

**Additional Data**

Failover waiting time\* 10

Failover repetitions\* 3

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}$`

Save Cancel

Fig. 476: Configure tab MiVoice MX-ONE (CSTA)

Configure the **CSTA** connection so that monitoring can use it even if your recording runs via a **MBG**.



For parallel recording, you must configure the **MBG** in the tab **MBG**.

### 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. 477: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 103: 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 MiVoice MX-ONE (CSTA)

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.

**Connection Data Device Group 1** ▼

---

**PBX IP address**

No records found

[Add](#) [Edit](#) [Delete](#)

**Connection Data Device Group 2** ▼

---

**PBX IP address**

No records found

[Add](#) [Edit](#) [Delete](#)

Fig. 478: 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
✕

PBX IP address\* 192.168.170.219

PBX CSTA port\* 8882

Transport Layer Security (TLS) ☐

☒ Activate authentication

Application ID\* 1234

Password\* ●●●●●●●●●●●●●●●●

[Add](#) [Cancel](#)

Fig. 479: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
<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 run. Default is TCP 8882, optional for TLS 8883.
<i>Transport Layer Security</i>	Activate this check box to use the connection with TLS.

Parameter	Value/Description
<i>Activate authentication</i>	Activate this check box to use authentication for this connection. If you use authentication, it must have been activated in the Service Node Manager and in the application System Configuration. See <a href="#">chapter "Configure CSTA server", p. 14.</a>
<i>Application ID</i>	Enter the corresponding application ID from the Service Node Manager. The application ID must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See <a href="#">chapter "Configure CSTA server", p. 14.</a>

Tab. 104: Configure connection data

- 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.

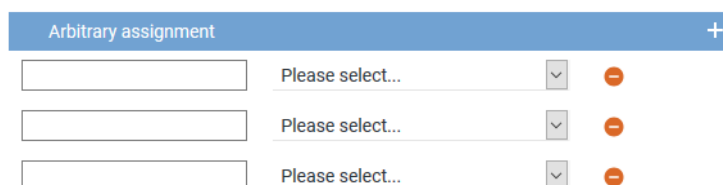



Fig. 480: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
  - *End time*
  - *Duration*
  - *Calling party phone number*
  - *Called party phone number*
  - *Conversation direction*
2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
  3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
  4. To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.  
⇒ An additional row appears to assign another additional data type.
  5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.



To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.



For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

### Configure 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 CTIconnect 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. 481: Configure switching conditions

<i>Failover waiting time</i>	This value indicates the maximum waiting time until the CTI <u>connect</u> 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 <u>connect</u> module is supposed to try to establish a connection before switching to the next configured connection. The CTI <u>connect</u> 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.



Following an update, you must configure this section 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. 482: 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.



As parallel recording is only possible via the MBG, the regular expression should be adjusted in this recording solution in a way that it never matches (e. g. Reg-Ex = "Parallel"). This allows identifying the recording type as "SRC".



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..](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 MBG

1. Select the tab [MBG](#) to configure the connection data for recording by means of MiVoice Border Gateway.

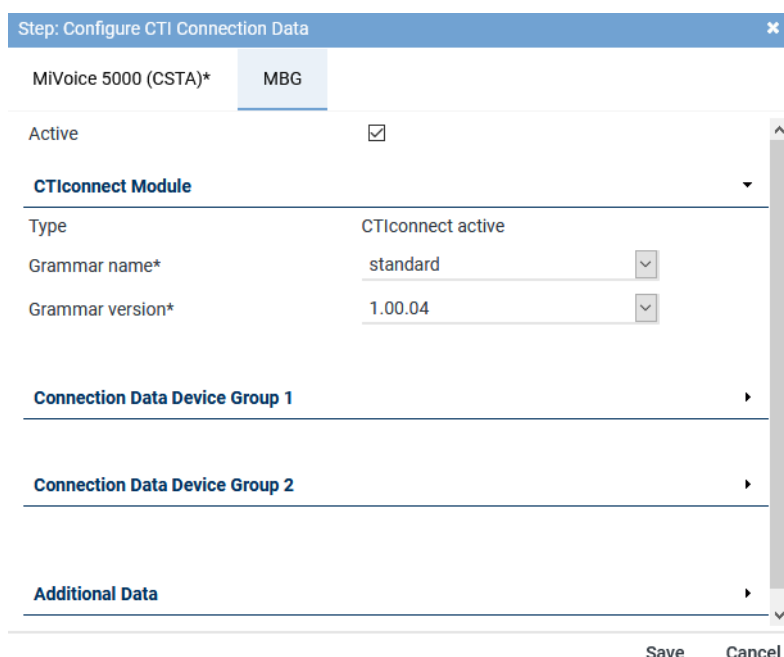


Fig. 483: Configure CTIconnect connection data to [MBG](#)



Following an update, you must configure this section again.

### ATTENTION!

In parallel recording architectures, calls must be recorded by means of the [MBG](#).

### Group field CTIconnect Module

In this group field, you can configure the parameters for the CTIconnect module.

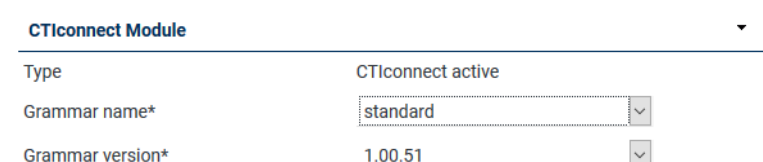


Fig. 484: Configure CTIconnect module

1. Enter the following parameters for the grammar:

Parameter	Value/Description
Type	Is filled automatically.
Grammar name	A default grammar has been preset. If required, select the name of the grammar from the drop-down list.
Grammar version	Select the current version of the grammar from the drop-down list.

Tab. 105: 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

For this recording architecture, you can configure the connection data for 2 servers.

For every device group, you can enter one or several sets of connection data.

The entries of the first set of data will be used by default during the connection establishment. If errors occur during this connection, it will be switched to the configured alternative connection.

**Connection Data Device Group 1**

---

Connection data

No records found

Add Edit Delete

**Connection Data Device Group 2**

---

Connection data

No records found

Add Edit Delete

Fig. 485: Group field Connection Data

- In the group field *Connection Data* in the table, click on the button *Add*.  
⇒ The following window appears:



Configure Connection
✕

Connection data\*
192.168.170.116

PBX port\*
6810

Activate indirect recording
☐

☒ Use pre-shared key

Pre-shared key (PSK)\*
••••••••••

[Add](#)
[Cancel](#)

Fig. 486: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the <a href="#">MBG</a> .
<i>PBX port</i>	Enter the port for the <a href="#">MBG</a> or the <a href="#">SRC</a> , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.
<i>Use pre-shared key</i>	Activate the check box if the <a href="#">MBG</a> is used in the PSK mode and the authentication is supposed to be done via the pre-shared procedure.
<i>Pre-shared key (PSK)</i>	Enter the pre-shared key.

Tab. 106: 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.

### Group field Additional Data MBG

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.



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*

For this recording variant, you can opt for an arbitrary assignment of additional data delivered by the PBX.

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.

**Additional Data** ▼

---

Arbitrary assignment


Key 0	Please select...	▼
Key 1	Please select...	▼
Key 2	Please select...	▼

Fig. 487: CTI connection data - additional data module 1

2. Click on the respective entry field, e. g. *Key 0* and enter the name of the database field from the protocol that the information is supposed to be extracted from. Observe the correct spelling.
3. From the drop-down list, select the entry which is supposed to appear as column headline in the players.
4. Click on the button *Save* to apply the settings and to finish this configuration step.

### Configure monitor points for MX-ONE CSTA

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.

Step: Configure Monitor Points ✕

Extension Monitor Points

---

Extension ▲ Active ⇅ Intrusion ⇅

No records found

**Add** Active/Inactive Delete

---

Save Cancel

Fig. 488: Configuration step - configure monitor points

### Tab 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. 489: Add extension monitor points

<b>File import</b>	<p>Select this option to import extensions from an existing <b>CSV</b> 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"> <li>• Click on the button <span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <span style="background-color: #4a86e8; color: white; padding: 0 5px;">↗</span> (<i>Upload file</i>).</li> </ul>
	<p><b>File contains a headline</b></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The <b>CSV</b> file may not contain more than 1 column. If commas or other column delimiters are found in the <b>CSV</b> 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 <b>CSV</b> file, you have to pack it in a ZIP file.</p>
	<p><b>File name</b></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>• Click on the button <span style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>• Click on the button <i>Choose File</i>.</li> <li>• Select the respective ZIP file via the Explorer and click on the button <i>Open</i>.</li> <li>• Click on the button <span style="background-color: #4a86e8; color: white; padding: 0 5px;">↗</span> (<i>Upload file</i>).</li> </ul>
<b>Manual entry</b>	<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. 490: Configured extension monitor points

<b>Add</b>	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.
<b>Active/Inactive</b>	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.

<i>Delete</i>	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.
---------------	--



In parallel recording, you cannot use the Intrusion feature.

<i>Intrusion</i>	Do not enter a check mark in the line Intrusion when recording in parallel. <input type="checkbox"/> = Intrusion feature has not been activated.
------------------	---


- 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. 16](#).

### Global recording settings

- Click on the button  (*Edit configuration step*) in the line *Global recording settings* in the main view.

⇒ The window *Step: Global Recording Settings* appears.

Step: Global Recording Settings

Details\*

Transport protocol	UDP	
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. 491: Configuration step - Global Recording Settings

- Set the following parameters in the tab *Details*:

Parameter	Value/Description
<i>Transport protocol</i>	Select the transport protocol that the recording server uses for SIP signaling from the drop-down list. In <i>active-stream recording</i> , the transport protocol applies for the SIP com-

Parameter	Value/Description
	<p>munication between the recording server and the phones; in case of <i>intrusion</i>, for the SIP communication between the PBX and the recording server.</p> <p>The following protocols are available:</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p>
Port SIP signaling	Enter the port for SIP signaling that is opened on the recording server for incoming SIP communication and that has been selected in the outgoing SIP notifications as the port of the recording server. Default 5060.
Remote SIP port	Enter the port for the end devices. On this port, the recording server can reach the Mitel end devices by SIP to start <i>active-stream recording</i> . Default 7300.
Activate SIP authentication	Activate the check box if 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> .
User name of the SIP registration	Enter the user name for SIP registration of extensions recorded with intrusion feature. The user name is configured in the PBX and applies for all extensions to be registered.
Password of the SIP registration	Enter the password for SIP registration of extensions recorded with intrusion feature. The password is configured in the PBX and applies for all extensions to be registered.
Activate PBX connection	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.
SIP registration expiration	Enter the period in seconds until the registration runs out.
PBX IP address	Enter the IP address of the PBX.
PBX port	Enter the port for the communication with the PBX, default 5060.


Tab. 107: Global recording settings

- Click on the button **Save** to apply the settings and to finish this configuration step.



Following an update, you must configure this section 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.

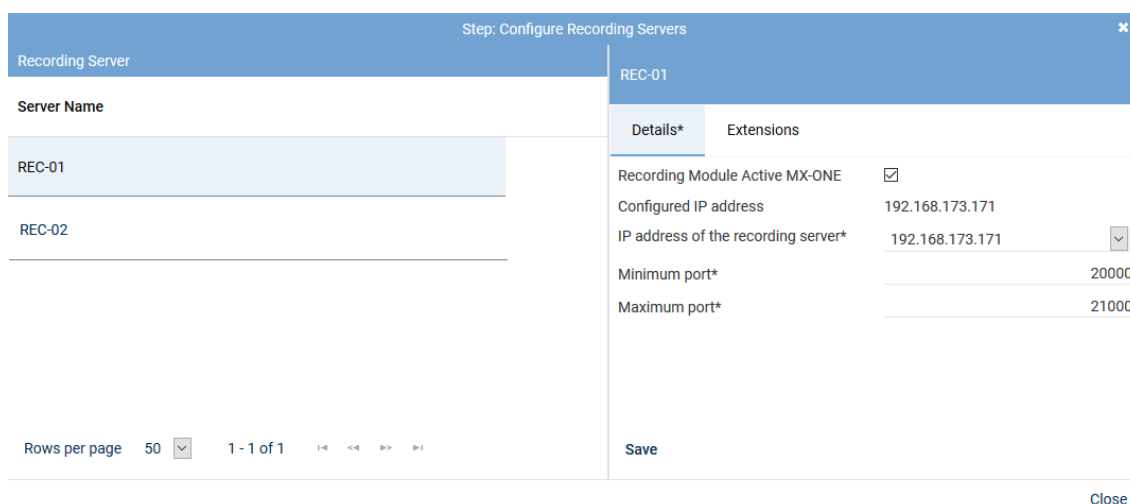


Fig. 492: Configuration step - Configure recording servers

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 <b>RTP</b> data from the recording server, e. g. <b>20000</b> .
<i>Maximum port</i>	Enter the highest port configured on the PBX that is used to receive the <b>RTP</b> data from the recording server, e. g. <b>21000</b> .

Tab. 108: 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.



Following an update, you must configure this section 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.



Only those add-ons are displayed for which a license has been installed in the system.

### 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. 493: Configure add-on for MiContact Center Enterprise

### Group field CTIconnect Module

1. Enter the following parameters for the grammar:



Parameter	Value/Description
<i>Type</i>	Is filled automatically.
<i>Grammar name</i>	A default grammar has been preset. If required, 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. 109: 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. 110: 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. 494: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
  - *End time*
  - *Duration*
  - *Calling party phone number*
  - *Called party phone number*
  - *Conversation direction*
2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
  3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
  4. To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.  
⇒ An additional row appears to assign another additional data type.
  5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.



To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.



For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

### **Configure add-on for 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<sup>connect</sup> 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

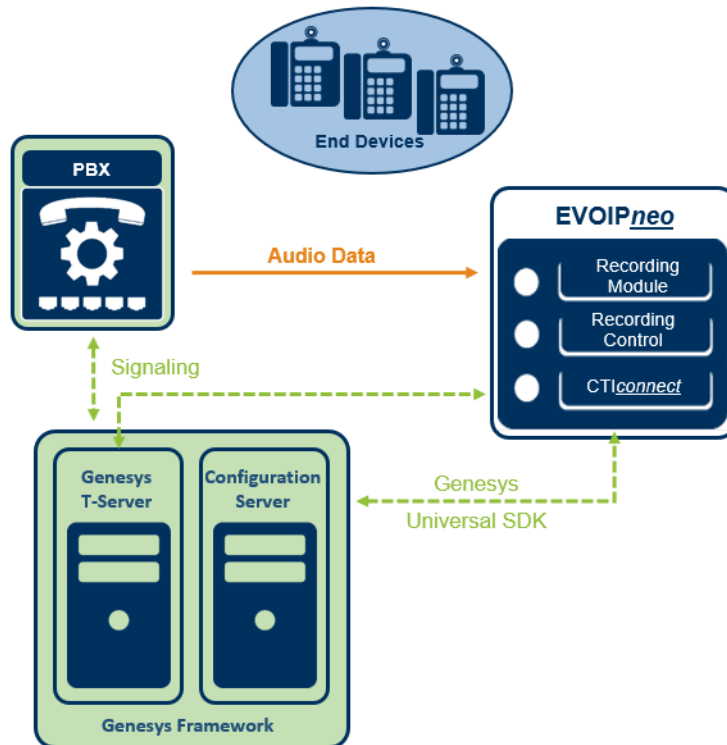


Fig. 495: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 465](#).

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*.

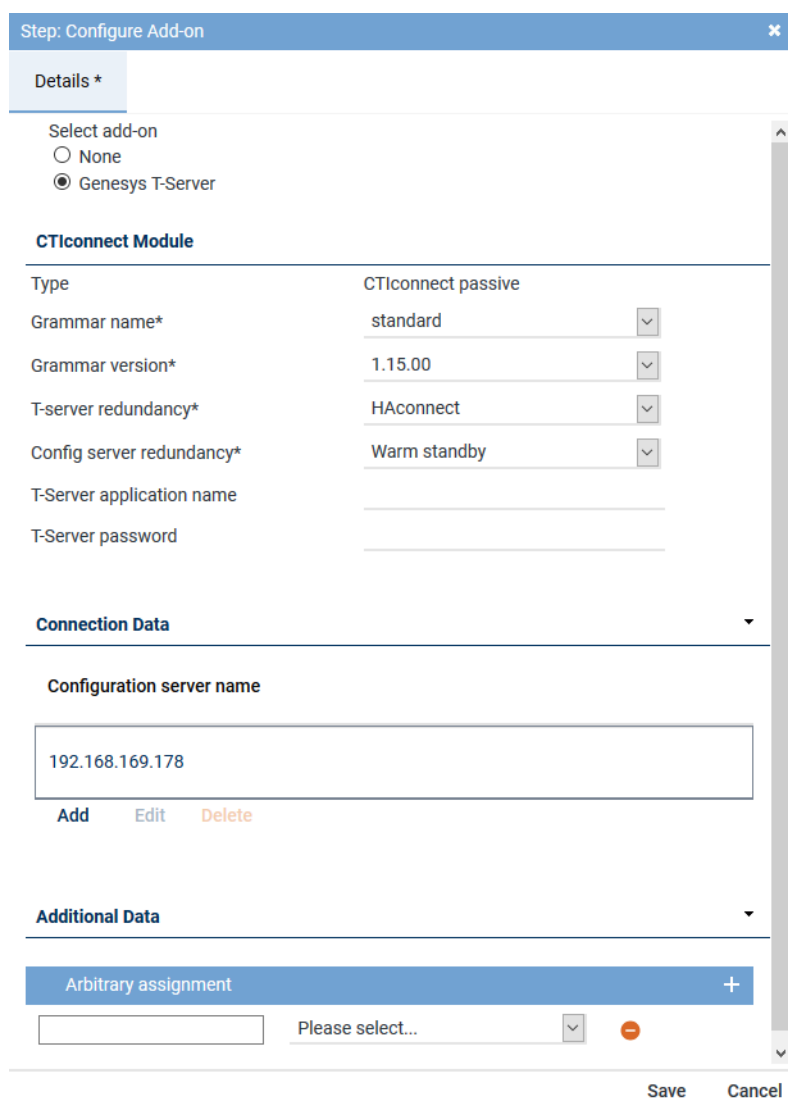
### Adjust configuration file for Genesys add-on

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. 496: 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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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"> <li>• <i>No redundancy</i></li> <li>• <i>HAconnect</i> - for High Availability Connection</li> <li>• <i>Warm Standby</i> - for a connectable redundancy</li> </ul>
<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. 111: 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:

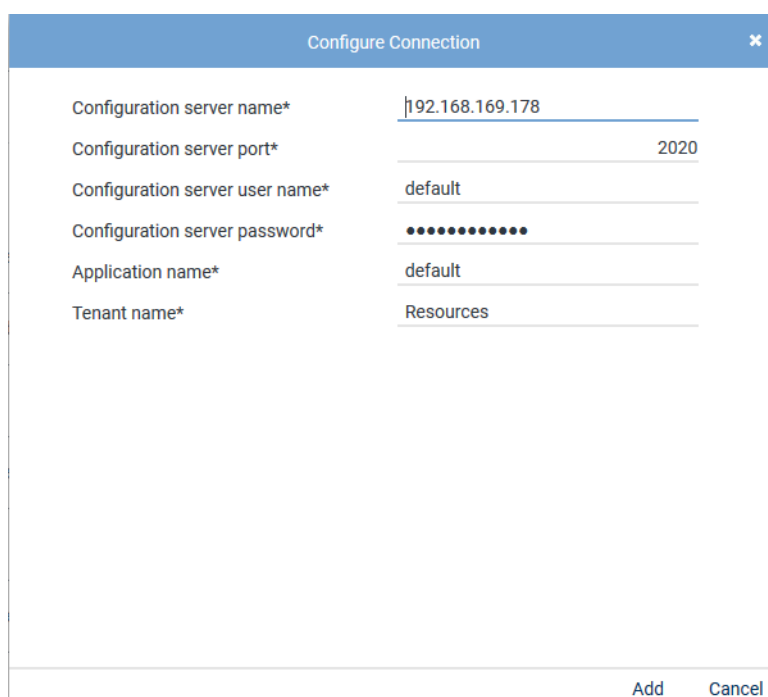


Fig. 497: Configure connection data

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. 112: 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. 498: Arbitrary assignment of the additional data

The following additional data is always available:

- *Start time*
  - *End time*
  - *Duration*
  - *Calling party phone number*
  - *Called party phone number*
  - *Conversation direction*
2. In the entry field on the left, enter the description of the additional data type from the protocol. Observe the same spelling as it is used in the protocol. The information which is read out of the protocol is displayed in the columns in the players.
  3. From the drop-down list, select the respective display name that you have configured in the Additional Data module. Only those display names are displayed for which the option *Available* has been activated in the Additional Data module.
  4. To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.
    - ⇒ An additional row appears to assign another additional data type.
  5. Click on the button *Save* in the detail view to save the entries and finish this configuration step.

