

EVOIPneo active for Mitel MiVoice MX-ONE (CSTA3)



Administration manual for system providers

6/2/2022

Product line Neo, version 7.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 <https://www.asctechnologies.com>.

Copyright © 2022 ASC Technologies AG. All rights reserved.

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

Contents

1	General information.....	5
2	Introduction.....	6
3	System requirements	9
3.1	Hardware components.....	9
3.1.1	Recorder	9
3.2	Software components.....	9
3.3	Mitel system components	9
3.4	Genesys system components (optional).....	9
3.4.1	Genesys Framework.....	9
4	Installation requirements	10
4.1	Licenses.....	10
4.2	Information.....	11
5	Overview install and configure product	12
6	Installation.....	13
7	Configuration	14
7.1	Configure Mitel MiVoice MX-ONE CSTA 3.....	14
7.1.1	Configure CSTA server.....	14
7.1.2	Configure extension monitor points	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	Configure MiVoice Border Gateway for NEO access via Web Proxy	23
7.2.3	Confirm certificate on MBG.....	24
7.3	System Configuration	26
7.3.1	Start application	27
7.3.2	Configure recording solution Mitel MX-ONE CSTA	28
7.3.2.1	Configure recording solution All-in-one Basic.....	28
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	222
7.3.2.5	Configure recording solution Multi-Server Failover.....	287
7.3.2.6	Configure recording solution Multi-Server Parallel Recording	353
7.3.3	Configure Recording Content Validation	418
7.3.4	Configure PHONEapp for Mitel.....	421
7.3.4.1	Configure Servers module	422
7.3.4.2	Configure PHONEapp module.....	423
7.3.4.3	Configure PBX module	431
7.3.4.4	Configure Phones module	432

7.3.4.5	Configure Recording Planner module.....	435
7.3.4.6	Configure key functions on the Mitel phone.....	436
7.3.5	Synchronization options.....	438
7.3.5.1	Synchronization of recording control	439
7.3.5.2	Synchronization of system storage.....	440
7.3.6	Configure duplicate detection	442
7.3.6.1	Tab Detect Duplicates	443
7.3.6.2	Additional data	445
7.3.6.3	Criteria to be ignored	446
7.3.7	Standby management for failover architectures	447
7.3.7.1	Standby management for All-in-one Failover	447
7.3.7.2	Standby management for Multi-Server Failover	449
7.3.8	Software update.....	450
7.4	Configure CTIconnect add-on.....	451
7.4.1	Configure Genesys T-Server (optional).....	451
7.4.1.1	Configure IP address and port of the Genesys T-Server.....	451
7.4.1.2	Configure IP address and port of the Genesys Configuration Server.....	452
7.4.1.3	Configure switch instance in the Genesys Configuration Server.....	453
7.4.1.4	Create users for the Genesys Configuration Server.....	454
8	Troubleshooting	455
	List of figures	456
	List of tables.....	470
	Glossary	473

1 General information

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

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

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

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

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

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

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

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



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

The recording solution EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA 3) provides the functionality which is necessary for 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_{neo} 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 Stream Recording)

The recording server receives the audio data of the monitored end devices directly from the phones. For each recorded end device, 2 separate RTP streams are sent. Depending in the configuration of the PBX, these streams may be encrypted. The respective key is provided via the "CSTA-Phase-III" protocol.

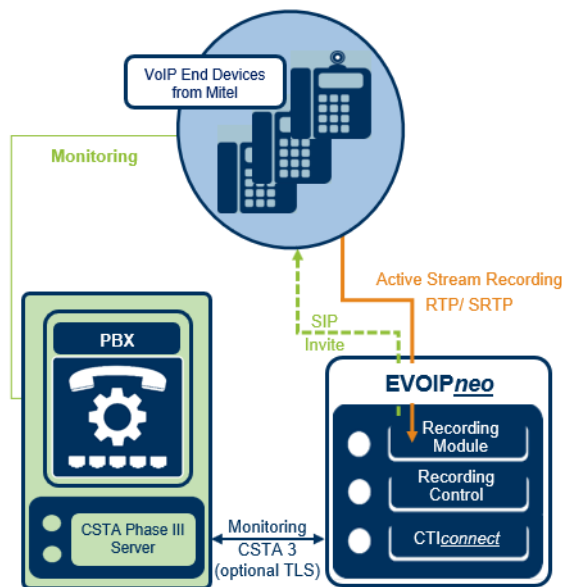


Fig. 1: Recording solution with VoIP end devices without MBG (Active Stream Recording)

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](#).

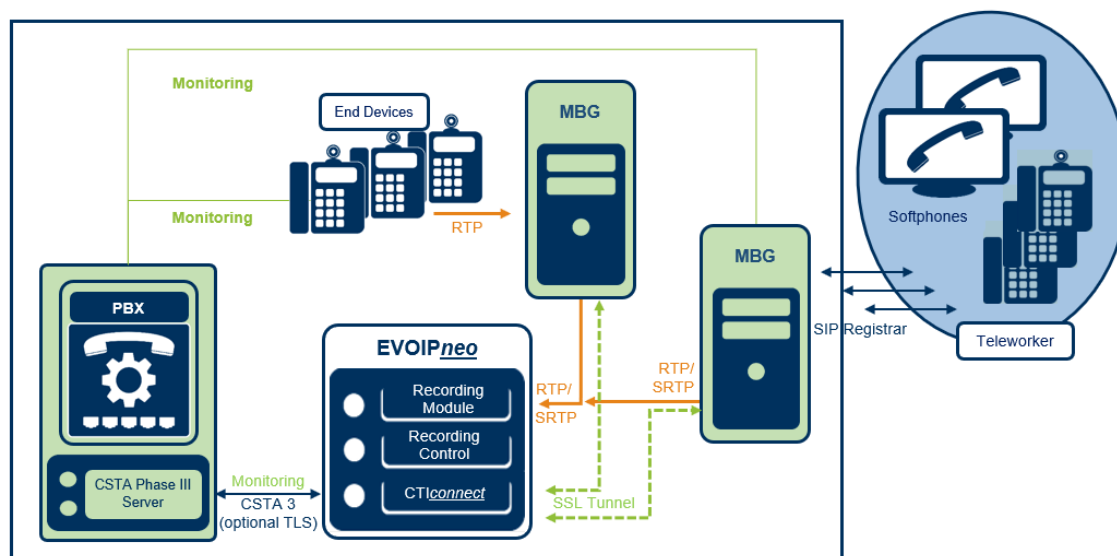


Fig. 2: Recording solution with MBG

Recording solution with intrusion

For this recording solution Neo offers the feature Intrusion which records the recording server by means of silent call intrusion. This allows recording [VoIP](#) and [TDM](#) end devices. In silent call intrusion, the recording server initiates a silent conference including itself and other call participants. The recording server registers on the PBX with the configured recording server extension via the [CSTA](#) connection. For concurrent recording, an extension for the recording server must be available, too.