The add-on provides additional data that can be tagged in customer-specific additional data fields (customCP fields). By means of these additional data fields, the respective recording behavior can be reached by means of the recording planner, e. g. recording start beginning with tagging or threat call scenario.




To allow users to control the recording by means of keys, you must configure the recording profile accordingly in the Recording Planner module.



For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

### Configure miscellaneous settings

1. Click on the button  (*Edit configuration step*) in the line *Configure recording servers* in the main view.
  - ⇒ The window *Step: Miscellaneous Settings* appears.

Step: Miscellaneous Settings

×

Details

Dispatcher

Please select...

▼

Save

Cancel

Fig. 499: 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. 500: 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. 501: 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. 502: Deactivate integration

- Click on the icon  (*Delete*) and confirm the security prompt to delete the integration.

### 7.3.3 Configure Recording Content Validation

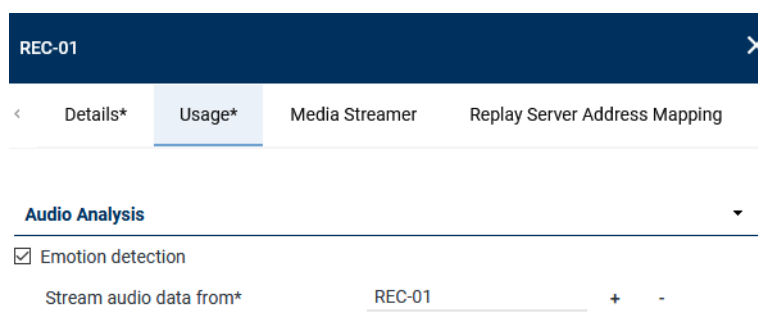
Recording Content Validation is an easy and quick possibility to check the functionality of the recording system whenever required. The information is displayed in the Notifications module. Reports can be used to visualize the results.

Preconditions for validation:

- The license *Recording Content Validation* must have been installed.
- *Emotion detection* must have been activated in the *Servers* module.
- The server for emotion detection must have been selected.

#### Configuration in the Servers module

- Go to the *Servers* module.
- In the main view, select the server that you would like to configure.
- Select the tab *Usage*.
- Open the group field *Audio Analysis*.



REC-01

< Details\* Usage\* Media Streamer Replay Server Address Mapping

Audio Analysis

☒ Emotion detection

Stream audio data from\* REC-01 + -

Fig. 503: Servers module - Activate emotion detection

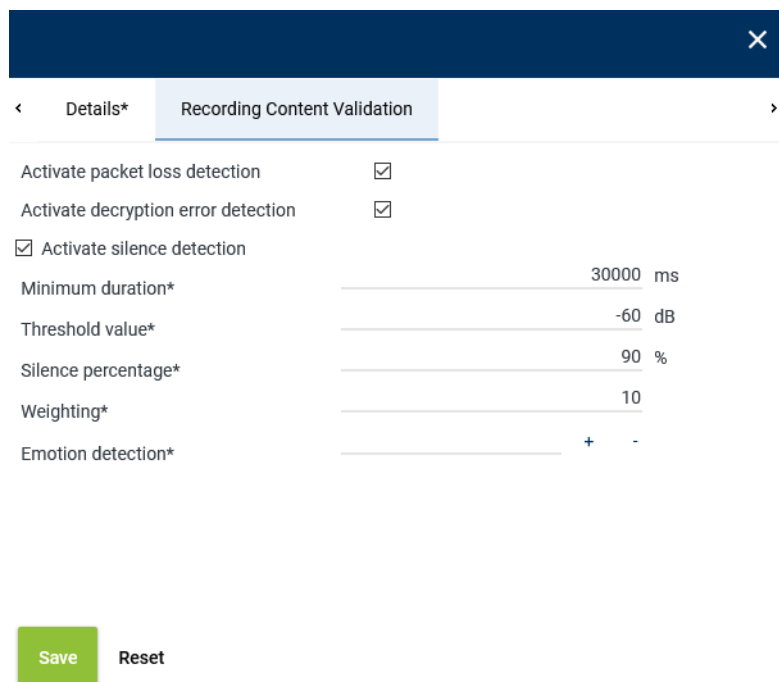
5. Activate the function *Emotion detection*.
6. By clicking on the icon **+**, select the server that emotion detection runs on.
  - ⇒ This server will then appear in the list in the Integrations module in the tab *Recording Content Validation* to configure silence detection.

### Configuration in the Integrations module

1. In the main view, select the integration for which you would like to check the validity of recording.
2. Select the tab *Recording Content Validation*.

The following criteria are available to check proper recording:

- *Packet loss detection*
- *Decryption error detection*
- *Silence detection*



Details\* Recording Content Validation

Activate packet loss detection ☒

Activate decryption error detection ☒

☒ Activate silence detection

Minimum duration\* 30000 ms

Threshold value\* -60 dB

Silence percentage\* 90 %


Weighting\* 10

Emotion detection\* + -

Save Reset

Fig. 504: Create integration - tab Recording Content Validation

Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost.
<b>NOTICE!</b> Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.	

Activate decryption error detection	<input checked="" type="checkbox"/> Activate the check box to check whether errors occurred during decryption. <b>NOTICE!</b> Decryption errors result in noise which may corrupt the audio file.
Activate silence detection	<input checked="" type="checkbox"/> Activate the check box to check whether the recording contain sections of silence and under which conditions sections are recognized as silence. <b>NOTICE!</b> Detection is useful in case the PBX sends RTP packages which contain silence instead of an audio signal.
<i>Minimum duration</i>	Enter the minimum duration of silence after which a notification is supposed to be issued. Default value is 30000 ms (30 seconds).
<i>Threshold value</i>	Enter a threshold value of the audio level in dB under which the section is supposed to be considered a silence section. Default value is -60 dB.
<i>Silence percentage</i>	Enter the percentage of silence in a recording which is supposed to trigger a notification. Default value is 90 %.
<i>Weighting</i>	Enter the smoothing factor defining to which extent the audio curves (samples) are supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 0-10000 can be recommended.
<i>Emotion detection server</i>	By clicking on the icon  , select the server that emotion detection runs on. The speech analysis software recognizes whether there are silence sections in the recording.

**NOTICE!** The list only displays servers which have been configured for audio analysis and have been assigned in the Servers module.

3. Select the respective server from the list of available servers.





Emotion Detection

Name

REC-01

Rows per page 20

1 - 8 of 8

Add

Cancel

Fig. 505: Select server for emotion detection

- Click on the button *Add* to apply the selected server.
- To save the settings, click on the button *Save*.  
To discard the settings, click on the button *Reset*.

### Configuration in the Notifications module

To issue notifications in case of an error, the corresponding notifications must be configured in the Notifications module.



For basic information about the Notifications module refer to the administration manual for tenants *Notifications module*.

### Configuration in the application INSIGHT<sub>neo</sub>

To issue a report visualizing the errors occurred, a report must be created in the application INSIGHT<sub>neo</sub>.



For information about using the Report Templates module and the Report Instances module refer to the respective INSIGHT<sub>neo</sub> user manuals.

## 7.3.4 Configure PHONEapp for Mitel

If you would like to use the XML PHONE<sub>app</sub>, 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 PHONE<sub>app</sub> 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 Servers module

To be able to control the recording by means of PHONE<sub>app</sub>, 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*.

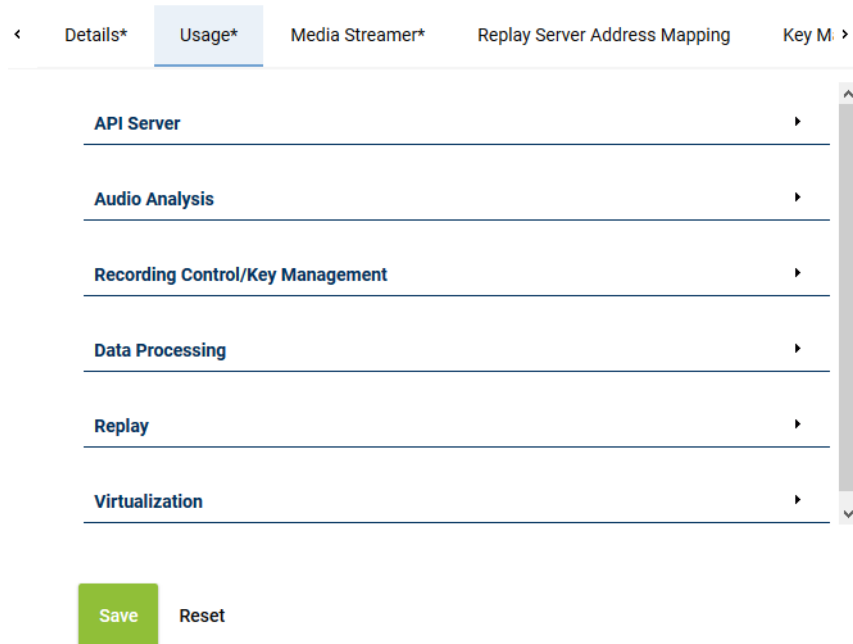


Fig. 506: Servers - tab Usage

- Open the group field *Recording Control/Key Management*.

#### 7.3.4.1.1 Group field Recording Control/Key Management

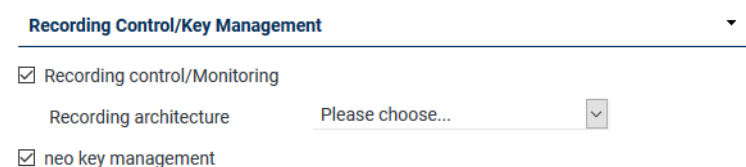


Fig. 507: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Monitoring</i>	<p>Activate the check box if you would like to use <a href="#">CLIENT</a><i>command</i> or <a href="#">API</a> recording control or monitoring for live listening and viewing. The function is only available if a recording architecture has been configured and activated.</p> <ul style="list-style-type: none"> <li>Recording architecture From the drop-down list, select the recording architecture via which you would like to control the recording.</li> </ul>
<i>neo key management</i>	<p>This function serves for customer-specific recording encryption. To be able to configure the conditions for key management, activate the check box <i>Key management</i>.</p> <p>The function can only be activated if the license <code>ASC_KEY_MANAGEMENT</code> is available.</p> <p>For more information about the configuration of key management refer to the administration manual <i>Configuration server and recording architectures</i> and to the installation manual <i>Installation Dongle Manager</i>.</p>

Tab. 113: Configure recording control/key management

### 7.3.4.2 Configure PHONEapp module

In the PHONEapp module, you can configure the default settings for phone applications and configure phone types.

1. In the navigation bar, select the menu item *Setup > PHONEapp*.

⇒ The following window appears:

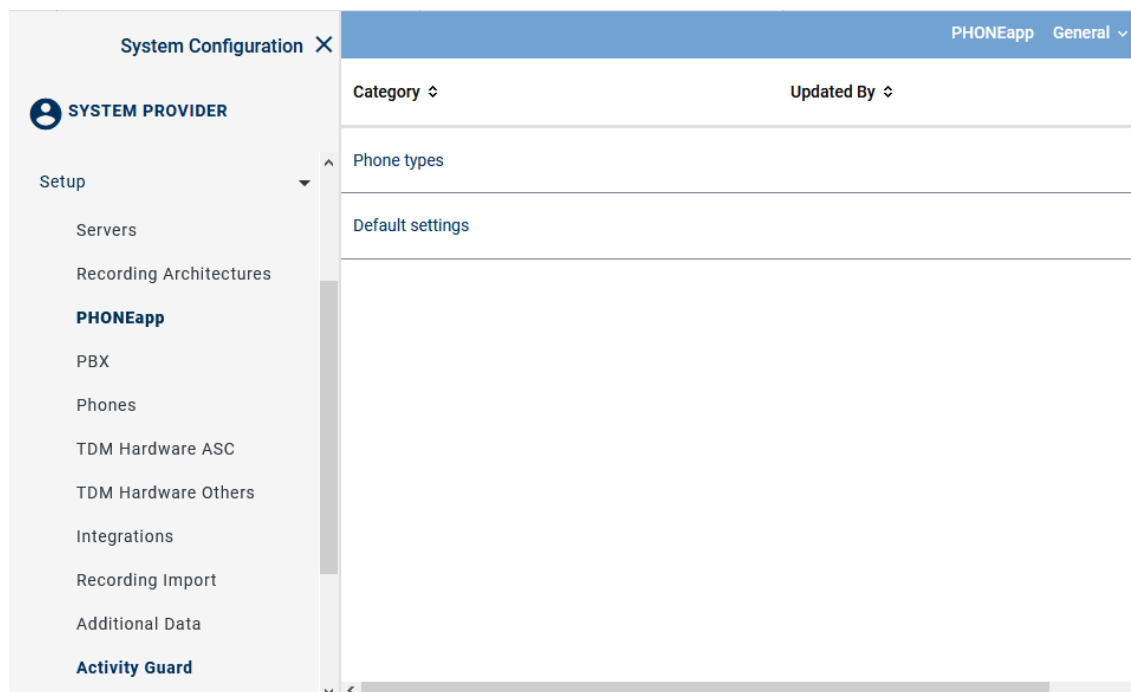


Fig. 508: PHONEapp - main view:

In the category *Phone types*, you can display the properties of the supported end devices and add additional phone types.

#### 7.3.4.2.1 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.

Phone Types	
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. 509: Detail view phone types

- 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.

MITEL	
Details	
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"/>
Save    Reset	
OK	

Fig. 510: 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.

### 7.3.4.2.2 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\*

http://192.168.170.218

Only certified requests

☐

Language

Time Parameter

Response waiting time\*

2000

Milliseconds

Error waiting time\*

2000

Milliseconds

Phone refresh interval\*

4000

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

No records found

Save

Reset

Fig. 511: Detail view Default settings



2. Adjust the respective settings.
3. Click on the button **Save**.

<i>General</i>	Here, you have to enter the address of the <u>PHONEapp</u> and activate it.
<ul style="list-style-type: none"> <li>• <i>Activated</i></li> </ul>	Activates the recording control by means of the <u>PHONEapp</u> .
<ul style="list-style-type: none"> <li>• <i>PHONEapp URL</i></li> </ul>	<p>Enter the URL under which the <u>PHONEapp</u> is supposed to be accessible. You may use the IP address or the host name of the application server.</p> <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://&lt;core_ip&gt;:90</i>.</p> <p>The end device will establish a connection with this URL. The <u>PHONEapp</u> 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"> <li>• <i>Only certified requests</i></li> </ul>	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.
<i>Language</i>	Select the respective default language for the <u>PHONEapp</u> from the drop-down list. The selected language applies to all end devices, unless the display language in the module <i>Setup &gt; Phones</i> is not configured otherwise.
<i>Time Parameter</i>	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.
<ul style="list-style-type: none"> <li>• <i>Response waiting time</i></li> </ul>	Define the period of time during which the <u>PHONEapp</u> 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.
<ul style="list-style-type: none"> <li>• <i>Error waiting time</i></li> </ul>	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 <u>PHONEapp</u> 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.
<ul style="list-style-type: none"> <li>• <i>Phone refresh interval</i> (this setting is only relevant for Alcatel and Cisco)</li> </ul>	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.

<i>Tagging Attributes</i>	Here, you define which data field is filled when tagging via the PHONEapp. All additional data fields as well as the field <code>ASC_COMMENT</code> are available.
<i>Register Fields</i>	Here, you configure how the tagging value is displayed. All IDs listed under <i>Setup &gt; Additional Data</i> as well as the field <code>ASC_COMMENT</code> can be used.
<i>Predefined Tagging Fields</i>	Define whether a comment field with free text or selectable predefined tagging fields are supposed to be used and saved on the end devices.
<ul style="list-style-type: none"> <li>• <i>Activated</i></li> </ul>	Activates the list of predefined tagging fields on the end device. If the function has been deactivated, a manual comment field is displayed.
<ul style="list-style-type: none"> <li>• <i>Tagging Field</i></li> </ul>	Define which selectable predefined tagging fields are supposed to be used and saved on the end devices.

### Configure group field 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. 512: 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.

**Tagging Attributes**

Request Parameter	Field	
tag_field	ASC_COMMENT	
<input type="text" value="New request parameter"/>	<input type="text" value="New field"/>	 

**Add** **Delete**

Fig. 513: Edit tagging attributes

- Enter the respective parameters.
- To save the changes, click on the icon  .  
To discard the changes, click on the icon  .
- In the detail view, click on the button *Save* to apply the changes in the tab *Default Settings*.

### Delete tagging attributes



- In the detail view, select the attribute you would like to delete.
- Click on the button *Delete*.
- Click on the button *Yes*.  
⇒ The selected attribute is removed from the list.
- Click on the button *Save* to apply the change in the tab *Default settings*.

### Configure group field Register Fields

#### Add and edit register fields


- 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. 514: Group field Register Fields



- Click on the button *Add*.  
⇒ A new entry is added.
- To edit the entry, click on the icon  .  
⇒ The line can be edited.

**Register Fields**

Field	Recording Control Field	Active
Comment	ASC_COMMENT	<input checked="" type="checkbox"/> 
<input type="text" value="New field"/>	<input type="text" value="New RC field"/>	<input checked="" type="checkbox"/>  

[Add](#) [Delete](#)

Fig. 515: Edit register fields

- 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.
- Activate or deactivate the register field via the check box.
- To save the changes, click on the icon .  
To discard the changes, click on the icon .
- In the detail view, click on the button *Save* to apply the changes in the tab *Default Settings*.

#### Delete register fields

- In the detail view, select the attribute you would like to delete.
- Click on the button *Delete*.
- Click on the button *Yes*.  
⇒ The selected attribute is removed from the list.
- Click on the button *Save* to apply the change in the tab *Default Settings*.

#### Configure group field 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

- In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Predefined Tagging Fields*.
- 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.

- In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Predefined Tagging Fields*.