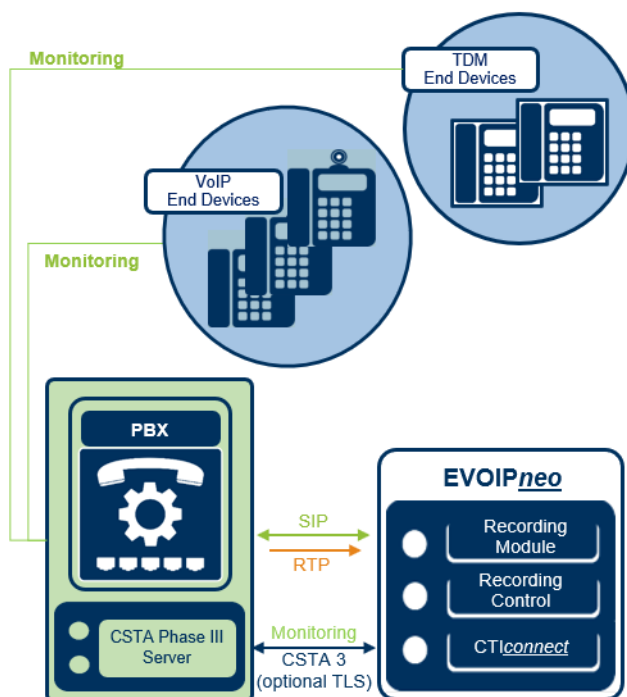


Fig. 3: Recording solution with intrusion



As intrusion is basically a conference recording, this recording type does not allow for recording actual conference calls. 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 EVOIP^{neo} passive for Mitel MiVoice MX-ONE trunk-side recording.



For a description of the import of InAttend conversations refer to the administration manual for system providers EVOIP^{neo} passive for SIP with Mitel InAttend.

3 System requirements



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



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



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

3.1 Hardware components



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



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

3.1.1 Recorder

For the recording solution you can use the following systems:

- EVOLUTION_{neo} eco
- EVOLUTION_{neo}
- EVOLUTION_{neo} XXL



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

3.2 Software components

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

3.3 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_{connect} for Genesys T-Server, a Genesys Framework with T-Servers and Genesys Configuration Servers are required.

4 Installation requirements



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



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

4.1 Licenses

ASC

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

Tab. 1: Licenses for recording server

License name	Number
PHONE _{app} for Mitel MiVoice Business, MiVoice 5000 and MX-ONE per system	1 license per recording system
PHONE _{app} 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 Microsoft Windows Server 2016*, *Configuration Microsoft Windows Server 2019* or *Configuration Microsoft Windows Server 2022*.



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

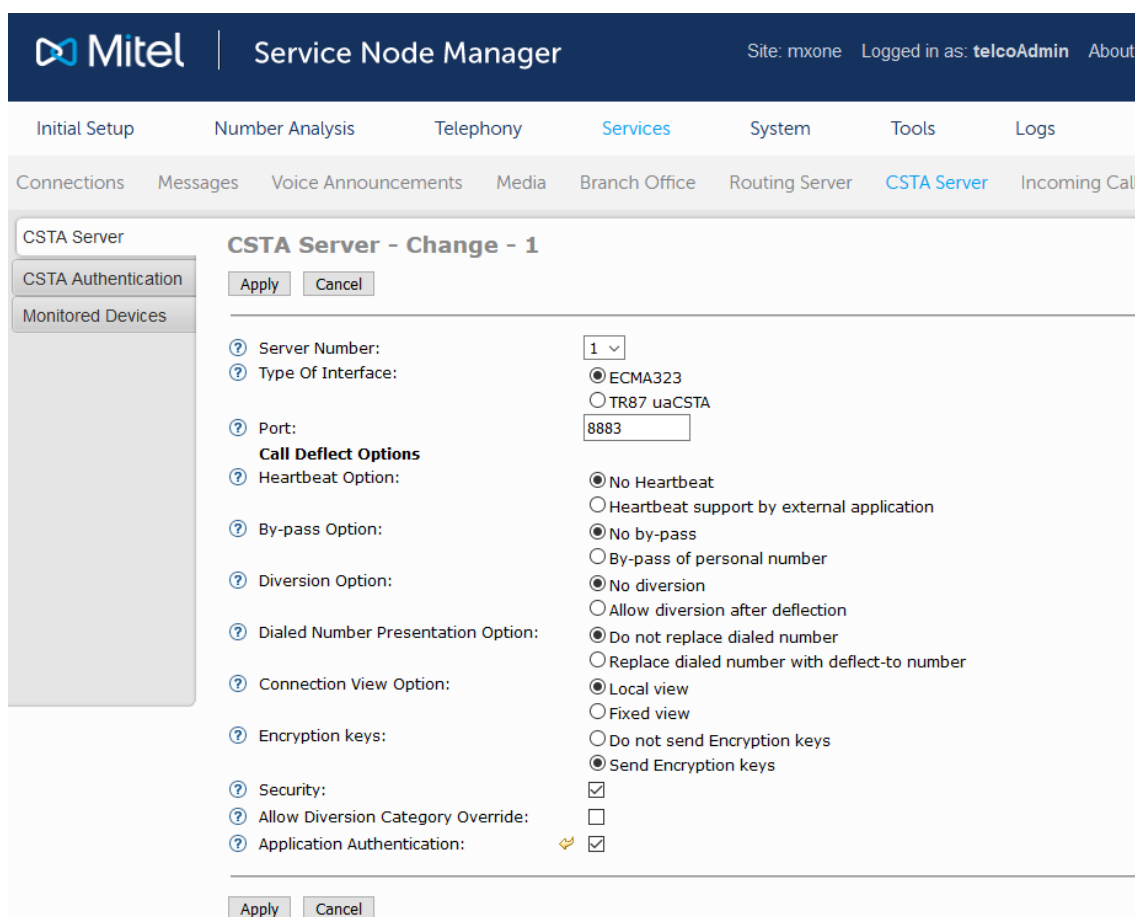
7.1 Configure Mitel MiVoice MX-ONE CSTA 3