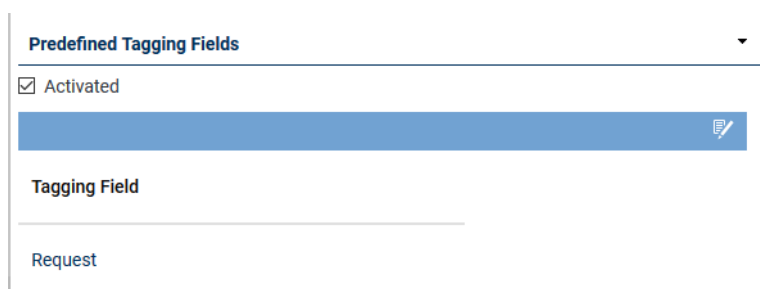

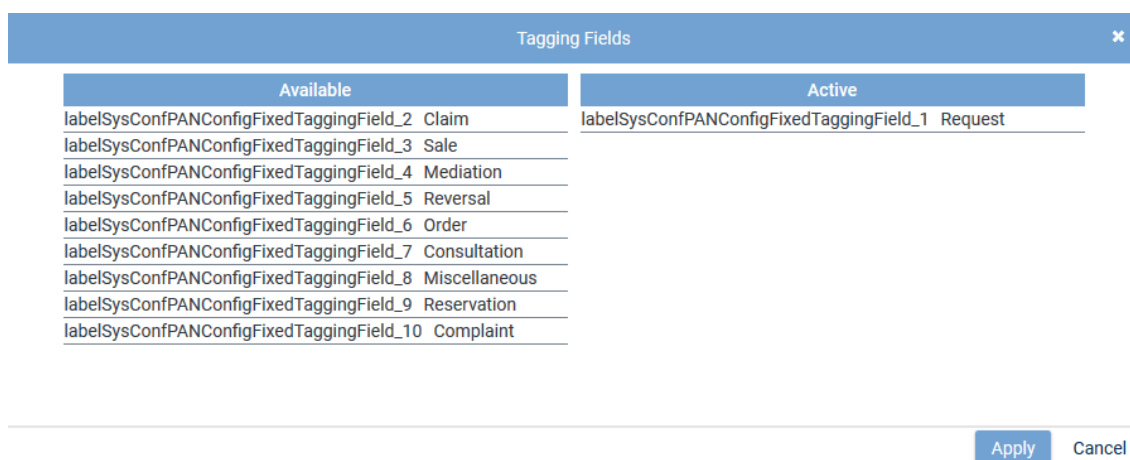



Fig. 516: Configure tagging fields

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. 517: 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.
	<i>Apply</i>	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.

### 7.3.4.3 Configure PBX module

In the PBX module, you must activate the PHONEapp configuration.

1. Select the menu item *Setup > PBX* in the navigation bar.
2. Select the tab PHONEapp Configuration.

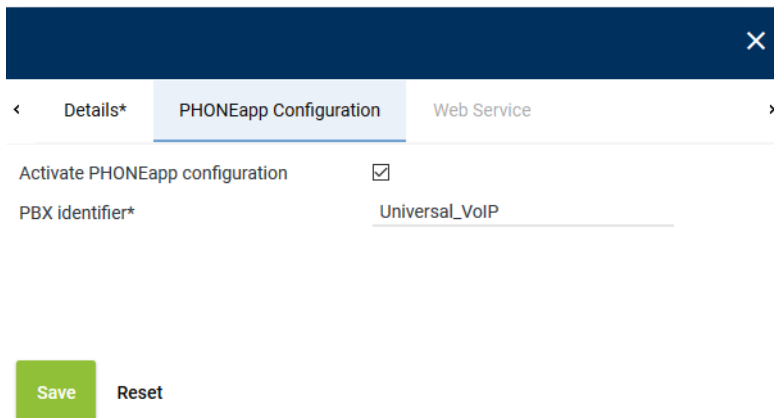


Fig. 518: Activate PHONEapp configuration

3. Enter the following parameters:

Activate PHONE <u>app</u> configuration	Here, the PHONE <u>app</u> is activated.
---	--

**PBX identifier**

Enter the identifier of the PBX. The ID allows identifying the end devices unambiguously when using several PBXs in connection with PHONEapps.. This identifier is defined during the installation of the PBX. Use letters, numbers, and understrikes.

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.

#### 7.3.4.4 Configure Phones module

To use the Mitel PHONEapp, you must create the phone type in the Phones module.

1. Select the menu item *Setup > Phones* in the navigation bar.

⇒ The following window appears:

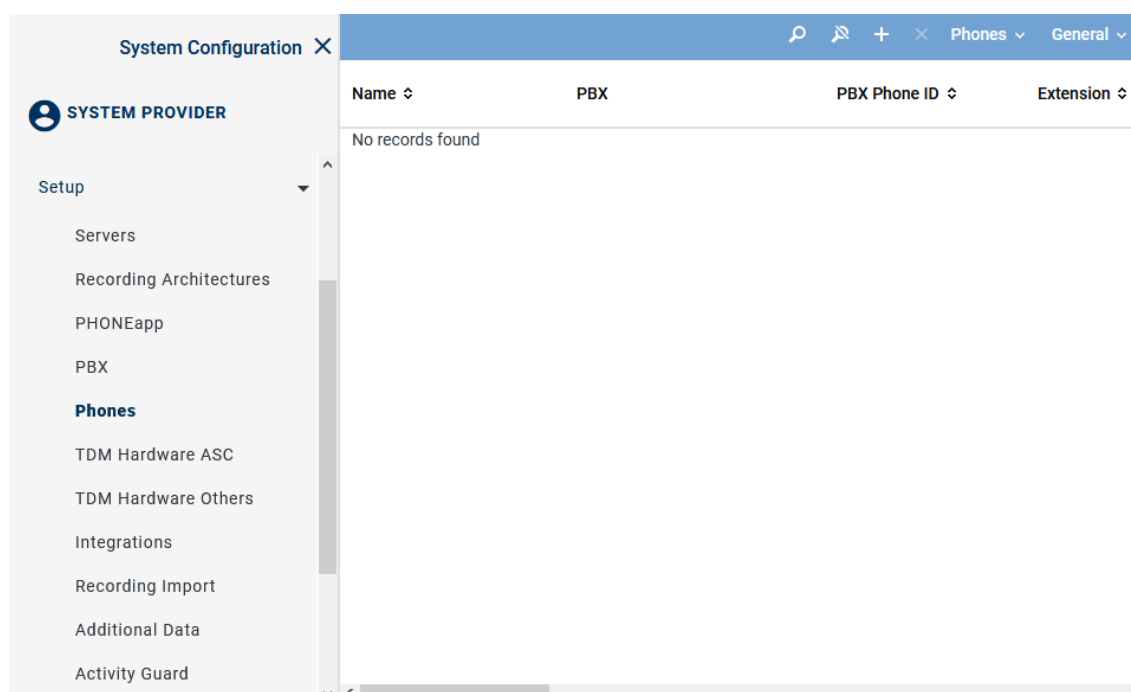


Fig. 519: Phones - main view

Depending on the table configuration, the following information is displayed in the table in the main view:






<b>Name</b>	Shows the name of the phone.
<b>PBX</b>	Shows the name of the PBX.
<b>PBX Phone ID</b>	Shows the identifier which has been configured for the phone in the PBX.
<b>Extension</b>	Shows the assigned extension of the phone.
<b>Computer Name</b>	Shows the computer name if it has been defined in the details.
<b>Phone Type</b>	Shows the selected phone type if the PHONE <u>app</u> configuration has been activated.
<b>Display Language</b>	Shows the selected display language.

#### 7.3.4.4.1 Toolbar of the Phones module


The toolbar offers the following functions.



Fig. 520: Toolbar

	<i>Create</i>	Create a new phone. Available are <ul style="list-style-type: none"> <li>• IP phone</li> <li>• TDM phone</li> </ul>
	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see Search.  The icon  is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all search filters so that the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected phone upon confirming the security prompt.
<i>Phones</i>	<i>Import</i>	Opens a window in which you can select an XSLT file to be imported.
	<i>Edit</i>	Allows multiple editing of existing phones.
<i>General</i>	<i>Print</i>	Opens a list of existing phones along with the option to print it.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
	<i>Save Table Configuration</i>	Saves the current table configuration of the main view as the default view of the user.
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.

#### 7.3.4.4.2 Create phones

1. To create and configure new phones manually, click on the icon  (*Create*) in the toolbar of the main view.

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.

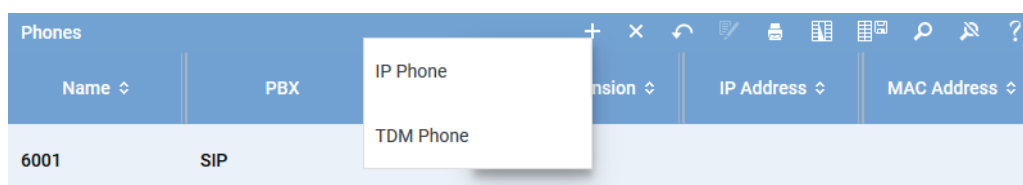


Fig. 521: Create phone

2. Select the menu item *IP Phone*.  
⇒ In the detail view, the tab *Details* appears.



× ...

< Details\*
>

Name\*

1234

PBX\*

Mitel

▼

PBX phone ID

Extension

1234

Computer name

Address for replay via phone

Display language

en\_US

▼

IP address

MAC address

**PHONEapp**
▼

Activate PHONEapp configuration

☒

Phone type

MITEL

▼

Recording LED identifier

topsoftkey3

Mute LED identifier

topsoftkey4

Keep LED identifier

topsoftkey5

Save

Reset

Fig. 522: Create phones - activate PHONEapp

The configuration parameters are closely correlated.

Parameter	Value/Description
<i>Name</i>	Enter the name of the phone.
<i>PBX</i>	From the drop-down list, select the PBX for which you would like to create the phone.
<i>PBX phone ID</i>	Here, you can enter the ID of the end device which is used in the PBX.
<i>Extension</i>	Enter the extension of the end device to be recorded.
<i>Address for replay via phone</i>	<p>Here, you can enter the address of the phone where the calls are supposed to be replayed. Depending on which agent logs in on this phone, the audio data that the participant is allowed to replay is provided.</p> <p>For further information about this function refer to the administration manual <i>Configuration Replay via phone</i>.</p>
<i>Display language</i>	Select the language for the display from the drop-down list.
<i>IP address</i>	Here, you can enter the IP address of the end device to be recorded.
<i>MAC address</i>	Here, you can enter the MAC address of the end device to be recorded.


Tab. 114: Add phone

### Group field PHONEapp

Parameter	Description
Activate PHONEapp configuration	<p>Activate the check box to use the functions of the PHONEapp.</p> <p>This function is only available if it has been activated previously in the following modules:</p> <ul style="list-style-type: none"> <li>• in the PBX module in the tab PHONEapp</li> <li>• and in the PHONEapp module</li> </ul>
Phone type	<p>Select the corresponding phone type from the drop-down list. The phone types are only displayed if the corresponding license for the PHONEapp has been installed and the PHONEapp has been activated in the PHONEapp module.</p>
Recording LED identifier	<p>Enter the softkey for the recording start.</p> <ul style="list-style-type: none"> <li>• For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey3</i>.</li> <li>• For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey3</i>.</li> </ul>
Mute LED identifier	<p>Enter the softkey for the mute function.</p> <ul style="list-style-type: none"> <li>• For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey4</i>.</li> <li>• For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey4</i>.</li> </ul>
Keep LED identifier	<p>Enter the softkey for the keep function.</p> <ul style="list-style-type: none"> <li>• For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey5</i>.</li> <li>• For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey5</i>.</li> </ul>

1. Click on the button *Save*.
2. Click on the button *Close* to finish this configuration step.
3. Repeat the steps for every end device.

#### 7.3.4.4.3 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.

#### 7.3.4.5 Configure Recording Planner module

The different operation modes of call recording are configured in the Recording Planner module of the application System Configuration.

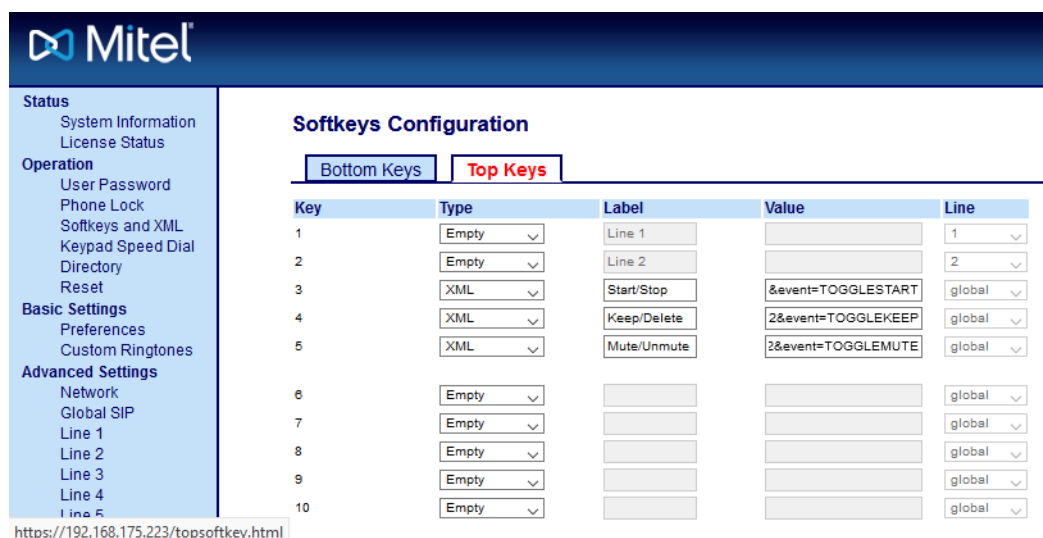


For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

### 7.3.4.6 Configure key functions on the Mitel phone

To be able to use the keys and the **LED** display on the phone, you must configure the key functions of every phone.

1. Call up the **URL** of the phone via the web interface.
2. Select the menu item *Operation > Softkeys and XML* in the navigation bar.



Key	Type	Label	Value	Line
1	Empty	Line 1		1
2	Empty	Line 2		2
3	XML	Start/Stop	&event=TOGGLESTART	global
4	XML	Keep/Delete	2&event=TOGGLEKEEP	global
5	XML	Mute/Unmute	2&event=TOGGMUTE	global
6	Empty			global
7	Empty			global
8	Empty			global
9	Empty			global
10	Empty			global

Fig. 523: Configure key function via the web interface

3. Click on the tab *Top Keys*.
4. Select the entry *XML* from the drop-down list.
5. In the entry field *Label*, enter the information that is supposed to be visible on the display.
6. In the entry field *Value*, enter the command which is supposed to be triggered when pressing the key:

**NOTICE!** The phone will replace the placeholder `$$$SIPUSERNAME$$` with the extension.

Start/Stop	http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGLESTART
Keep/Delete	http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGLEKEEP
Mute/Unmute	http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGMUTE

7. Click on the button *Save Settings* to apply the entries.

### Configure network settings

To enable the **LEDs**, the HTTPS network settings must be configured for each phone.

1. Select the menu item *Advanced Settings > Network*.

<b>Status</b> System Information License Status <b>Operation</b> User Password Phone Lock Softkeys and XML Keypad Speed Dial Directory Reset <b>Basic Settings</b> Preferences Custom Ringtones <b>Advanced Settings</b> Network Global SIP Line 1 Line 2 Line 3 Line 4 Line 5 Line 6 Line 7 Line 8 Line 9 Line 10 Line 11 Line 12 Line 13 Line 14 Line 15 Line 16 Line 17 Line 18 Line 19 Line 20 Line 21 Line 22 Line 23 Line 24 Action URI Configuration Server	<h3>Network Settings</h3> <div> <b>IPv6 Settings</b>          IPv6 <input type="checkbox"/> Enabled       </div> <div> <b>Basic Network Settings</b>          DHCP <input checked="" type="checkbox"/> Enabled          IP Address 192.168.175.223          Subnet Mask 255.255.240.0          Gateway 192.168.168.11          Primary DNS 192.168.168.11          Secondary DNS 0.0.0.0          Hostname 692008000FE15893          LAN Port Auto Negotiation          PC Port PassThru Enable/Disable <input checked="" type="checkbox"/> Enabled          PC Port Auto Negotiation       </div> <div> <b>Advanced Network Settings</b>          DHCP Download Option Any          LLDP <input type="checkbox"/> Enabled          LLDP packet interval 30          NAT IP 0.0.0.0          NAT SIP Port 51620          NAT RTP Port 51720          Rport (RFC 3581) <input type="checkbox"/> Enabled       </div> <div> <b>HTTPS Settings</b>          HTTPS Server - Redirect HTTP to HTTPS <input type="checkbox"/> Enabled          HTTPS Server - Block XML HTTP POSTs <input type="checkbox"/> Enabled          Client Method TLS 1.2          Validate Certificates <input type="checkbox"/> Enabled          Check Certificate Expiration <input checked="" type="checkbox"/> Enabled          Check Certificate Hostnames <input checked="" type="checkbox"/> Enabled          Trusted Certificates Filename       </div>
---	---

Fig. 524: Configure HTTPS settings

2. Deactivate the check box for the following parameters:

- HTTPS Server - Redirect HTTP to HTTPS
- HTTPS Server - Block XML HTTPS POSTs

### Configure IP address of the XML Push Server

To ensure that the events are executed completely, you must configure the IP address of the XML Push Server for the communication between the phone and the recording server.

1. Select the menu item *Advanced Settings > Configuration Server Settings* in the navigation bar.

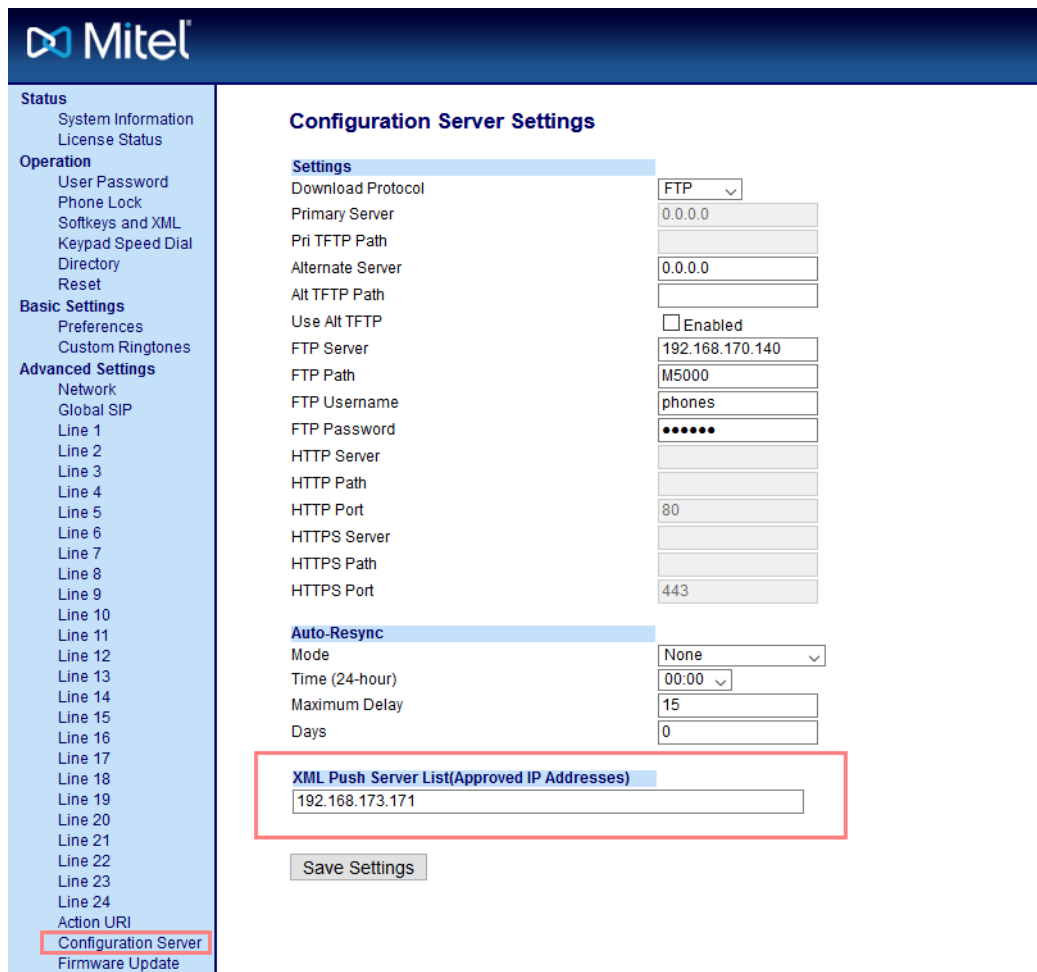


Fig. 525: Configure XML Push Server

2. In the section *XML Push Server List (Approved IP Addresses)*, enter the IP address of the recording server.
3. Click on the button *Save Settings* to apply the entries.
  - ⇒ In the display of the phone, the LED indicator shows the respective status.



Fig. 526: Assignment of the top keys and displayed status of the recording

### 7.3.5 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

### 7.3.5.1 Synchronization of recording control

#### Recording Control Services

For parallel recording servers installed in the same system architecture, you can configure synchronization of recording control.

#### ATTENTION!

Before the configuration, contact your ASC support to ensure that this function is suitable for your recording solution and to avoid a possible loss of recordings!

For information about which recording solutions support this function refer to the file *neo* Integration Overview.

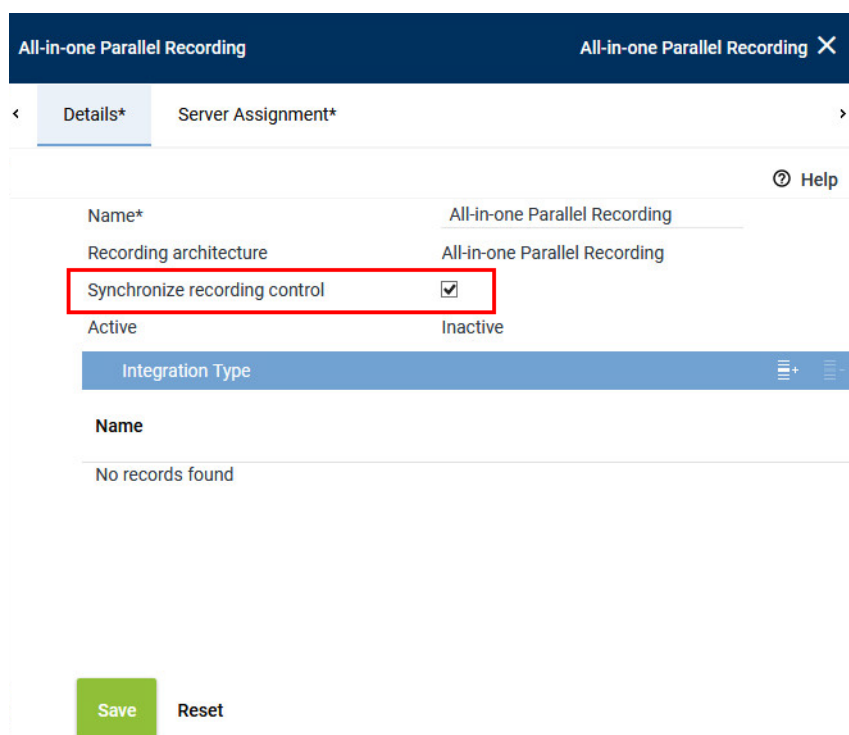
If recording is supposed to be controlled manually by means of applications such as *CLIENT-command*, *PHONEapp*, *SCREENrec* scan Editor, or by external control, synchronization of the Recording Control Services of the parallel recording servers must be created.

Initially, the 1st Recording Control Service is responsible for recording control. The Recording Control Service ensures that the conversations of both recording servers are recorded.

If the 1st Recording Control Service fails, the 2nd Recording Control Service takes over recording control for both recording servers each of which then records the conversations.

Synchronization of recording control is configured in the Recording Architectures module. In parallel recording architectures, the check box *Synchronize recording control* appears in the tab *Details*.

1. Activate the check box *Synchronize recording control* so that the Recording Control Services can be synchronized and only one service controls recording for the two recording servers.



The screenshot shows the configuration page for 'All-in-one Parallel Recording'. The 'Details\*' tab is active. The form contains the following fields:

- Name\*: All-in-one Parallel Recording
- Recording architecture: All-in-one Parallel Recording
- Synchronize recording control: ☒ (highlighted with a red box)
- Active: Inactive

Below the form is a table with the header 'Integration Type' and a 'Name' column. The table is currently empty, showing 'No records found'. At the bottom of the form are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 527: Synchronize recording control

2. To save the settings, click on the button *Save*.  
To discard the settings, click on the button *Reset*.



Synchronization of recording control brings stricter timeouts between the components. Observe the increased hardware and network requirements. Latency must be < 100 ms.

**If you activate or deactivate this synchronization option subsequently, you must repeat the following configuration steps for the changes to take effect:**

1. Select the required state of recording control:
  - ☒ = *Recording control is synchronized*
  - ☐ = *Recording control is not synchronized*
2. Deactivate the integration.
3. Deactivate the recording architecture.
4. Ensure that the following services have been stopped:
  - *ASC RecordingControl*
  - *ASC RecordingModule*
  - *ASC CTIconnect(integration name)*
5. Activate the recording architecture.

**WARNING! In this status, all services have received the updated configuration but states may be conflicting.**

**Therefore, repeat the following steps:**

6. Deactivate the recording architecture again.
  7. Ensure that the services have been stopped.
  8. Activate the recording architecture again.
  9. Activate the integration.
- ⇒ The changes are now active.

### 7.3.5.2 Synchronization of system storage

In recording architectures with 2 system storages, you can configure synchronization to compare recordings.

A synchronization configuration is always created for 2 system storages. All recordings which are saved on one system storage are also copied to the other one and vice versa. That way, all recordings always exist on both system storages.



In a multi-core architecture, the system storage must not be synchronized between the Enterprise Cores.

Synchronization of the system storages is configured in the Servers module.

1. To create a synchronization configuration, click on the menu item *Servers > Manage Synchronization Configuration* in the toolbar of the main view.



Fig. 528: Menu item Manage Synchronization Configurations

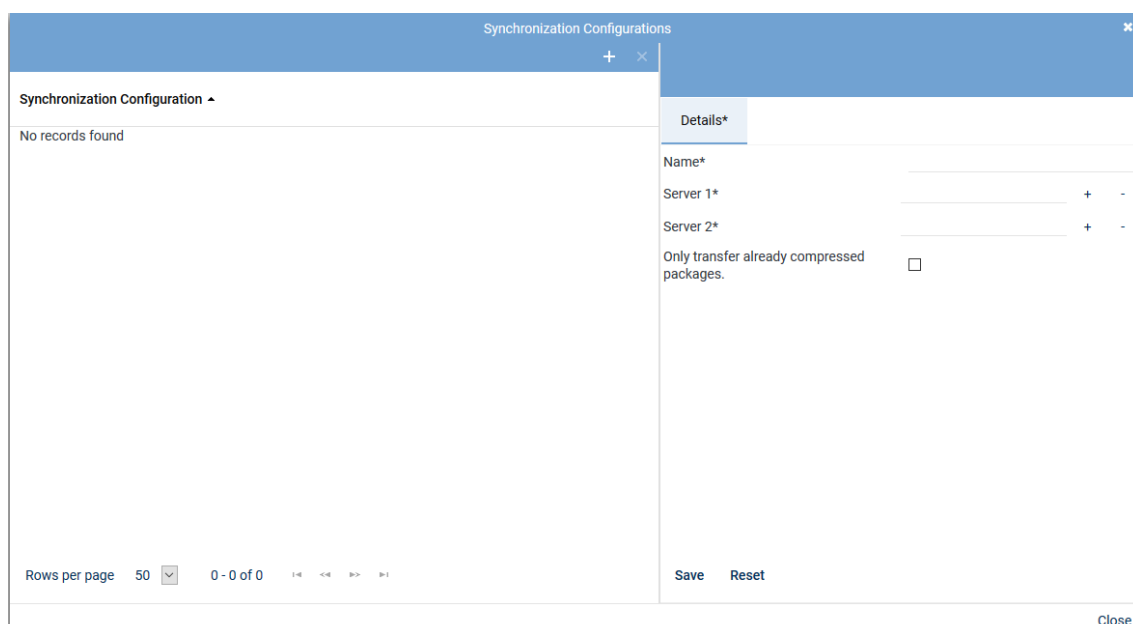




Fig. 529: Configure synchronization configurations

The following options are available:


	<b>Create</b>	Creates a new synchronization configuration, see <a href="#">chapter "Create synchronization configuration", p. 444</a> .
	<b>Delete</b>	Deletes the selected synchronization configuration, see <a href="#">chapter "Delete synchronization configuration", p. 445</a> .

A synchronization configuration becomes active upon saving it and remains active until deleted. During this time, both system storages are regularly checked for new content and synchronized.

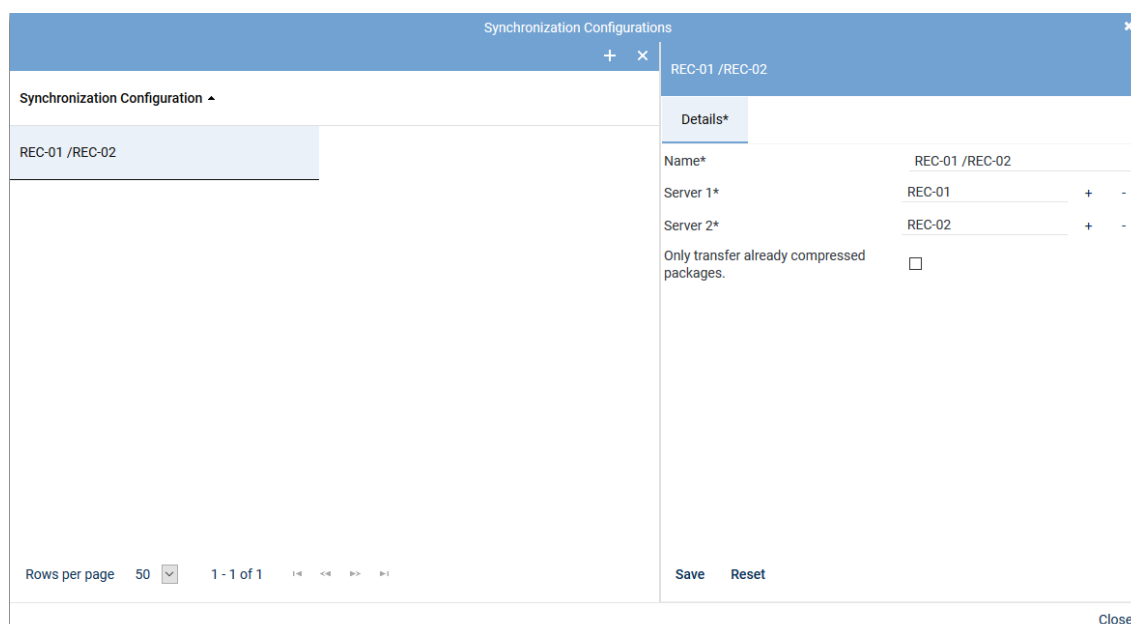


A server which is already used in a synchronization configuration cannot be used in another synchronization configuration.

#### 7.3.5.2.1 Create synchronization configuration

- In the window *Administrate Synchronization Configuration*, click on the icon  (*Create*).  
⇒ The tab *Details* becomes active.





Synchronization Configurations

REC-01 / REC-02

Synchronization Configuration

REC-01 / REC-02

Details\*

Name\* REC-01 / REC-02

Server 1\* REC-01 + -

Server 2\* REC-02 + -

Only transfer already compressed packages. ☐

Rows per page 50 1 - 1 of 1

Save Reset

Close


Fig. 530: Create synchronization configuration

- Complete all fields for the new synchronization configuration:

<b>Name</b>	Enter a name for the synchronization configuration.
<b>Server 1 / Server 2</b>	Click on the button <b>+</b> 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 <b>-</b> next to the respective entry field.
<b>Only transfer already compressed packages</b>	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. <b>NOTICE!</b> 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.

### 7.3.5.2.2 Delete synchronization configuration

- In the window *Administrate synchronization configurations*, select the synchronization configuration you would like to delete.
- Click on the icon  (**Delete**) in the toolbar of the window.
  - ⇒ The synchronization of the two entered system storages is finished.
  - ⇒ The selected synchronization configuration is deleted.

### 7.3.6 Duplicates in parallel recording architectures



In parallel recording architectures in which recording control is synchronized, no duplicates are created which could be deleted. Both recordings are merged in one package and thus cannot be deleted separately. Keep in mind that more storage space must thus be available for the recordings.

A parallel recording without synchronization results in redundant recording data in the system. To avoid that conversations are displayed twice in the replay applications (e. g. *POWERplay Web*) because the database contains them twice, you can delete duplicates so that only one of the double recordings remains.

Conversations with the following characteristics are considered identical:

- Identical start and end times

You can define an allowed difference for the start and end times so that the conversations are still considered duplicates despite a differing start or end time, see [chapter "Configure duplicate detection", p. 446](#).

The start and end times of complete conversations as well as the start and end times of the individual recordings belonging to a conversation are checked.

- Identical call participants
- Identical additional data

Duplicate detection is configured in the Integrations module. There, you can configure for each integration individually under which circumstances conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings, see [chapter "Configure duplicate detection", p. 446](#).

The shorter one of the two identical recordings is deleted. To calculate the total recording length, the recording lengths of all sections of a conversation are added. The additional data as well as the audio data of the duplicate are deleted. On which of the two recording servers a duplicate is deleted thus depends on the location where the shorter recording has been saved. If the recording length is the same, the recording which has been checked second is considered a duplicate and deleted.

Duplicate detection is executed regularly for all new recordings from the moment on it has been activated but not for past recordings. This means Recordings which already exist when duplicate detection is activated are not checked for duplicates.



For information about the status of a job refer to the Jobs module in the application System Monitoring, see user manual *Usage System Monitoring*.



If you would like to delete duplicates but nevertheless want that all conversations exist on both recording servers, you can create a synchronization configuration in the Servers module which synchronizes the system storages of the two recording servers.

### 7.3.6.1 Configure duplicate detection

In the Integrations module, you can configure for each integration separately under which circumstances 2 conversations are supposed to be considered identical. Upon selecting an architecture for an integration which is based on parallel recording, the tab *Parallel Recording* is displayed which allows adjusting the required settings.

1. In the main view of the Integrations module, select the integration for which you would like to configure duplicate detection.
2. Select the tab *Parallel Recording* in the detail view and adjust the following settings:

Details\*
Recording Content Validation
Parallel Recording

☒ Delete duplicates if the participants of the conversations are identical and the following criteria are met:  
The start times differ in a maximum of  Milliseconds  
\*  
The end times differ in a maximum of  Milliseconds  
\*  
Additional settings  
Time after which conversations are to be checked at the earliest \*  minutes  
Interval in which the check is to take place \*  minutes

Additional Data

ID ↕
Displayed Name

No records found



Criteria to be Ignored

Available attributes	Ignored attributes
CHATIDENTIFIER	
DISPLAYNAME	
EMAILADDRESS	
EMPLOYEEID	
EXTENSION	
IPADDRESS	
MACADDRESS	
PBXAGENTID	
PBXID	

Save
Reset

Fig. 531: Tab Parallel Recording (integration)

<i>Delete duplicates,....</i>	<p>When activating this option, you can define by means of the displayed criteria when 2 recordings are supposed to be identified as identical.</p> <p><input checked="" type="checkbox"/> = Duplicate detection has been activated. Duplicates are deleted according to the defined criteria.</p> <p><input type="checkbox"/> = Duplicate detection has been deactivated.</p>
<i>The start times differ in a maximum of</i>	<p>Enter the maximum difference with regards to the start time. The start times of complete conversations as well as the start times of the individual recordings belonging to a conversation are checked.</p> <p>Example: <i>1000 milliseconds</i></p> <p>If one conversation started at 2:20:15 PM and a second conversation started at 2:20:16 PM, and if the start times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their start time.</p>
<i>The end times differ in a maximum of</i>	<p>Enter the maximum difference with regards to the end time. The end times of complete conversations as well as the end times of the individual recording sections belonging to a conversation are checked.</p> <p>Example: <i>1000 milliseconds</i></p> <p>If one conversation ended at 2:20:15 PM and a second conversation ended at 2:20:16 PM, and if the end times of the individual recordings of those two conversations differ less than 1000 milliseconds, then these conversations are considered possible duplicates with regards to their end time.</p>

<i>Time after which conversations are to be checked at the earliest</i>	<p>Enter the time interval which is supposed to pass before a recording is checked for duplicates.</p> <p>Example: <i>3 minutes</i></p> <p>If one conversation ended at 2:20 PM, i. e. the recording has been saved at 2:20 PM, then the recording is not check for duplicates before 2:23 PM.</p>
<i>Interval in which the check is to take place</i>	<p>Select the intervals in which the job for duplicate detection is supposed to be executed.</p> <p>Example: <i>2 minutes</i></p> <p>The job for duplicate detection is started over again every 2 minutes to search for new recordings and possible duplicates and to delete duplicates.</p>
List <i>Additional Data</i>	<p>Add all additional data to the list which are supposed to be used as criteria. When searching for duplicates, only those recordings are considered which contain an additional data type from the list. If an additional data type is empty in both conversations, this is considered identical, too, and one of the conversations is deleted.</p> <p> = Add additional data to the list, see <a href="#">chapter "Map additional data", p. 448</a>.</p> <p> = Remove additional data from the list, see <a href="#">chapter "Delete additional data assignment", p. 449</a>.</p>

- To save the settings, click on the button **Save**.
- ⇒ Upon activating the option *Delete duplicates...* the recordings are checked for duplicates and the detected duplicates are deleted.

### 7.3.6.2 Additional data

#### 7.3.6.2.1 Map additional data

In addition to the start time and the end time, you can configure more additional data which is supposed to be used for checking for duplicates.

- In the list *Additional data*, click on the icon  (*Add*) to configure more additional data.

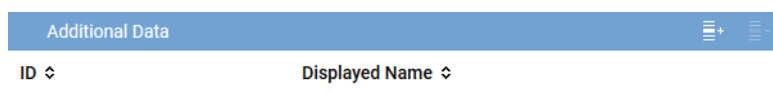


Fig. 532: Map additional data

- Select the respective additional data from the list which are supposed to be used additionally to check for duplicates.  
To select several entries or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Additional Data			
Displayed Name ↕	Available ↕	Editable ↕	External Recording Control ↕
Kommentar	✓	✓	✗
Universal Call ID	✓	✓	✗

Rows per page 20 1 - 2 of 2

Add Cancel

Fig. 533: Select additional data


**NOTICE!** The list contains only additional data which have been configured in the Additional Data module previously.



For information about the configuration of additional data refer to the administration manual for system providers *Additional Data module*

- To apply the selection, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.

#### 7.3.6.2.2 Delete additional data assignment

- Select the tab *Parallel Recording*.
- Select the additional data that you would like to remove in the list *Additional Data*.
- Click on the icon  (*Delete*).

Additional Data	
ID ↕	Displayed Name ↕
customCP01	Kommentar
customCP02	Universal Call ID

Fig. 534: Delete additional data assignment

#### 7.3.6.3 Criteria to be ignored

In this group field, you can exclude certain criteria for duplicate detection which may prevent conversations to be detected as duplicates.