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. Select the menu item *Subsystem*.
4. Select the respective subsystem.
⇒ The *Service Node Manager* opens.
5. Select the menu item *Services*.
6. In the menu bar below, select the menu item *CSTA Server*.
7. In the navigation bar, select the menu item *CSTA Server*.



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 that 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 mandatory 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 the option, if the connection via TLS is supposed to be used. Default is unencrypted.</p> <p>NOTICE! When the option <i>Encryption keys</i> has been activated and the option <i>Security</i> has been deactivated at the same time, the <i>encryption keys</i> are transferred without encryption. This is a security gap as potential attackers could pick off these keys and decrypted encrypted audio data streams.</p>
<i>Application Authentication</i>	<p>Activate this option to use authentication for this application.</p> <p>NOTICE! If you would like to use authentication, you must activate it here and in the Neo application System Configuration in the CTI connection data.</p>

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

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

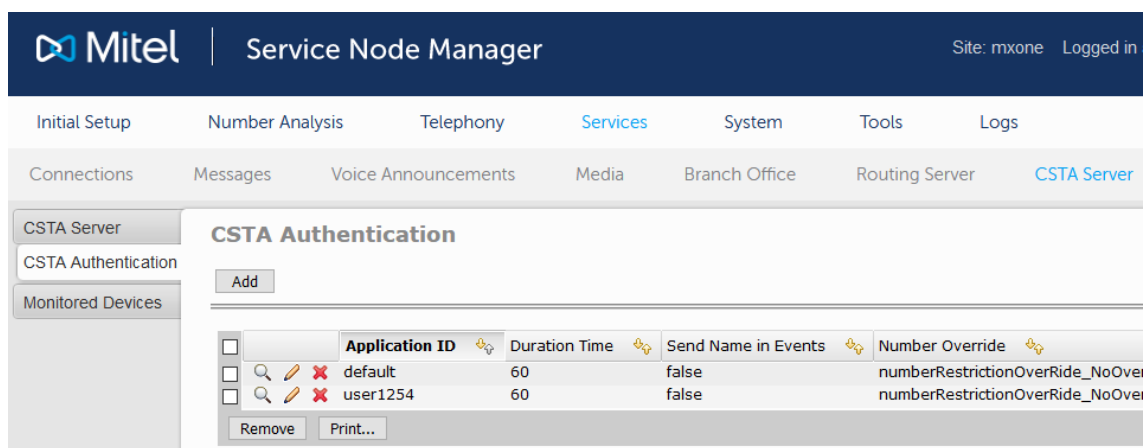
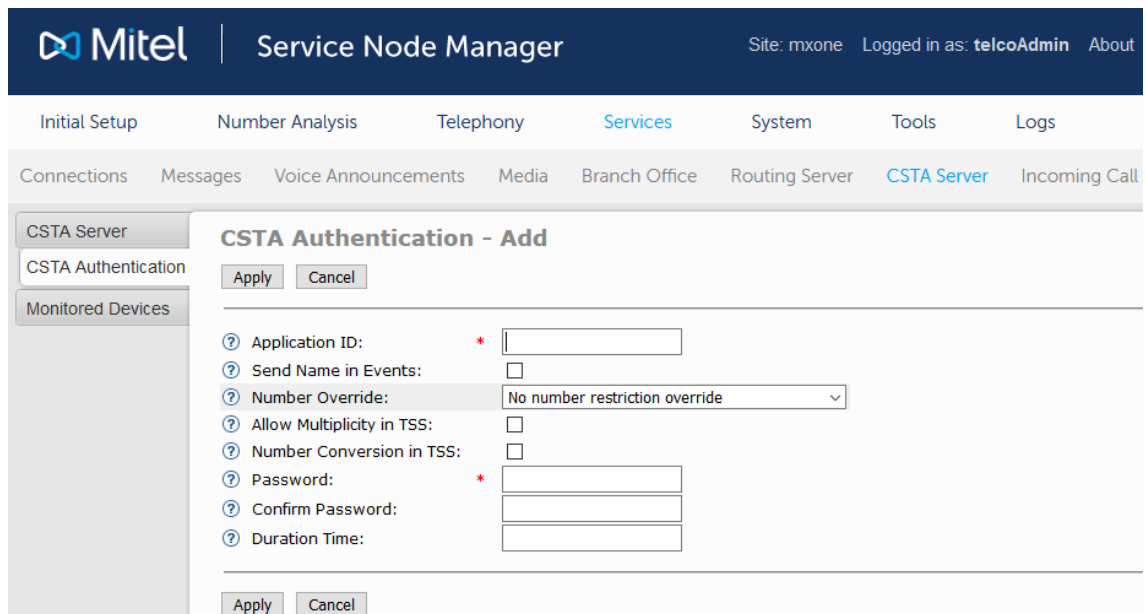


Fig. 5: Configure CSTA server

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



The screenshot shows the Mitel Service Node Manager web 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:

At the bottom of the form are 'Apply' and 'Cancel' buttons.

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:

Name Identity

? First Name:

? Last Name:

Authorization Code

MX-ONE

22001

1

IP

None ▾

0 - CSP0 (None) ▾

Default ▾

☒

NO

None ▾

☒ SIP

☐ IP

No, can not be changed via terminal menu ▾

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.