If conversations differ in just one attribute, they are not considered as duplicates. This holds true for conversations with different PBX IDs, for example.

To exclude this criterion during duplicate detection, add the respective attribute to the list of attributes which are supposed to be ignored.

In the list of available attributes, you can select which attributes are supposed to be excluded during duplicate detection. Click on the respective attributes and drag and drop them in the list of attributes to be ignored.

### 7.3.7 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.



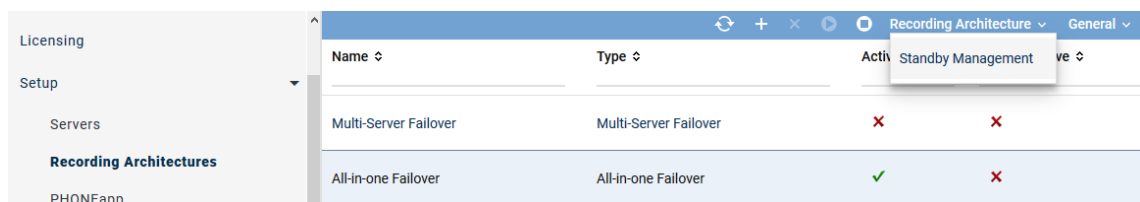
You can only edit the standby management if the corresponding architecture has been activated.

#### 7.3.7.1 Standby management for All-in-one Failover

For failover recording architectures, the menu *Recording Architectures* appears in the toolbar of the main view. If you have installed the required redundancy options on different servers, you can switch from primary to standby server and vice versa by clicking on the menu item *Standby Management*.

The menu item *Standby Management* is only active if the selected recording architecture has been activated.

1. In the main view, select the recording architecture the standby management of which you would like to call up.
2. Click on the menu *Recording Architectures* in the toolbar of the main view.
  - ⇒ If the selected recording architecture has been activated, the menu item *Standby Management* is active.



			Recording Architecture ▾		General ▾	
Name ↕	Type ↕	Active	Standby Management	ve ↕		
Multi-Server Failover	Multi-Server Failover	✗	✗			
All-in-one Failover	All-in-one Failover	✓	✗			

Fig. 535: 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. 536: 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.

### 7.3.7.2 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.

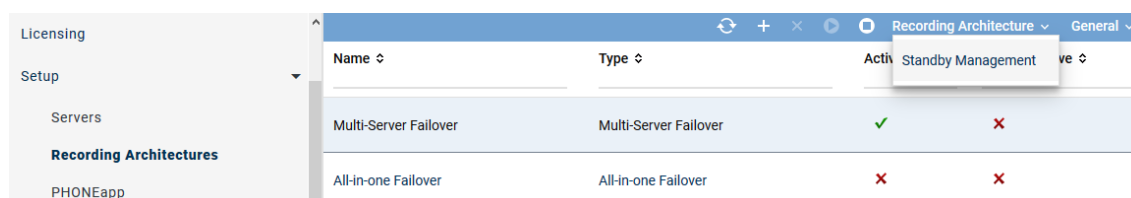


Fig. 537: Menu of the standby management

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. 538: 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.

#### 7.3.8 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.

### 7.3.9 Import InAttend conversation to neo

#### Supported import formats

##### WAVE / MP3 + CSV

This import format allows you to import recordings which have been created by a third-party system. Audio data must be available either in [WAVE](#) format or in [MP3](#) 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.

##### WAVE / MP3 + XML

This import format allows you to import recordings which have been created by a third-party system. Audio data must be available either in [WAVE](#) format or in [MP3](#) format.

If the required additional data is contained in the file name, 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.

#### 7.3.9.1 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*.

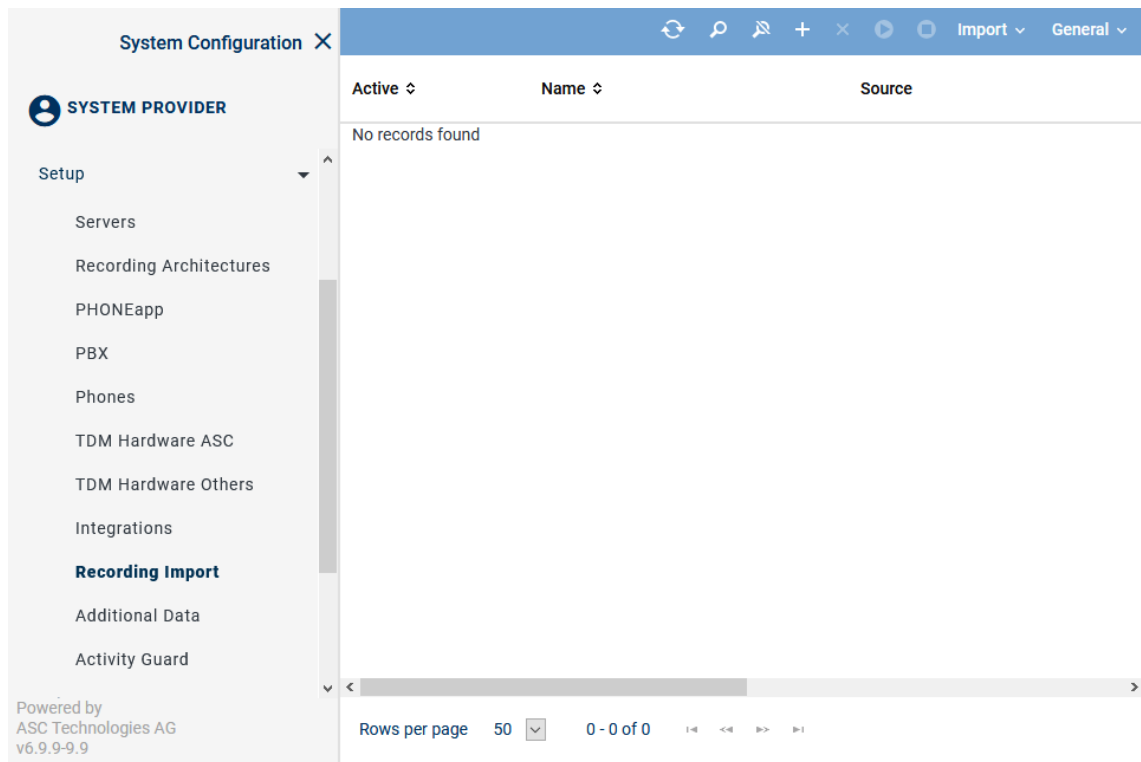



Fig. 539: Main view

4. 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.

## 7.3.9.1.1 Tab Details

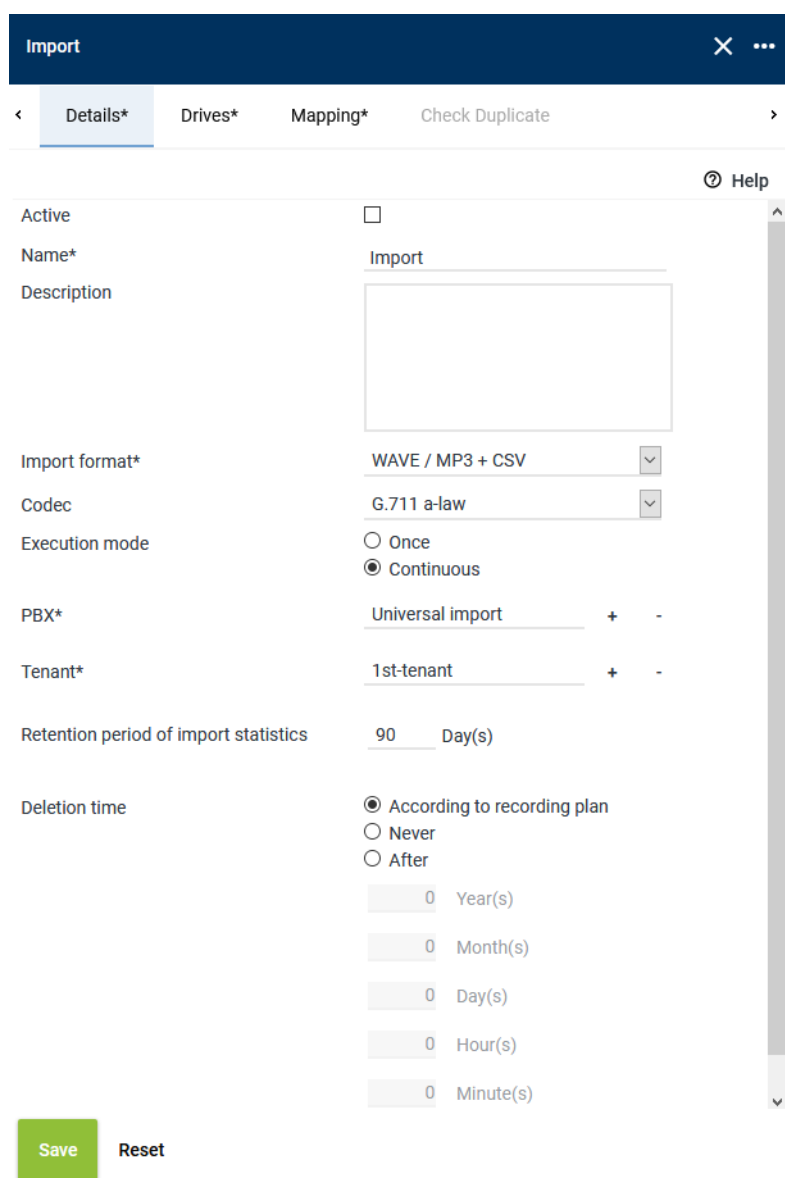





Fig. 540: Tab Details (example)

<b>Active</b>	<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>
<b>Name</b>	Enter the name for the import job.
<b>Description</b>	Here, you can enter a description of the import job.
<b>Import format</b>	<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"> <li>• WAVE / MP3 + CSV</li> <li>• WAVE / MP3 + XML</li> </ul>
<b>Codec</b>	Select the <a href="#">codec</a> from the drop-down list in which the recordings are supposed to be saved.

	<p>The following codecs are supported:</p> <ul style="list-style-type: none"> <li>• G.711 <a href="#">A-law</a></li> <li>• G.711 <a href="#">μ-law</a></li> <li>• G.729a</li> <li>• Linear <a href="#">PCM</a> 8 bit</li> </ul>
<i>Execution mode</i>	<p>Select whether the import is supposed to be executed once or continuously.</p> <ul style="list-style-type: none"> <li>• <i>Once</i> The import is started upon activating the import configuration. The source directory is checked for data only once.</li> <li>• <i>Continuous</i> 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.</li> </ul> <p><b>NOTICE!</b> 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 <a href="#">PBX</a> the data is supposed to be imported, see <a href="#">chapter "Assign PBX", p. 457</a>.</p> <p>It is necessary to map the imported data to a <a href="#">PBX</a> so that the extensions can be mapped. For a mere import, you can either select a configured Mitel <a href="#">PBX</a> or a <a href="#">PBX</a> of the type <i>Universal Import</i>. The <a href="#">PBX</a> 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 <a href="#">chapter "Assign tenant", p. 458</a>.</p> <p><b>NOTICE!</b> In a 1-tenant system, the tenant is entered here automatically. The setting cannot be changed.</p>
<i>Retention period of import statistics</i>	<p>Enter the retention period for the import statistics. With this information, you can generate a report about the imports of recordings. The entries apply from the time of the import.</p>
<i>Deletion time</i>	<p>Select the conditions for deletion by activating the corresponding radio buttons.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>Check recording plan</i> The imported data is deleted based on the configuration in the Recording Planner.</li> <li>• <i>Never</i> The imported data is never deleted.</li> <li>• <i>After</i> The imported data is deleted after the time configured here. Enter the corresponding time.</li> </ul>

### Assign PBX

1. Click on the button  on the right of the entry field.
2. Select a [PBX](#) from the list.

PBX

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

1 - 20 of 21

<<

>>

Add

Cancel

Fig. 541: 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.

Tenant

Tenant

Type

System	System provider
1st-Tenant	Tenant
3rd-Tenant	Tenant
2nd-Tenant	Tenant

Add

Cancel

Fig. 542: Add tenant

- To apply the selection, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.

#### 7.3.9.1.2 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.

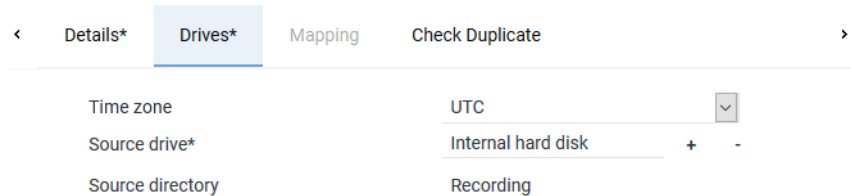
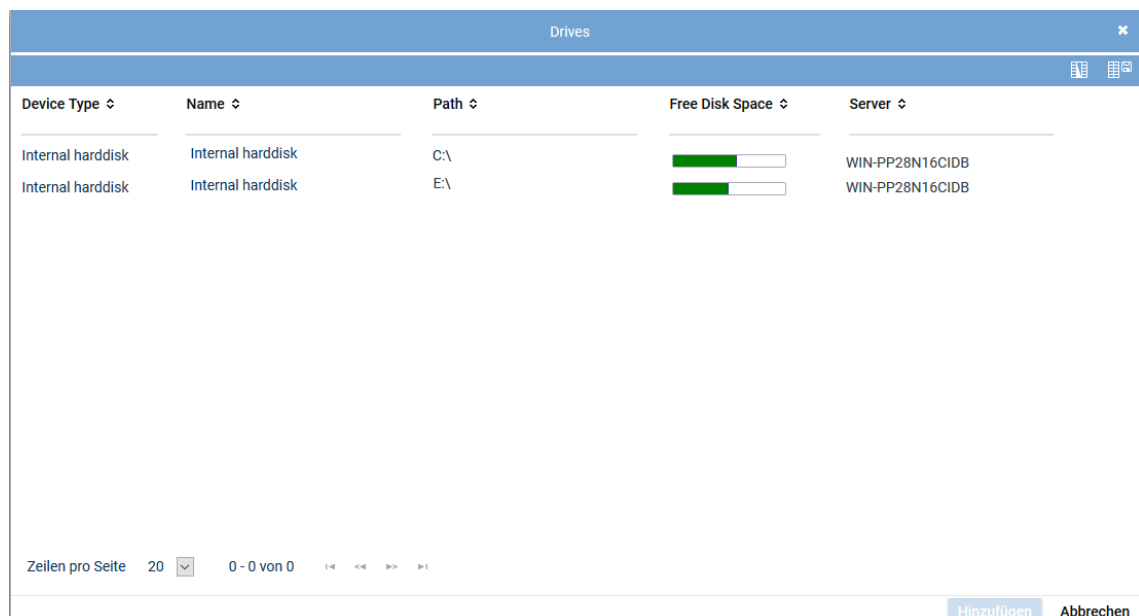


Fig. 543: Tab Drives - [WAVE](#) / [MP3](#) formats

<i>Time zone</i>	Select the time zone from the drop-down list that the time indicated in the data to be imported refers to.
<i>Source drive</i>	Select the drive from which the data is supposed to be imported, see <a href="#">chapter "Assign drive", p. 459</a> .
<i>Source directory</i>	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.



Device Type	Name	Path	Free Disk Space	Server
Internal harddisk	Internal harddisk	C:\	<div style="width: 100%;"></div>	WIN-PP28N16CIDB
Internal harddisk	Internal harddisk	E:\	<div style="width: 100%;"></div>	WIN-PP28N16CIDB

Fig. 544: 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**.

#### 7.3.9.1.3 Tab Mapping with CSV file

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:

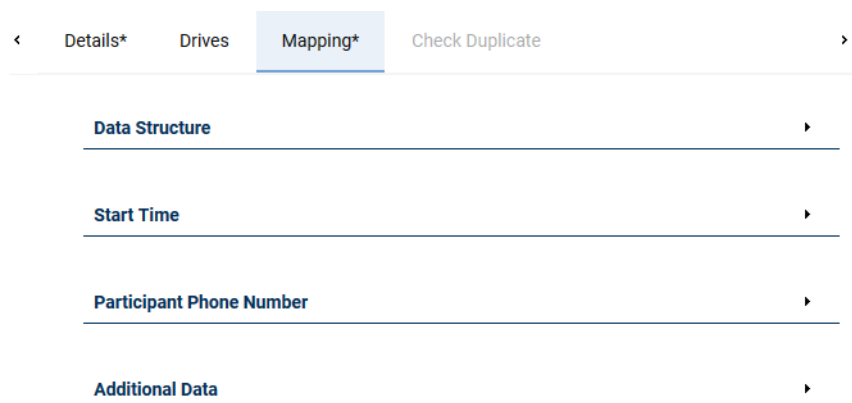


Fig. 545: Tab Mapping for *WAVE* / *MP3* import formats

The additional data can either be extracted from the file name of the *WAVE* or *MP3* file or from the file content of the delivered *CSV* or *XML* file.

The file names of associated files (*WAVE* / *MP3* and *XML* file or *WAVE* / *MP3* and *CSV* file) must 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* or *MP3* file.

### Group field Data Structure

Enter the format of the file name so that information can be read out.

The file name consists of information sections which are separated by a certain delimiter.

A new section begins at the beginning of the file name and after a delimiter. Every section ends with a delimiter as well as with the period in front of the file extension.

Example:

The file name "2019-11-06\_10-44-46\_Shruthiv\_9002\_61.wav" consists of 5 sections separated from each other by an underscore.

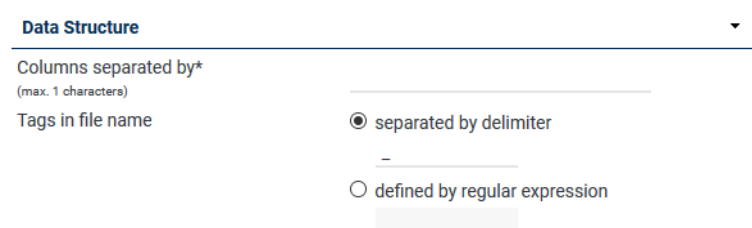


Fig. 546: Group field Data Structure

In this case, select the option *separated by delimiter* and enter an underscore in the entry field as delimiter.

**NOTICE!** Digits and letters are not recognized as delimiters.



## 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 WAVE / MP3 + CSV

Start Time	Start Time
Source <span>File name</span>	Source <span>File content</span>
<input type="radio"/> Date and time in same section Section no.* <input type="text"/> Format* <input type="text"/>	<input checked="" type="radio"/> Date and time in the same column Column* <span>Starttime</span> Format* <span>yy-MM-dd-hh-mm-ss</span>
<input checked="" type="radio"/> Date and time in separate sections Section no. for date* <input type="text"/> Format* <span>yyyy-MM-dd</span> Section no. for time* <input type="text"/> Format* <span>hh-mm-ss</span>	<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. 547: Group field Start time - Import format WAVE / MP3 + 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 Group field Data Structure.
  - 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 WAVE / MP3 + XML

Start Time	Start Time
Source <span>File content</span>	Source <span>File name</span>
<input checked="" type="radio"/> Date and time in the same XML tag XML tag* <span>Recording/Starttime</span> Format* <span>yy-MM-dd-hh-mm-ss</span>	<input type="radio"/> Date and time in same section Section no.* <input type="text"/> 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"/> Format* <span>yyyy-MM-dd</span> Section no. for time* <input type="text"/> Format* <span>hh-mm-ss</span>

Fig. 548: Group field Start time - Import format WAVE / MP3 + XML

- 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 Group field Data Structure.
  - 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 ☐ Mix stereo to mono

Several phone numbers in a column separated by \_\_\_\_\_  
(max. 1 character)

Source	Section No./Column	Track
File name	4	left
File name	5	left

[New](#) [Edit](#) [Delete](#)

Fig. 549: Group field Participant phone number (example)

<i>Handling stereo recordings</i>	This option is not relevant for InAttend conversation, as <a href="#">WAVE</a> files are available in mono only.
<i>Several phone numbers in a column separated by</i>	This option is not relevant, as the information is read out from the <a href="#">WAVE</a> files name.