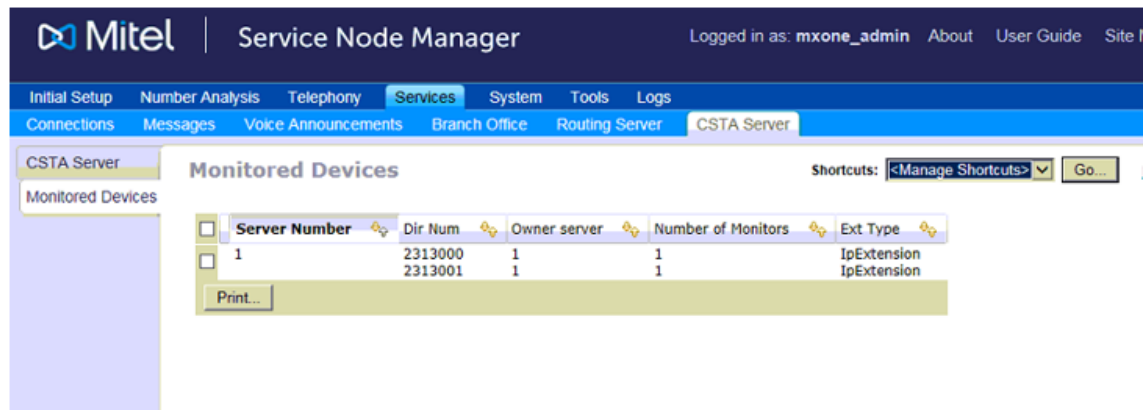


Fig. 8: Check set monitor points

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.

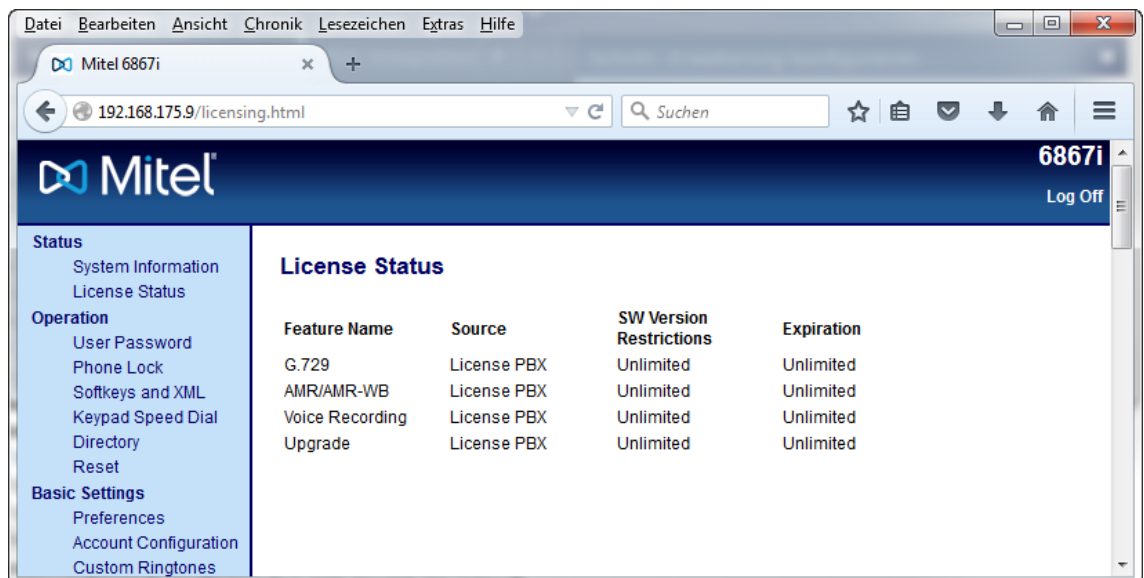


Fig. 9: Check license status

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.