### List

The list shows all import configuration rules that have been saved to be able to map the participant phone numbers.

<i>Source</i>	Shows whether the information is read out of the file name or out of the file content.
<i>Section No./XML Tag or Section no./Column</i>	Shows from which information section the information is read out. <b>NOTICE!</b> The column title depends on the import format.
<i>Track</i>	Selecting a track is not relevant for InAttend conversations, as the import files are available in mono.

Tab. 115: Mapping rules for participant phone numbers

<i>New</i>	The button opens a window in which you can create a new entry. See <a href="#">chapter "Configure source for participant phone numbers", p. 463.</a>
<i>Edit</i>	The button opens a window in which you can edit a selected entry. See <a href="#">chapter "Configure source for participant phone numbers", p. 463.</a>
<i>Delete</i>	The button deletes the selected entry from the list.

Tab. 116: 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.

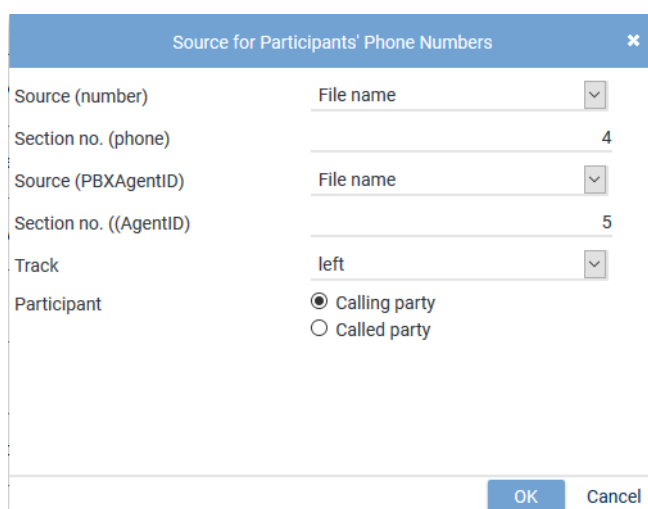


Fig. 550: Edit source for participant phone number (example)

<i>Source</i>	From the drop-down list, select the file name 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. <b>NOTICE!</b> 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.

2. Click on the button *OK* to apply the configuration and close the window.

### Configure source for additional data

1. 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.

2. In the group field *Additional Data*, click on the button *New* or *Edit*.

⇒ The following window appears:

Source for Additional Data

Source

File name

Section no.\*

3

Additional data\*

customCP01

OK

Cancel

Fig. 551: Edit source for additional data (example for WAVE import format)

Source	From the drop-down list, select the <i>file name</i> as the source for the additional data.
XML Tag or Column Name or Section No.	Enter the number of the file name section that contains the information. <b>NOTICE!</b> The name of the entry field depends on the source and the import format.
Additional data	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.

### 7.3.9.2 Replaying conversations in POWERplay Web

- Log in to the application *POWERplay Web* as administrator of the tenant to replay conversations.
- Select the menu item *Recording View* in the navigation bar.

Loaded

Section ID

Start Time

End Time

5489e9bc-e9e5-47fa-a0f8-4dae3ba74233	11/05/2019 10:44:46 AM	11/05/2019 10:45:03 AM
5489e9bc-e9e5-47fa-a0f8-4dae3ba74233	11/05/2019 10:44:46 AM	11/05/2019 10:45:03 AM

Rows per page: 50

1 - 2 of 2

Last filtered on 02/20/2020 12:23:58 PM; Number of records: 2

Recording View

Details

Participants

Additional Data

Start time

11/05/2019 10:44:46 AM

End time

11/05/2019 10:45:03 AM

Duration

00:00:17:480

Active participant name

Device name

Deletion time

12/31/9999 12:00:00 AM

Statistics of the Conversation

Number of connected sections

1

Duration of connected sections

00:00:17:480

Number of failed callbacks

0

Number of successful callbacks

0

Conversation ID of callback request

Calling Party Information

Save

Reset

Fig. 552: 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*.

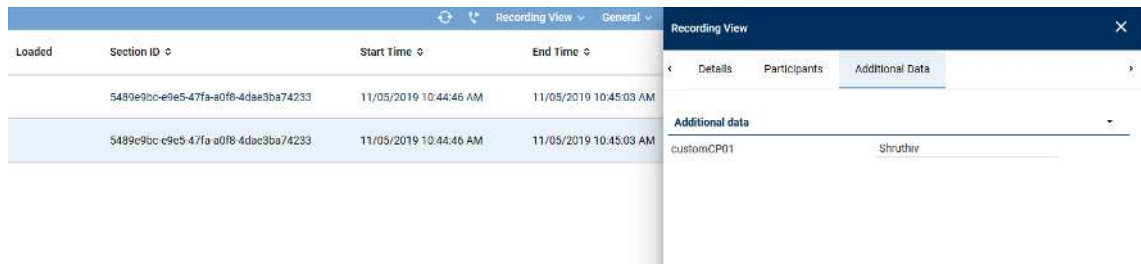


Fig. 553: Recording View - tab Additional Data

⇒ 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.

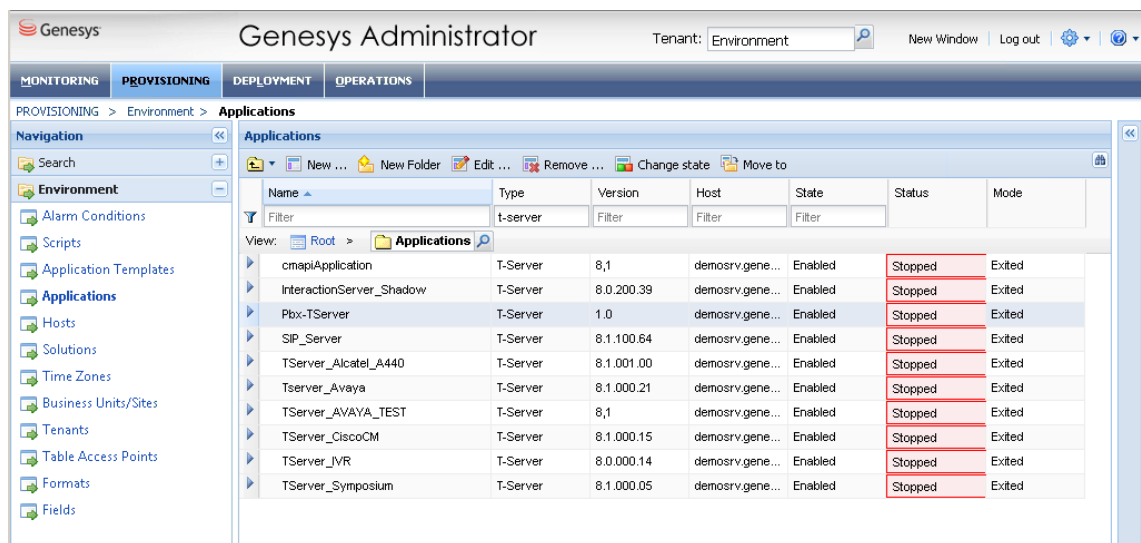


Fig. 554: Genesys Administrator - select T-Server

3. Double-click on the entry T-Server which has been connected to the switch instance to be monitored.
 

⇒ The window *Configuration* appears.
4. Expand the area *Server Info*.

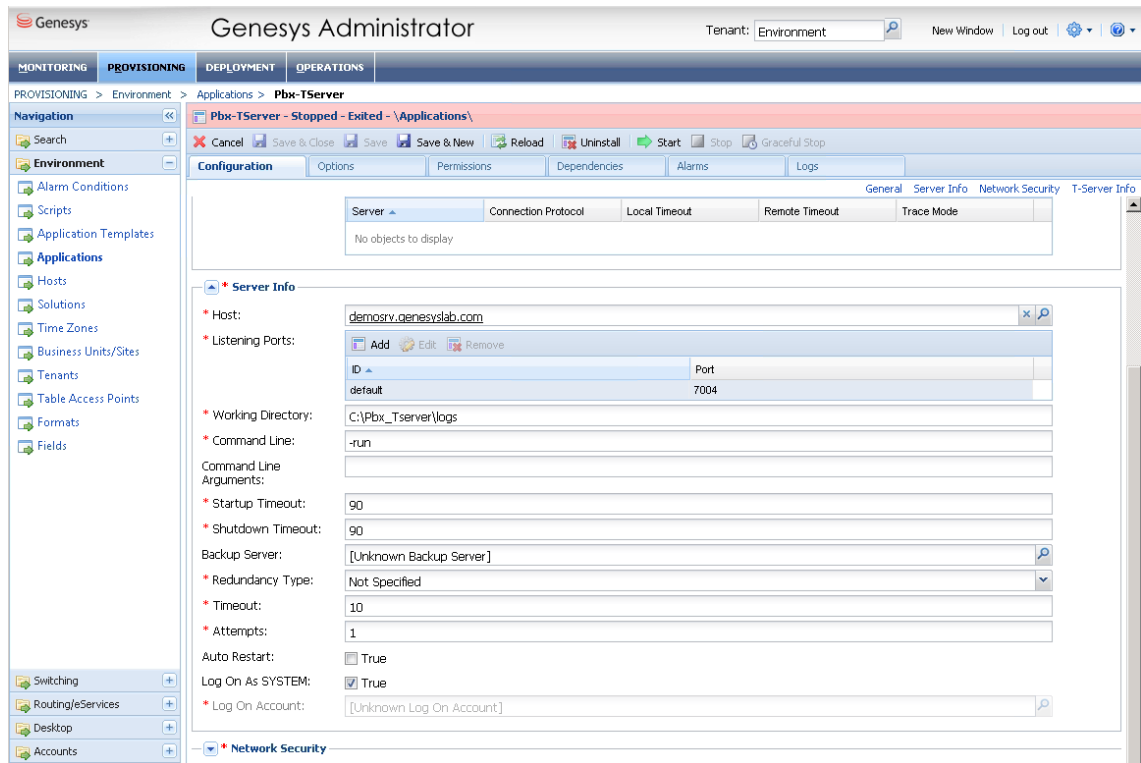


Fig. 555: Genesys Administrator - configure T-Server

5. In the field *Host*, enter the IP address or the computer name of the T-Server, e. g. *demosrv8.genesyslab.com*.
6. 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

1. Click on the menu item *Environment > Applications* in the navigation bar.

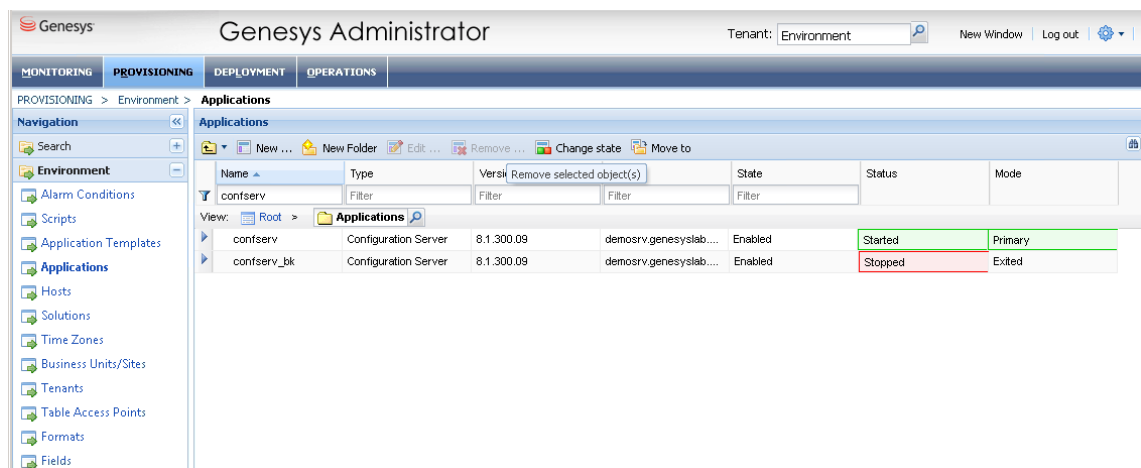


Fig. 556: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.  
⇒ The window *Configuration* appears.
3. Expand the area *Server Info*.

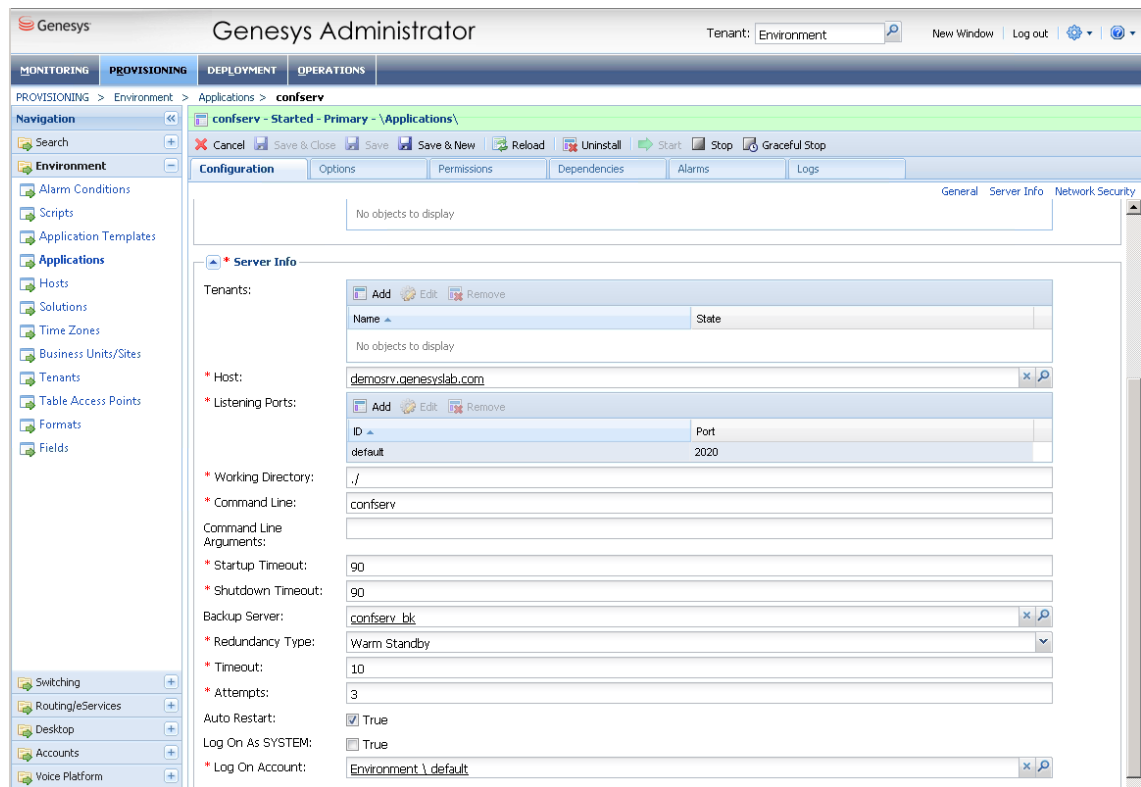


Fig. 557: Genesys Administrator - configure configuration server

4. In the field *Host*, enter the IP address or the computer name of the configuration server, e. g. *demosrv8.genesyslab.com*.
5. In the field *Listening Port*, enter the port of the configuration server, e. g. *2020*.

#### 7.4.1.3 Configure switch instance in the Genesys Configuration Server

1. Click on the menu item *Switching > Switches* in the navigation bar.

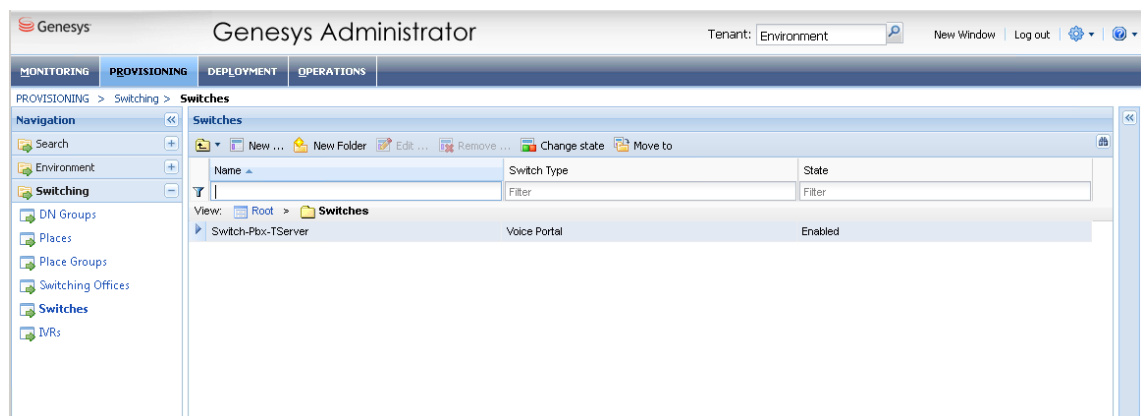
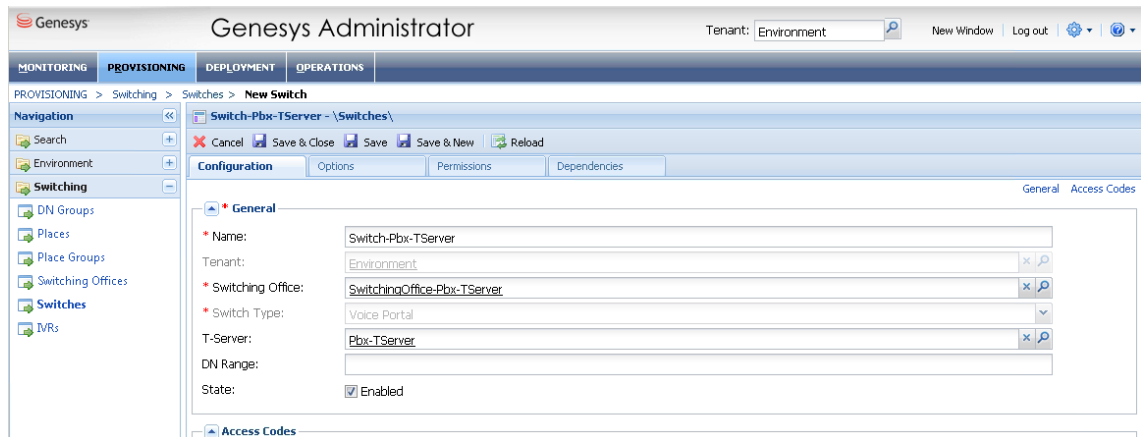


Fig. 558: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.  
⇒ The window *Configuration > General* appears.



The screenshot shows the Genesys Administrator web interface. The top navigation bar includes tabs for MONITORING, PROVISIONING, DEPLOYMENT, and OPERATIONS. The left sidebar shows a tree view with categories like Environment, Switching, and IVRs. The main content area is titled 'Switch-Pbx-TServer - \Switches\' and contains a 'Configuration' tab. The 'General' sub-tab is active, displaying fields for Name (Switch-Pbx-TServer), Tenant (Environment), Switching Office (SwitchingOffice-Pbx-TServer), Switch Type (Voice Portal), T-Server (Pbx-TServer), DN Range, and State (Enabled). Buttons for Cancel, Save & Close, Save, Save & New, and Reload are visible at the top of the configuration area.