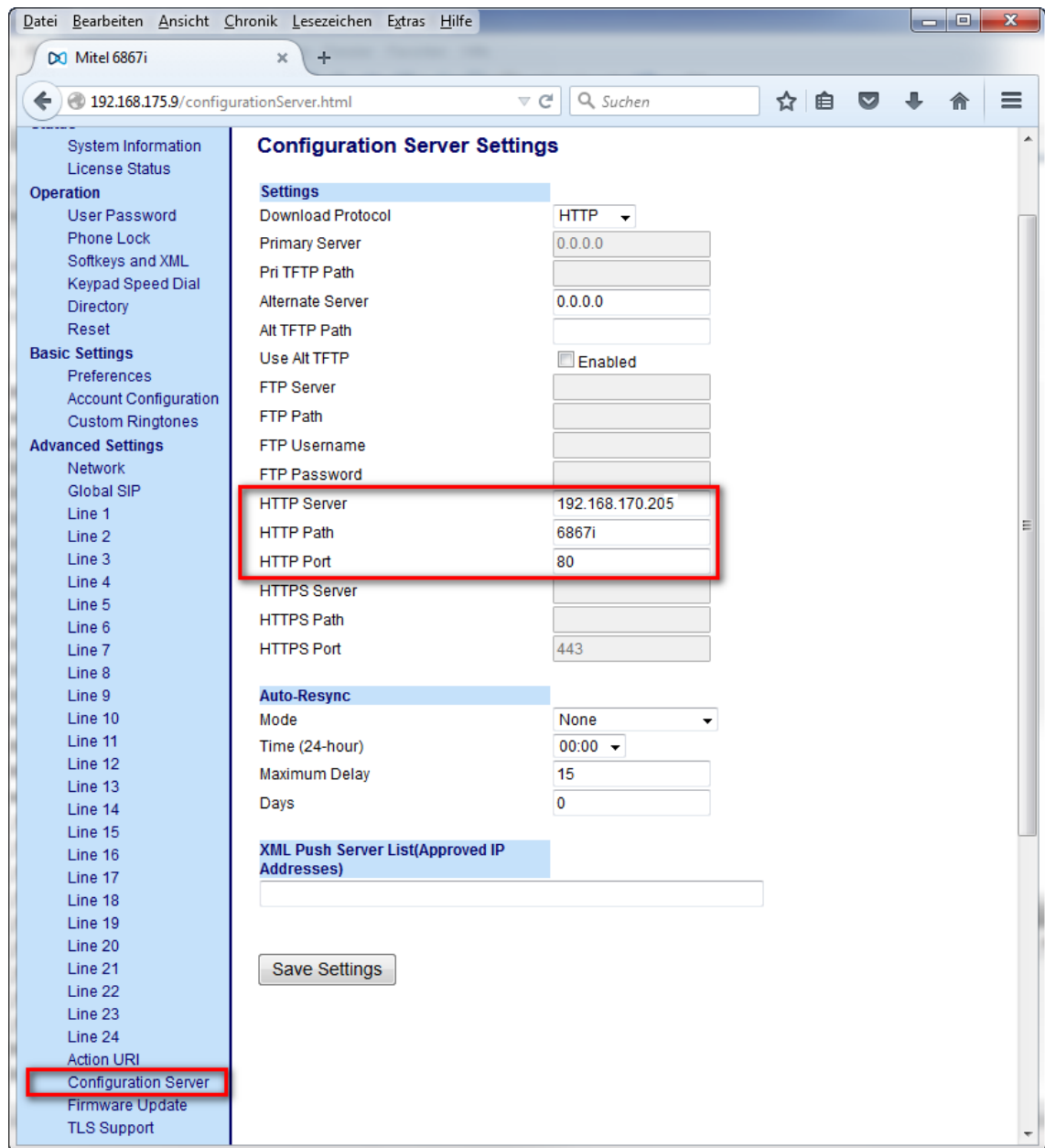


Fig. 10: Check server, path and port

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 SIP configuration of the end devices in the PBX.
<i>recorder periodic beep</i>	If this parameter has been configured, a beep signal is sent in defined intervals during the recording. This entry only appears if it has been configured in the PBX.

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

7.2 Configure 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*.

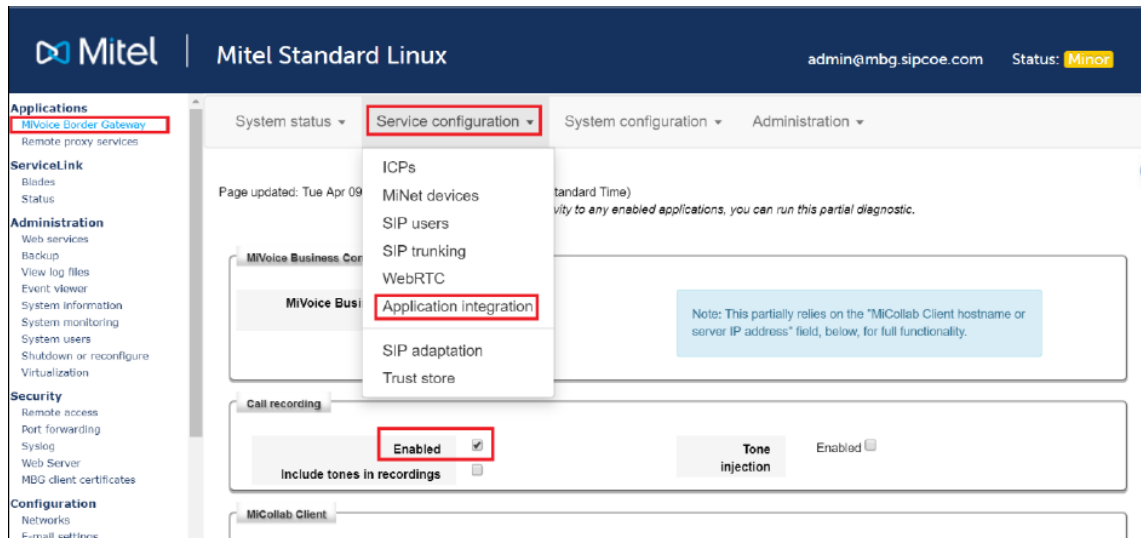


Fig. 12: Activate MBG for Call Recording

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*.

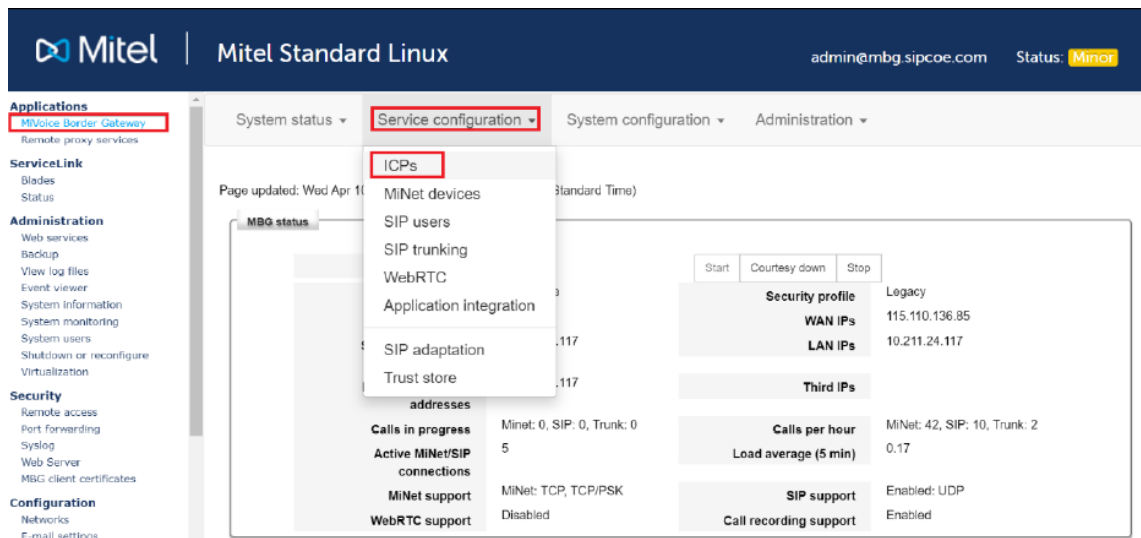


Fig. 13: Add MBG ICPs

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

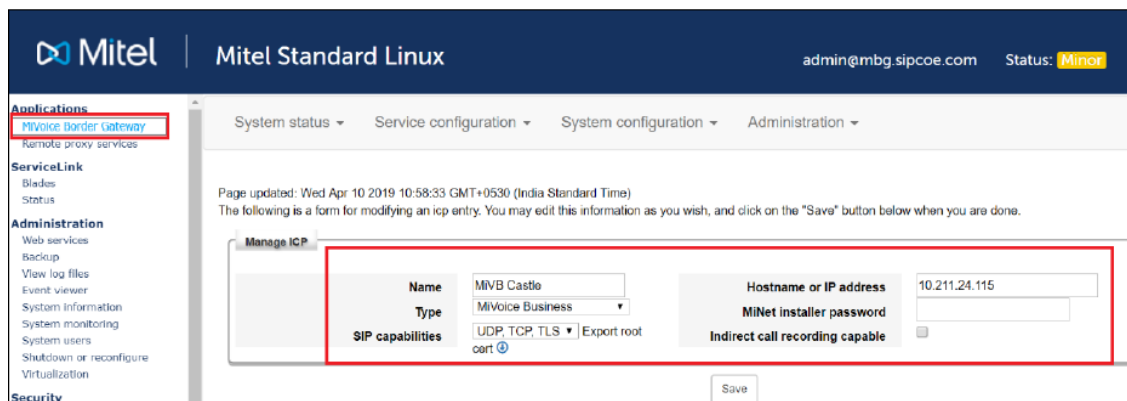


Fig. 14: Configure MBG ICP

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:

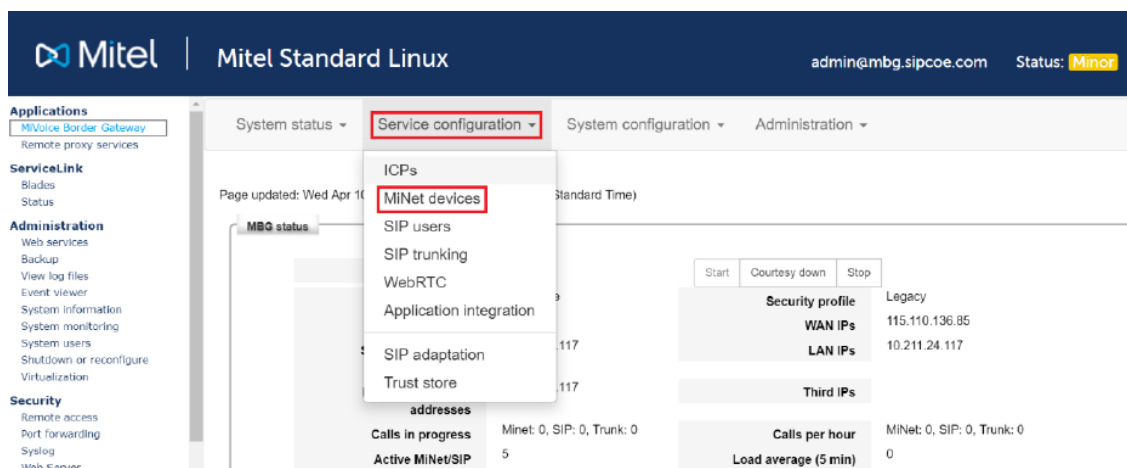
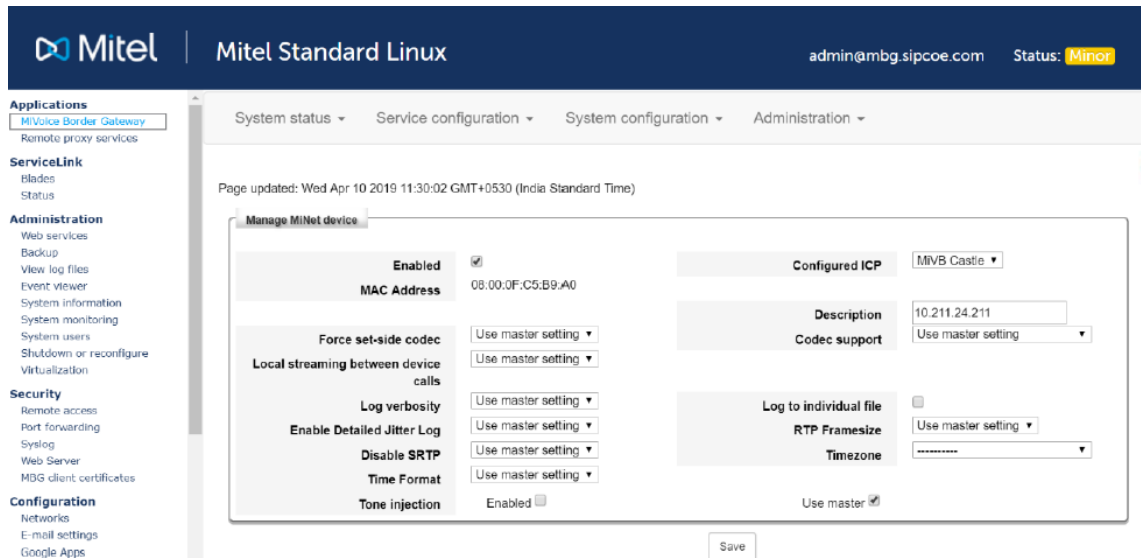


Fig. 15: Add MiNET devices

<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



Mitel | Mitel Standard Linux admin@mbg.sipcoe.com Status: Minor

System status ▾ Service configuration ▾ System configuration ▾ Administration ▾

Page updated: Wed Apr 10 2019 11:30:02 GMT+0530 (India Standard Time)

Manage MiNET device

Enabled ☒ **MAC Address** 08:00:0F:C5:B9:A0 **Configured ICP** MVB Castle ▾

Force set-side codec Use master setting ▾ **Description** 10.211.24.211

Local streaming between device calls Use master setting ▾ **Codec support** Use master setting ▾

Log verbosity Use master setting ▾ **Log to individual file** ☐

Enable Detailed Jitter Log Use master setting ▾ **RTP Framesize** Use master setting ▾

Disable SRTP Use master setting ▾ **Timezone** ▾

Time Format Use master setting ▾ **Use master** ☒

Tone injection Enabled ☐ **Save**

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

Configure MiVoice Border Gateway for NEO access via Web Proxy

If the MBG is supposed to be used as Web Proxy for accessing the Neo web applications the following configuration steps must be carried out:

1. For administration purposes, log in to the web interface of the MBG.
2. Select the menu item *Security > Remote access* in the navigation bar. Here, you find a MIR profile for the web access to Neo via the MBG.