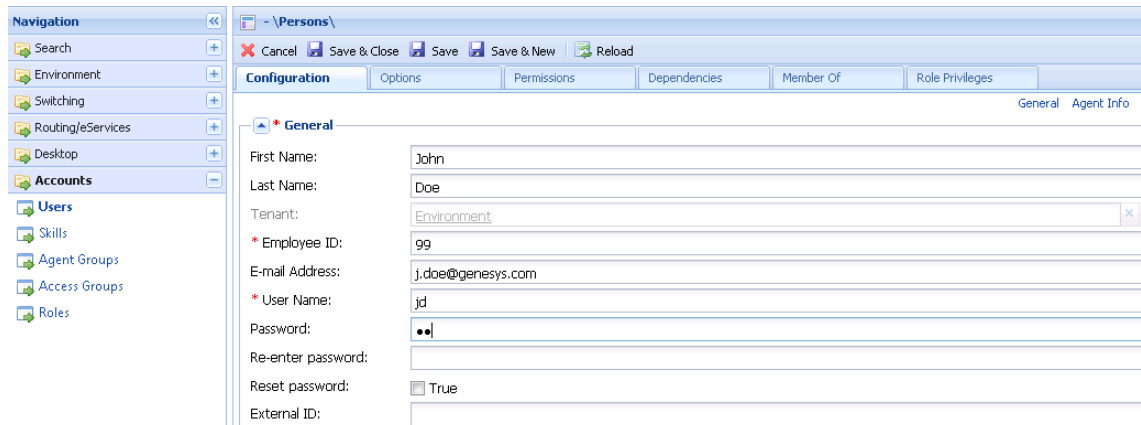
Fig. 559: Genesys Administrator - configure switch instance

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.



The screenshot shows the Genesys Administrator web interface with the 'Accounts' section selected in the left sidebar. The main content area is titled '- \Persons\' and contains a 'Configuration' tab. The 'General' sub-tab is active, displaying fields for First Name (John), Last Name (Doe), Tenant (Environment), Employee ID (99), E-mail Address (j.doe@genesys.com), User Name (jd), Password (masked with dots), Re-enter password, Reset password (checkbox), and External ID. Buttons for Cancel, Save & Close, Save, Save & New, and Reload are visible at the top of the configuration area.

Fig. 560: 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 VoIP end devices without MBG .....	6
Fig. 2	Recording solution with MBG .....	7
Fig. 3	Recording solution with intrusion .....	8
Fig. 4	Configure CSTA server .....	14
Fig. 5	Configure CSTA server .....	15
Fig. 6	Configure CSTA server .....	16
Fig. 7	Configure free-line signal for extension.....	17
Fig. 8	Check set monitor points.....	18
Fig. 9	Check license status .....	18
Fig. 10	Check server, path and port.....	19
Fig. 11	Check IP address and transport protocol.....	20
Fig. 12	Activate MBG for Call Recording .....	21
Fig. 13	Add MBG ICPs.....	21
Fig. 14	Configure MBG ICP .....	22
Fig. 15	Add MiNET devices.....	22
Fig. 16	Add MiNET devices.....	23
Fig. 17	Login screen MBG .....	23
Fig. 18	Certificate Management .....	24
Fig. 19	Confirm selected certificate.....	24
Fig. 20	Success notification for shared certificate .....	25
Fig. 21	System Configuration - web interface .....	26
Fig. 22	System Configuration - main view:.....	26
Fig. 23	Recording architectures - main view .....	27
Fig. 24	Toolbar Recording Architectures module.....	28
Fig. 25	Create recording architecture - All-in-one Basic Recording .....	29
Fig. 26	Recording architecture - tab Details.....	29
Fig. 27	Select integration type.....	30
Fig. 28	Recording architecture - tab Server Assignment .....	31
Fig. 29	Recording architecture - assign server .....	31
Fig. 30	Recording architecture - activate recording variant.....	32
Fig. 31	Recording architecture - activate recording architecture.....	32
Fig. 32	Servers - main view.....	33
Fig. 33	Toolbar Servers module.....	33
Fig. 34	Add server locations.....	34
Fig. 35	Delete server location .....	35
Fig. 36	Servers - tab Details.....	36
Fig. 37	Servers - tab usage.....	36
Fig. 38	Group field API Server .....	37
Fig. 39	Select storage expansion.....	38
Fig. 40	Group field Audio Analysis .....	39
Fig. 41	Select server for emotion detection.....	39

Fig. 42	Group field Recording Control/Key Management .....	39
Fig. 43	Group field Data Processing .....	40
Fig. 44	Select server .....	42
Fig. 45	Group field Replay .....	43
Fig. 46	Select server .....	44
Fig. 47	Group field Virtualization .....	45
Fig. 48	Servers module - tab Media Streamer .....	46
Fig. 49	Servers Module - tab Replay Server Address Mapping .....	48
Fig. 50	Servers module - tab Key Management.....	49
Fig. 51	Servers module - tab Keystore/Virtualization .....	51
Fig. 52	PBX module - main view .....	52
Fig. 53	Toolbar PBX module .....	52
Fig. 54	Create new PBX - tab Details .....	53
Fig. 55	Tenants - main view - tab Extensions .....	54
Fig. 56	Assign extensions to tenants .....	55
Fig. 57	Remove extensions.....	56
Fig. 58	Select extensions .....	57
Fig. 59	Tenants - main view - tab PBX Agent ID.....	58
Fig. 60	Assign PBX Agent IDs to tenants.....	58
Fig. 61	Select PBX Agent IDs .....	60
Fig. 62	Additional Data module main view .....	60
Fig. 63	Configure additional data .....	61
Fig. 64	Additional data - configure availability .....	61
Fig. 65	Integrations - main view .....	62
Fig. 66	Toolbar Integrations module .....	62
Fig. 67	Choose file .....	63
Fig. 68	Upload grammar .....	63
Fig. 69	Create integration type.....	64
Fig. 70	Integrations - select PBX.....	64
Fig. 71	Assign recording architecture - All-in-one Basic .....	65
Fig. 72	Configuration steps of the integration .....	65
Fig. 73	Configuration step - Configure Recording Architecture.....	66
Fig. 74	CTI connection data - tab MiVoice MX-ONE (CSTA).....	67
Fig. 75	Configure CTIconnect module .....	67
Fig. 76	Configure connection data .....	68
Fig. 77	Configure connection data .....	68
Fig. 78	Arbitrary assignment of the additional data.....	69
Fig. 79	Configure switching conditions.....	70
Fig. 80	Configure regular expression for phone type identification .....	71
Fig. 81	Activate CTIconnect connection data for MBG .....	72
Fig. 82	Configure CTIconnect module .....	72
Fig. 83	Group field Connection Data.....	73

Fig. 84	Configure connection .....	73
Fig. 85	CTI connection data - additional data module 1.....	74
Fig. 86	Configuration step - configure monitor points .....	74
Fig. 87	Add extension monitor points.....	75
Fig. 88	Configured extension monitor points.....	76
Fig. 89	Configuration step - Global Recording Settings .....	78
Fig. 90	Configuration step - Configure recording servers .....	79
Fig. 91	Configure add-on for MiContact Center Enterprise.....	81
Fig. 92	Arbitrary assignment of the additional data.....	82
Fig. 93	Overview of the add on of Genesys T-Server .....	84
Fig. 94	Configure add-on for Genesys T-Server .....	85
Fig. 95	Configure connection data .....	86
Fig. 96	Arbitrary assignment of the additional data.....	88
Fig. 97	Configure miscellaneous settings .....	88
Fig. 98	Activate integration.....	89
Fig. 99	Activated integration.....	89
Fig. 100	Deactivate integration .....	90
Fig. 101	Recording architectures - main view .....	91
Fig. 102	Toolbar Recording Architectures module.....	91
Fig. 103	Create recording architecture - All-in-one Failover .....	92
Fig. 104	Recording architecture - tab Details - All-in-one Failover.....	93
Fig. 105	Select integration type.....	94
Fig. 106	Recording Architecture - tab Server Assignment.....	95
Fig. 107	Recording Architecture - assign server - example .....	95
Fig. 108	Recording Architecture - activate recording type .....	96
Fig. 109	Recording architecture - activate recording architecture.....	96
Fig. 110	Servers - main view.....	97
Fig. 111	Toolbar Servers module.....	97
Fig. 112	Add server locations.....	99
Fig. 113	Delete server location .....	100
Fig. 114	Servers - tab Details.....	100
Fig. 115	Servers - tab usage .....	101
Fig. 116	Group field API Server .....	101
Fig. 117	Select storage expansion.....	103
Fig. 118	Group field Audio Analysis .....	103
Fig. 119	Select server for emotion detection.....	104
Fig. 120	Group field Recording Control/Key Management .....	104
Fig. 121	Group field Data Processing .....	105
Fig. 122	Select server .....	107
Fig. 123	Group field Replay .....	107
Fig. 124	Select server .....	109
Fig. 125	Group field Virtualization .....	109

Fig. 126 Servers module - tab Media Streamer .....	110
Fig. 127 Servers Module - tab Replay Server Address Mapping .....	112
Fig. 128 Servers module - tab Key Management.....	113
Fig. 129 Servers module - tab Keystore/Virtualization .....	115
Fig. 130 PBX module - main view .....	116
Fig. 131 Toolbar PBX module .....	116
Fig. 132 Create new PBX - tab Details .....	118
Fig. 133 Tenants - main view - tab Extensions .....	119
Fig. 134 Assign extensions to tenants .....	120
Fig. 135 Remove extensions.....	121
Fig. 136 Select extensions .....	122
Fig. 137 Tenants - main view - tab PBX Agent ID.....	123
Fig. 138 Assign PBX Agent IDs to tenants.....	123
Fig. 139 Select PBX Agent IDs .....	125
Fig. 140 Additional Data module main view .....	125
Fig. 141 Configure additional data .....	126
Fig. 142 Additional data - configure availability .....	126
Fig. 143 Integrations - main view .....	127
Fig. 144 Toolbar Integrations module .....	127
Fig. 145 Choose file .....	128
Fig. 146 Upload grammar .....	128
Fig. 147 Create integration type.....	129
Fig. 148 Integrations - select PBX.....	129
Fig. 149 Assign recording architecture - All-in-one Failover .....	130
Fig. 150 Configuration steps of the integration .....	130
Fig. 151 Configuration step - Configure Recording Architecture.....	131
Fig. 152 CTI connection data - tab MiVoice MX-ONE (CSTA).....	132
Fig. 153 Configure CTIconnect module .....	132
Fig. 154 Configure connection data .....	133
Fig. 155 Configure connection data .....	133
Fig. 156 Arbitrary assignment of the additional data.....	134
Fig. 157 Configure switching conditions.....	135
Fig. 158 Configure regular expression for phone type identification .....	136
Fig. 159 Activate CTIconnect connection data for MBG .....	137
Fig. 160 Configure CTIconnect module .....	137
Fig. 161 Group field Connection Data.....	138
Fig. 162 Configure connection .....	138
Fig. 163 CTI connection data - additional data module 1.....	139
Fig. 164 Configuration step - configure monitor points .....	139
Fig. 165 Add extension monitor points.....	140
Fig. 166 Configured extension monitor points.....	141
Fig. 167 Configuration step - Global Recording Settings .....	142

Fig. 168	Configuration step - Configure recording servers .....	144
Fig. 169	Tab Extensions .....	145
Fig. 170	Add extensions.....	145
Fig. 171	Added extensions.....	146
Fig. 172	Configuration step - Configure recording servers .....	146
Fig. 173	Tab Extensions .....	147
Fig. 174	Add extensions.....	148
Fig. 175	Added extensions.....	148
Fig. 176	Configure add-on for MiContact Center Enterprise.....	150
Fig. 177	Arbitrary assignment of the additional data.....	151
Fig. 178	Overview of the add on of Genesys T-Server .....	153
Fig. 179	Configure add-on for Genesys T-Server .....	154
Fig. 180	Configure connection data .....	155
Fig. 181	Arbitrary assignment of the additional data.....	157
Fig. 182	Configure miscellaneous settings .....	157
Fig. 183	Activate integration.....	158
Fig. 184	Activated integration.....	158
Fig. 185	Deactivate integration .....	159
Fig. 186	Recording architectures - main view .....	160
Fig. 187	Toolbar Recording Architectures module.....	160
Fig. 188	Create recording architecture - All-in-one Parallel Recording.....	161
Fig. 189	Recording architecture - tab Details - All-in-one Parallel Recording .....	162
Fig. 190	Select integration type.....	163
Fig. 191	Recording Architecture - tab Server Assignment.....	164
Fig. 192	Recording Architecture - assign server - example .....	164
Fig. 193	Recording Architecture - activate recording type .....	165
Fig. 194	Activate recording architecture.....	165
Fig. 195	Servers - main view.....	166
Fig. 196	Toolbar Servers module.....	166
Fig. 197	Add server locations.....	168
Fig. 198	Delete server location .....	169
Fig. 199	Servers - tab Details.....	169
Fig. 200	Servers - tab usage.....	170
Fig. 201	Group field API Server .....	170
Fig. 202	Select storage expansion.....	172
Fig. 203	Group field Audio Analysis .....	172
Fig. 204	Select server for emotion detection.....	173
Fig. 205	Group field Recording Control/Key Management .....	173
Fig. 206	Group field Data Processing .....	174
Fig. 207	Select server .....	176
Fig. 208	Group field Replay .....	176
Fig. 209	Select server .....	178

Fig. 210	Group field Virtualization .....	178
Fig. 211	Servers module - tab Media Streamer .....	179
Fig. 212	Servers Module - tab Replay Server Address Mapping .....	181
Fig. 213	Servers module - tab Key Management.....	182
Fig. 214	Servers module - tab Keystore/Virtualization .....	184
Fig. 215	PBX module - main view .....	185
Fig. 216	Toolbar PBX module .....	185
Fig. 217	Create new PBX - tab Details .....	187
Fig. 218	Tenants - main view - tab Extensions .....	188
Fig. 219	Assign extensions to tenants .....	189
Fig. 220	Remove extensions.....	190
Fig. 221	Select extensions .....	191
Fig. 222	Tenants - main view - tab PBX Agent ID.....	192
Fig. 223	Assign PBX Agent IDs to tenants.....	192
Fig. 224	Select PBX Agent IDs .....	194
Fig. 225	Additional Data module main view .....	194
Fig. 226	Configure additional data .....	195
Fig. 227	Additional data - configure availability .....	195
Fig. 228	Integrations - main view .....	196
Fig. 229	Toolbar Integrations module .....	196
Fig. 230	Choose file .....	197
Fig. 231	Upload grammar .....	197
Fig. 232	Create integration type.....	198
Fig. 233	Integrations - select PBX.....	198
Fig. 234	Assign recording architecture - All-in-one Parallel .....	199
Fig. 235	Configuration steps of the integration .....	199
Fig. 236	Configuration step - Configure Recording Architecture.....	200
Fig. 237	Configure tab MiVoice MX-ONE (CSTA) .....	201
Fig. 238	Configure CTIconnect module .....	201
Fig. 239	Configure connection data .....	202
Fig. 240	Configure connection data .....	202
Fig. 241	Arbitrary assignment of the additional data.....	203
Fig. 242	Configure switching conditions.....	204
Fig. 243	Configure regular expression for phone type identification .....	205
Fig. 244	Activate CTIconnect connection data for MBG .....	206
Fig. 245	Configure CTIconnect module .....	206
Fig. 246	Group field Connection Data.....	207
Fig. 247	Configure connection .....	207
Fig. 248	CTI connection data - additional data module 1.....	208
Fig. 249	Configuration step - configure monitor points .....	209
Fig. 250	Add extension monitor points.....	209
Fig. 251	Configured extension monitor points.....	211



Fig. 252	Configuration step - Global Recording Settings .....	212
Fig. 253	Configuration step - Configure recording servers .....	213
Fig. 254	Configure add-on for MiContact Center Enterprise .....	215
Fig. 255	Arbitrary assignment of the additional data .....	216
Fig. 256	Overview of the add on of Genesys T-Server .....	218
Fig. 257	Configure add-on for Genesys T-Server .....	219
Fig. 258	Configure connection data .....	220
Fig. 259	Arbitrary assignment of the additional data .....	222
Fig. 260	Configure miscellaneous settings .....	222
Fig. 261	Activate integration.....	223
Fig. 262	Activated integration.....	223
Fig. 263	Deactivate integration .....	224
Fig. 264	Recording architectures - main view .....	225
Fig. 265	Create recording architecture - Multi-Server Recording.....	226
Fig. 266	Recording architecture - tab Details - Multi-Server Recording .....	226
Fig. 267	Select integration type.....	227
Fig. 268	Recording architecture - tab Server Assignment .....	228
Fig. 269	Recording architecture - assign server - example.....	228
Fig. 270	Add recording server .....	229
Fig. 271	Recording architecture - activate recording architecture.....	230
Fig. 272	Servers - main view.....	231
Fig. 273	Toolbar Servers module.....	231
Fig. 274	Add server locations.....	232
Fig. 275	Delete server location .....	233
Fig. 276	Servers - tab Details.....	234
Fig. 277	Servers - tab usage .....	234
Fig. 278	Group field API Server .....	235
Fig. 279	Select storage expansion.....	236
Fig. 280	Group field Audio Analysis .....	237
Fig. 281	Select server for emotion detection.....	237
Fig. 282	Group field Recording Control/Key Management .....	237
Fig. 283	Group field Data Processing .....	238
Fig. 284	Select server .....	240
Fig. 285	Group field Replay .....	241
Fig. 286	Select server .....	242
Fig. 287	Group field Virtualization .....	243
Fig. 288	Servers module - tab Media Streamer .....	244
Fig. 289	Servers Module - tab Replay Server Address Mapping .....	246
Fig. 290	Servers module - tab Key Management.....	247
Fig. 291	Servers module - tab Keystore/Virtualization .....	249
Fig. 292	PBX module - main view .....	250
Fig. 293	Toolbar PBX module .....	250



Fig. 294	Create new PBX - tab Details .....	251
Fig. 295	Tenants - main view - tab Extensions .....	252
Fig. 296	Assign extensions to tenants .....	253
Fig. 297	Remove extensions.....	254
Fig. 298	Select extensions .....	255
Fig. 299	Tenants - main view - tab PBX Agent ID.....	256
Fig. 300	Assign PBX Agent IDs to tenants.....	256
Fig. 301	Select PBX Agent IDs .....	258
Fig. 302	Additional Data module main view .....	258
Fig. 303	Configure additional data .....	259
Fig. 304	Additional data - configure availability .....	259
Fig. 305	Integrations - main view .....	260
Fig. 306	Toolbar Integrations module .....	260
Fig. 307	Choose file .....	261
Fig. 308	Upload grammar .....	261
Fig. 309	Create integration type.....	262
Fig. 310	Integrations - select PBX.....	262
Fig. 311	Assign recording architecture - Multi-Server Recording.....	263
Fig. 312	Configuration steps of the integration .....	263
Fig. 313	Configuration step - Configure Recording Architecture.....	264
Fig. 314	CTI connection data - tab MiVoice MX-ONE (CSTA).....	265
Fig. 315	Configure CTIconnect module .....	265
Fig. 316	Configure connection data .....	266
Fig. 317	Configure connection data .....	266
Fig. 318	Arbitrary assignment of the additional data.....	267
Fig. 319	Configure switching conditions.....	268
Fig. 320	Configure regular expression for phone type identification .....	269
Fig. 321	Activate CTIconnect connection data for MBG .....	270
Fig. 322	Configure CTIconnect module .....	270
Fig. 323	Group field Connection Data.....	271
Fig. 324	Configure connection .....	271
Fig. 325	CTI connection data - additional data module 1.....	272
Fig. 326	Configuration step - configure monitor points .....	272
Fig. 327	Add extension monitor points.....	273
Fig. 328	Configured extension monitor points.....	274
Fig. 329	Configuration step - Global Recording Settings .....	276
Fig. 330	Configuration step - Configure recording servers .....	277
Fig. 331	Tab Extensions .....	278
Fig. 332	Add extensions.....	279
Fig. 333	Added extensions.....	279
Fig. 334	Configure add-on for MiContact Center Enterprise.....	280
Fig. 335	Arbitrary assignment of the additional data.....	282