In the Web Proxy server, the URLs for the following applications have been preconfigured:

Mitel Interaction Recording	mir	/INSPIRATIONneo /INSIGHTneo /REPORTneo /POWERplayWeb /Portal /SystemMonitoring /PHONEapp /ASCWebService	/SystemConfiguration		✓	User	Admin
-----------------------------	-----	--	----------------------	--	---	------	-------

Fig. 17: Proxy configuration

3. Activate the access for this MIR profile.

To enable replay in POWERplay Web via a MBG Web Proxy server, too, you must set up a forwarding for the default port of the replay server.

4. Select the menu item *Security > Port forwarding* in the navigation bar.
5. Click on the button *Create port forwarding rule* and create a new forwarding rule for the default port 4040 of the replay server.

Configure Port Forwarding

You can use this panel to modify your firewall rules so as to open a specific port on this server and forward it to a permit incoming traffic to directly access a private host on your LAN.

WARNING: Misuse of this feature can seriously compromise the security of your network. Do not use this feature implications of your actions.

Create port forwarding rule

Below you will find a table summarizing the current port-forwarding rules installed on this server. Click on the "Re

Protocol	Source Port(s)	Destination Host IP Address	Destination Port(s)	SNAT	Action
TCP	4040	10.0.0.122	4040	Yes	Remove

Fig. 18: Create forwarding rule for the port of the replay server

6. Scroll down to the group field *Secure Recording Connector*.

7. In the drop-down list *Mode*, select the entry *MBG*.

8. Define a password for the *PSK* mode.

NOTICE! The same password must be used in the System Configuration in the integration in the *MBG* connection data for the pre-shared key. See [chapter "Configure CTI connection data"](#), p. 68.



The image shows the 'Secure Recording Connector' configuration panel. It includes a 'PSK' mode dropdown menu, a 'PSK password' field with a masked password, a 'Tone Injection' section with an 'Enable' checkbox, and an 'Include tones in recordings' checkbox. A 'Save' button is at the bottom.

Fig. 19: Select PSK method

9. Configure the pre-shared key in the CTI connection data, see [chapter "Configure CTI connection data"](#), p. 68.

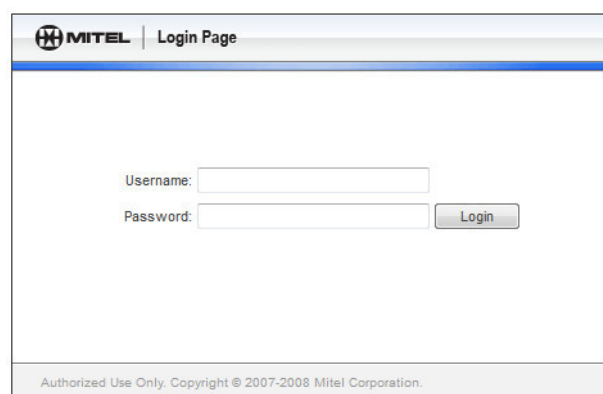
7.2.3 Confirm certificate on MBG

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.

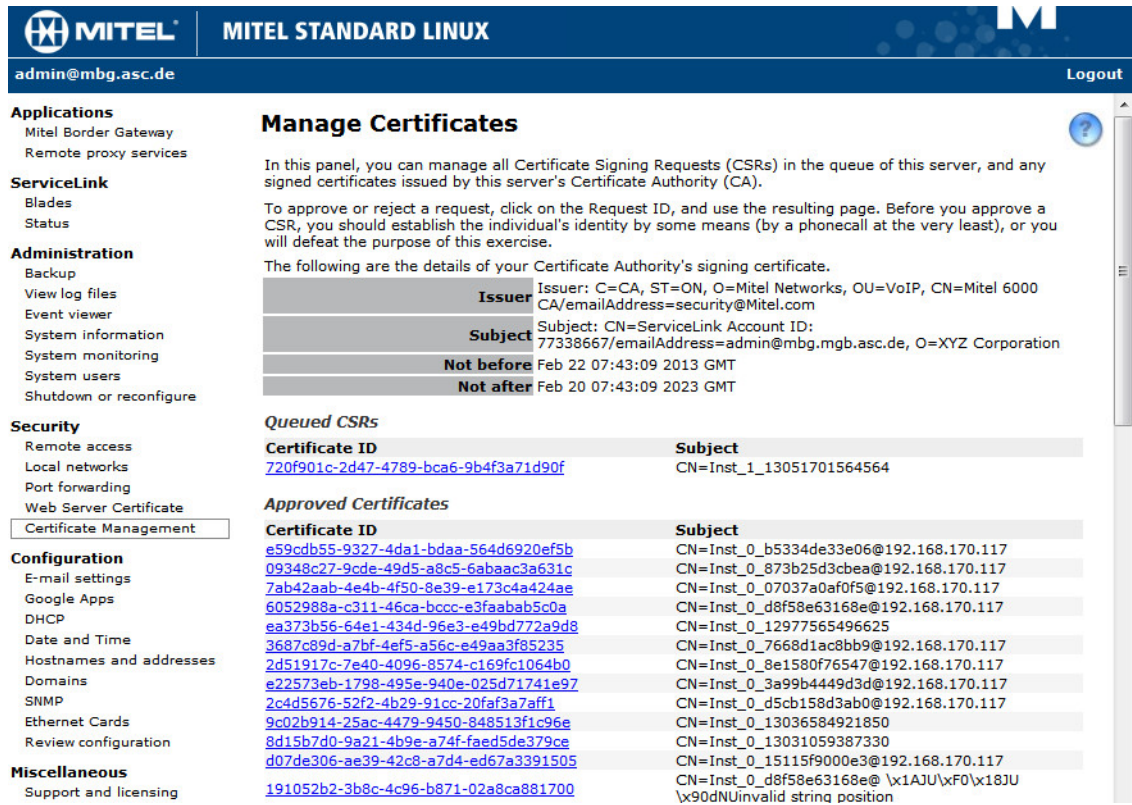
1. Connect to the *MBG*.