Fig. 336 Overview of the add on of Genesys T-Server .....	283
Fig. 337 Configure add-on for Genesys T-Server .....	284
Fig. 338 Configure connection data .....	285
Fig. 339 Arbitrary assignment of the additional data .....	287
Fig. 340 Configure miscellaneous settings .....	287
Fig. 341 Activate integration.....	288
Fig. 342 Activated integration.....	288
Fig. 343 Deactivate integration .....	289
Fig. 344 Recording architectures - main view .....	290
Fig. 345 Toolbar Recording Architectures module .....	290
Fig. 346 Create recording architecture - Multi-Server Failover .....	291
Fig. 347 Recording architecture - tab Details - Multi-Server Failover .....	292
Fig. 348 Select integration type.....	293
Fig. 349 Recording Architecture - tab Server Assignment .....	294
Fig. 350 Recording Architecture - assign server - example .....	295
Fig. 351 Add Recording Server .....	296
Fig. 352 Recording architecture - activate recording architecture.....	297
Fig. 353 Servers - main view.....	297
Fig. 354 Toolbar Servers module.....	298
Fig. 355 Add server locations.....	299
Fig. 356 Delete server location .....	300
Fig. 357 Servers - tab Details.....	300
Fig. 358 Servers - tab usage.....	301
Fig. 359 Group field API Server .....	301
Fig. 360 Select storage expansion.....	303
Fig. 361 Group field Audio Analysis .....	303
Fig. 362 Select server for emotion detection.....	304
Fig. 363 Group field Recording Control/Key Management .....	304
Fig. 364 Group field Data Processing .....	305
Fig. 365 Select server .....	307
Fig. 366 Group field Replay .....	307
Fig. 367 Select server .....	309
Fig. 368 Group field Virtualization .....	309
Fig. 369 Servers module - tab Media Streamer .....	310
Fig. 370 Servers Module - tab Replay Server Address Mapping.....	312
Fig. 371 Servers module - tab Key Management.....	313
Fig. 372 Servers module - tab Keystore/Virtualization .....	315
Fig. 373 PBX module - main view .....	316
Fig. 374 Toolbar PBX module .....	316
Fig. 375 Create new PBX - tab Details .....	318
Fig. 376 Tenants - main view - tab Extensions .....	319
Fig. 377 Assign extensions to tenants .....	320

Fig. 378 Remove extensions.....	321
Fig. 379 Select extensions .....	322
Fig. 380 Tenants - main view - tab PBX Agent ID.....	323
Fig. 381 Assign PBX Agent IDs to tenants.....	323
Fig. 382 Select PBX Agent IDs .....	325
Fig. 383 Additional Data module main view .....	325
Fig. 384 Configure additional data .....	326
Fig. 385 Additional data - configure availability .....	326
Fig. 386 Integrations - main view .....	327
Fig. 387 Toolbar Integrations module .....	327
Fig. 388 Choose file .....	328
Fig. 389 Upload grammar .....	328
Fig. 390 Create integration type .....	329
Fig. 391 Integrations - select PBX.....	329
Fig. 392 Assign recording architecture - Multi-Server Failover .....	330
Fig. 393 Configuration steps of the integration .....	330
Fig. 394 Configuration step - Configure Recording Architecture.....	331
Fig. 395 CTI connection data - tab MiVoice MX-ONE (CSTA).....	332
Fig. 396 Configure CTIconnect module .....	332
Fig. 397 Configure connection data .....	333
Fig. 398 Configure connection data .....	333
Fig. 399 Arbitrary assignment of the additional data.....	334
Fig. 400 Configure switching conditions.....	335
Fig. 401 Configure regular expression for phone type identification .....	336
Fig. 402 Activate CTIconnect connection data for MBG .....	337
Fig. 403 Configure CTIconnect module .....	337
Fig. 404 Group field Connection Data.....	338
Fig. 405 Configure connection .....	338
Fig. 406 CTI connection data - additional data module 1.....	339
Fig. 407 Configuration step - configure monitor points .....	339
Fig. 408 Add extension monitor points.....	340
Fig. 409 Configured extension monitor points.....	341
Fig. 410 Configuration step - Global Recording Settings .....	342
Fig. 411 Configuration step - Configure recording servers .....	344
Fig. 412 Tab Extensions .....	345
Fig. 413 Add extensions.....	345
Fig. 414 Added extensions.....	346
Fig. 415 Configure add-on for MiContact Center Enterprise.....	347
Fig. 416 Arbitrary assignment of the additional data.....	348
Fig. 417 Overview of the add on of Genesys T-Server .....	350
Fig. 418 Configure add-on for Genesys T-Server .....	351
Fig. 419 Configure connection data .....	352

Fig. 420	Arbitrary assignment of the additional data .....	354
Fig. 421	Configure miscellaneous settings .....	354
Fig. 422	Activate integration.....	355
Fig. 423	Activated integration.....	355
Fig. 424	Deactivate integration .....	356
Fig. 425	Recording architectures - main view .....	357
Fig. 426	Toolbar Recording Architectures module.....	357
Fig. 427	Create recording architecture - Multi-Server Parallel Recording.....	358
Fig. 428	Recording architecture - tab Details - Multi-Server Parallel Recording.....	359
Fig. 429	Select integration type.....	360
Fig. 430	Recording architecture - server assignment device group 1 .....	361
Fig. 431	Recording architecture - assign server - example.....	361
Fig. 432	Add recording server .....	362
Fig. 433	Recording architecture - activate recording architecture - example.....	363
Fig. 434	Servers - main view.....	364
Fig. 435	Toolbar Servers module.....	364
Fig. 436	Add server locations.....	365
Fig. 437	Delete server location .....	366
Fig. 438	Servers - tab Details.....	367
Fig. 439	Servers - tab usage .....	367
Fig. 440	Group field API Server .....	368
Fig. 441	Select storage expansion.....	369
Fig. 442	Group field Audio Analysis .....	370
Fig. 443	Select server for emotion detection.....	370
Fig. 444	Group field Recording Control/Key Management .....	370
Fig. 445	Group field Data Processing .....	371
Fig. 446	Select server .....	373
Fig. 447	Group field Replay .....	374
Fig. 448	Select server .....	375
Fig. 449	Group field Virtualization .....	376
Fig. 450	Servers module - tab Media Streamer .....	377
Fig. 451	Servers Module - tab Replay Server Address Mapping .....	379
Fig. 452	Servers module - tab Key Management.....	380
Fig. 453	Servers module - tab Keystore/Virtualization .....	382
Fig. 454	PBX module - main view .....	383
Fig. 455	Toolbar PBX module .....	383
Fig. 456	Create new PBX - tab Details .....	384
Fig. 457	Tenants - main view - tab Extensions .....	385
Fig. 458	Assign extensions to tenants .....	386
Fig. 459	Remove extensions.....	387
Fig. 460	Select extensions .....	388
Fig. 461	Tenants - main view - tab PBX Agent ID.....	389

Fig. 462	Assign PBX Agent IDs to tenants.....	389
Fig. 463	Select PBX Agent IDs .....	391
Fig. 464	Additional Data module main view .....	391
Fig. 465	Configure additional data .....	392
Fig. 466	Additional data - configure availability .....	392
Fig. 467	Integrations - main view .....	393
Fig. 468	Toolbar Integrations module .....	393
Fig. 469	Choose file .....	394
Fig. 470	Upload grammar .....	394
Fig. 471	Create integration type .....	395
Fig. 472	Integrations - select PBX.....	395
Fig. 473	Assign recording architecture - Multi-Server Parallel .....	396
Fig. 474	Configuration steps of the integration .....	396
Fig. 475	Configuration step - Configure Recording Architecture.....	397
Fig. 476	Configure tab MiVoice MX-ONE (CSTA) .....	398
Fig. 477	Configure CTIconnect module .....	398
Fig. 478	Configure connection data .....	399
Fig. 479	Configure connection data .....	399
Fig. 480	Arbitrary assignment of the additional data.....	400
Fig. 481	Configure switching conditions.....	401
Fig. 482	Configure regular expression for phone type identification .....	402
Fig. 483	Configure CTIconnect connection data to MBG.....	403
Fig. 484	Configure CTIconnect module .....	403
Fig. 485	Group field Connection Data.....	404
Fig. 486	Configure connection .....	405
Fig. 487	CTI connection data - additional data module 1.....	406
Fig. 488	Configuration step - configure monitor points .....	406
Fig. 489	Add extension monitor points.....	407
Fig. 490	Configured extension monitor points.....	408
Fig. 491	Configuration step - Global Recording Settings .....	409
Fig. 492	Configuration step - Configure recording servers .....	411
Fig. 493	Configure add-on for MiContact Center Enterprise.....	412
Fig. 494	Arbitrary assignment of the additional data.....	414
Fig. 495	Overview of the add on of Genesys T-Server .....	415
Fig. 496	Configure add-on for Genesys T-Server .....	416
Fig. 497	Configure connection data .....	417
Fig. 498	Arbitrary assignment of the additional data.....	419
Fig. 499	Configure miscellaneous settings .....	419
Fig. 500	Activate integration.....	420
Fig. 501	Activated integration.....	420
Fig. 502	Deactivate integration .....	421
Fig. 503	Servers module - Activate emotion detection.....	422

Fig. 504 Create integration - tab Recording Content Validation.....	422
Fig. 505 Select server for emotion detection.....	423
Fig. 506 Servers - tab Usage .....	425
Fig. 507 Group field Recording Control/Key Management .....	425
Fig. 508 PHONEapp - main view: .....	426
Fig. 509 Detail view phone types .....	427
Fig. 510 Display of the properties .....	427
Fig. 511 Detail view Default settings .....	428
Fig. 512 Group field Tagging Attributes .....	430
Fig. 513 Edit tagging attributes .....	431
Fig. 514 Group field Register Fields.....	431
Fig. 515 Edit register fields.....	432
Fig. 516 Configure tagging fields .....	433
Fig. 517 Edit tagging fields.....	433
Fig. 518 Activate PHONEapp configuration .....	434
Fig. 519 Phones - main view .....	435
Fig. 520 Toolbar .....	436
Fig. 521 Create phone .....	436
Fig. 522 Create phones - activate PHONEapp .....	437
Fig. 523 Configure key function via the web interface .....	439
Fig. 524 Configure HTTPS settings .....	440
Fig. 525 Configure XML Push Server .....	441
Fig. 526 Assignment of the top keys and displayed status of the recording .....	441
Fig. 527 Synchronize recording control.....	442
Fig. 528 Menu item Manage Synchronization Configurations.....	443
Fig. 529 Configure synchronization configurations .....	444
Fig. 530 Create synchronization configuration.....	445
Fig. 531 Tab Parallel Recording (integration) .....	447
Fig. 532 Map additional data .....	448
Fig. 533 Select additional data.....	449
Fig. 534 Delete additional data assignment.....	449
Fig. 535 Configure standby management.....	450
Fig. 536 Switch server.....	451
Fig. 537 Menu of the standby management.....	452
Fig. 538 Switch server.....	452
Fig. 539 Main view .....	455
Fig. 540 Tab Details (example).....	456
Fig. 541 Add PBX .....	458
Fig. 542 Add tenant.....	458
Fig. 543 Tab Drives - WAVE / MP3 formats.....	459
Fig. 544 Add drive .....	459
Fig. 545 Tab Mapping for WAVE / MP3 import formats .....	460

Fig. 546	Group field Data Structure .....	460
Fig. 547	Group field Start time - Import format WAVE / MP3 + CSV .....	461
Fig. 548	Group field Start time - Import format WAVE / MP3 + XML .....	461
Fig. 549	Group field Participant phone number (example) .....	462
Fig. 550	Edit source for participant phone number (example) .....	463
Fig. 551	Edit source for additional data (example for WAVE import format).....	464
Fig. 552	POWERplay Web - Recording View .....	464
Fig. 553	Recording View - tab Additional Data .....	465
Fig. 554	Genesys Administrator - select T-Server .....	465
Fig. 555	Genesys Administrator - configure T-Server.....	466
Fig. 556	Genesys Administrator - select configuration server.....	466
Fig. 557	Genesys Administrator - configure configuration server .....	467
Fig. 558	Genesys Administrator - switch instances .....	467
Fig. 559	Genesys Administrator - configure switch instance .....	468
Fig. 560	Genesys administrator - create user .....	468



## 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.....	11
Tab. 7	Parameters for the ICP .....	21
Tab. 8	Parameters for MiNET device .....	22
Tab. 9	Login data - system provider.....	26
Tab. 10	Configure audio analysis.....	39
Tab. 11	Configure recording control/key management .....	40
Tab. 12	Data storage.....	41
Tab. 13	Configure replay.....	43
Tab. 14	Configure virtualization.....	45
Tab. 15	Create PBX .....	53
Tab. 16	Create integration type.....	64
Tab. 17	Configure CTIconnect module .....	67
Tab. 18	Configure connection data .....	68
Tab. 19	Configure CTIconnect module .....	72
Tab. 20	Configure connection data .....	73
Tab. 21	Global recording settings .....	78
Tab. 22	Configure recording servers.....	79
Tab. 23	Configure CTIconnect module .....	81
Tab. 24	Configure connection data .....	82
Tab. 25	Configure add-on for Genesys T-Server .....	85
Tab. 26	Configure connection data .....	86
Tab. 27	Configure audio analysis.....	103
Tab. 28	Configure recording control/key management .....	104
Tab. 29	Data storage.....	105
Tab. 30	Configure replay.....	107
Tab. 31	Configure virtualization.....	109
Tab. 32	Create PBX .....	118
Tab. 33	Create integration type.....	129
Tab. 34	Configure CTIconnect module .....	132
Tab. 35	Configure connection data .....	133
Tab. 36	Configure CTIconnect module .....	137
Tab. 37	Configure connection data .....	138
Tab. 38	Global recording settings .....	143
Tab. 39	Configure recording servers.....	144
Tab. 40	Configure recording servers.....	146
Tab. 41	Configure CTIconnect module .....	150



Tab. 42	Configure connection data .....	151
Tab. 43	Configure add-on for Genesys T-Server .....	154
Tab. 44	Configure connection data .....	155
Tab. 45	Configure audio analysis.....	172
Tab. 46	Configure recording control/key management .....	173
Tab. 47	Data storage.....	174
Tab. 48	Configure replay.....	176
Tab. 49	Configure virtualization.....	178
Tab. 50	Create PBX .....	187
Tab. 51	Create integration type.....	198
Tab. 52	Configure CTIconnect module .....	201
Tab. 53	Configure connection data .....	202
Tab. 54	Configure CTIconnect module .....	206
Tab. 55	Configure connection data .....	207
Tab. 56	Global recording settings .....	212
Tab. 57	Configure recording servers.....	213
Tab. 58	Configure CTIconnect module .....	215
Tab. 59	Configure connection data .....	216
Tab. 60	Configure add-on for Genesys T-Server .....	219
Tab. 61	Configure connection data .....	220
Tab. 62	Configure audio analysis.....	237
Tab. 63	Configure recording control/key management .....	238
Tab. 64	Data storage.....	239
Tab. 65	Configure replay.....	241
Tab. 66	Configure virtualization.....	243
Tab. 67	Create PBX .....	251
Tab. 68	Create integration type.....	262
Tab. 69	Configure CTIconnect module .....	265
Tab. 70	Configure connection data .....	266
Tab. 71	Configure CTIconnect module .....	270
Tab. 72	Configure connection data .....	271
Tab. 73	Global recording settings .....	276
Tab. 74	Configure recording servers.....	277
Tab. 75	Configure CTIconnect module .....	281
Tab. 76	Configure connection data .....	281
Tab. 77	Configure add-on for Genesys T-Server .....	284
Tab. 78	Configure connection data .....	285
Tab. 79	Configure audio analysis.....	303
Tab. 80	Configure recording control/key management .....	304
Tab. 81	Data storage.....	305
Tab. 82	Configure replay.....	307
Tab. 83	Configure virtualization.....	309

Tab. 84	Create PBX .....	318
Tab. 85	Create integration type .....	329
Tab. 86	Configure CTIconnect module .....	332
Tab. 87	Configure connection data .....	333
Tab. 88	Configure CTIconnect module .....	337
Tab. 89	Configure connection data .....	338
Tab. 90	Global recording settings .....	343
Tab. 91	Configure recording servers .....	344
Tab. 92	Configure CTIconnect module .....	347
Tab. 93	Configure connection data .....	348
Tab. 94	Configure add-on for Genesys T-Server .....	351
Tab. 95	Configure connection data .....	352
Tab. 96	Configure audio analysis .....	370
Tab. 97	Configure recording control/key management .....	371
Tab. 98	Data storage .....	372
Tab. 99	Configure replay .....	374
Tab. 100	Configure virtualization .....	376
Tab. 101	Create PBX .....	384
Tab. 102	Create integration type .....	395
Tab. 103	Configure CTIconnect module .....	398
Tab. 104	Configure connection data .....	399
Tab. 105	Configure CTIconnect module .....	404
Tab. 106	Configure connection data .....	405
Tab. 107	Global recording settings .....	409
Tab. 108	Configure recording servers .....	411
Tab. 109	Configure CTIconnect module .....	413
Tab. 110	Configure connection data .....	413
Tab. 111	Configure add-on for Genesys T-Server .....	416
Tab. 112	Configure connection data .....	417
Tab. 113	Configure recording control/key management .....	425
Tab. 114	Add phone .....	437
Tab. 115	Mapping rules for participant phone numbers .....	462
Tab. 116	Buttons .....	463

## 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)

### **BIB**

Built-in Bridge The IP phone establishes a conference itself to send the audio stream to the recording server, too.

### **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

### **DNS**

Domain Name System is a worldwide directory service which administrates the name domain of the Internet. Its main task is to answer the queries regarding name resolutions. (Source: Wikipedia 5th April 2017)

### **ICP**

Internet Communications Platform

### **IP**

Internet Protocol, basic protocol for Internet communication

---

**LCR**

Last Conversation Repeat

---

**LED**

Light-emitting diode

---

**MBG**

MiVoice Border Gateway

---

**MP3**

Description of the digitally saved audio data. MP3 compression works by reducing (or approximating) the accuracy of certain components of sound that are considered (by psychoacoustic analysis) to be beyond the hearing capabilities of most humans. The remaining audio information is then recorded in a space-efficient manner. (Source: Wikipedia 9th July 2020)

---

**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 (Mitel)**

With Mitel, 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, former name Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

---

### **UDP**

User Datagram Protocol UDP is a minimal, connectionless network protocol which belongs to the core members of the Internet protocol suite. Its purpose is to make sure that data transmitted via the Internet reach the designated application. There is no destination check.

---

### **URL**

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)

---

### **VM**

Virtual machine

---

### **VoIP**

Voice over IP

---

### **WAVE**

WAVE file format is a container format to digitally save audio data and is based on the Resource Interchange File Format (RIFF) defined by Microsoft for Windows. (Source: Wikipedia 23rd February 2021)

---

### **XML**

Extensible Markup Language is a human-readable and machine-readable language which defines a set of rules for encoding documents.