The image shows the Mitel Login Page. It has a header with the Mitel logo and 'Login Page'. Below are fields for 'Username' and 'Password', followed by a 'Login' button. At the bottom, it says 'Authorized Use Only. Copyright © 2007-2008 Mitel Corporation.'

Fig. 20: 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:



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

Manage Certificates

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

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

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

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

Queued CSRs

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

Approved Certificates

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

Fig. 21: Certificate Management

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

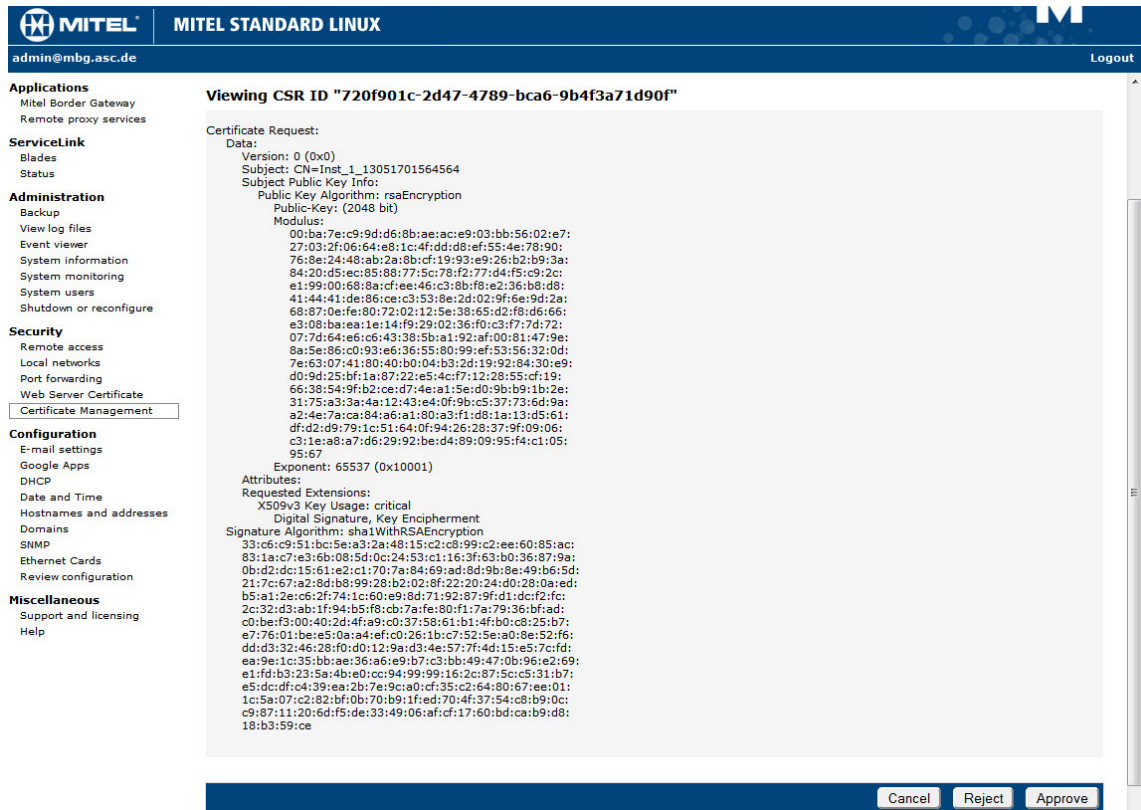


Fig. 22: Confirm selected certificate

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

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

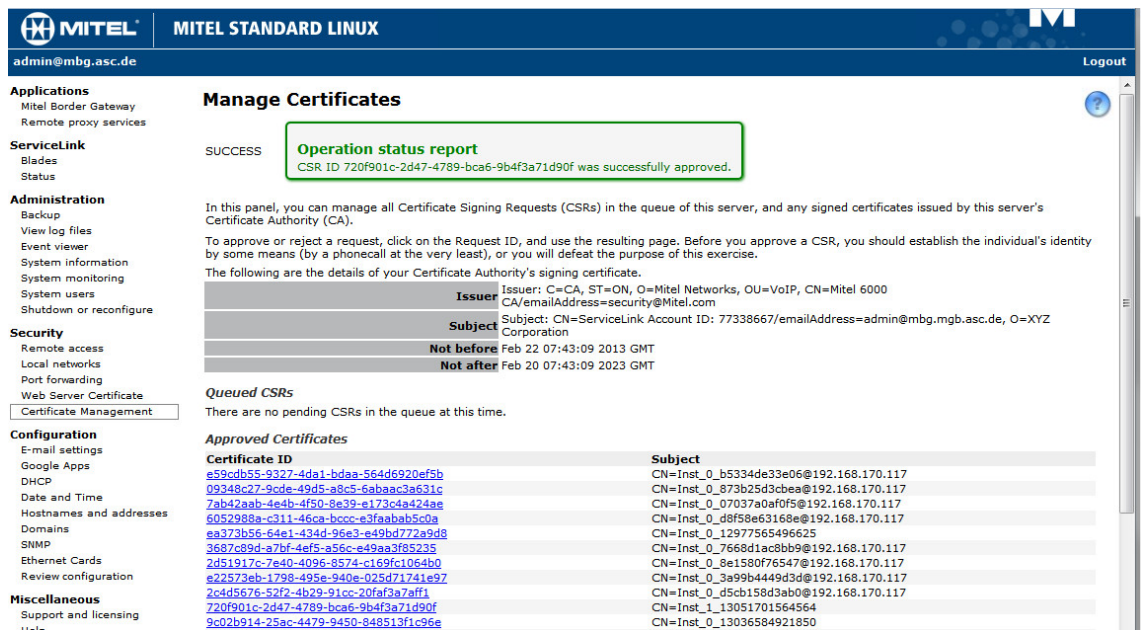


Fig. 23: Success notification for shared certificate

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, shortcuts for the Neo applications are created on the computer 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 of the browser:

https://<System-IP>/SystemConfiguration.

If you have configured customer-specific ports, you must add the port in the URL:

https://<System-IP>:<Port>/SystemConfiguration.

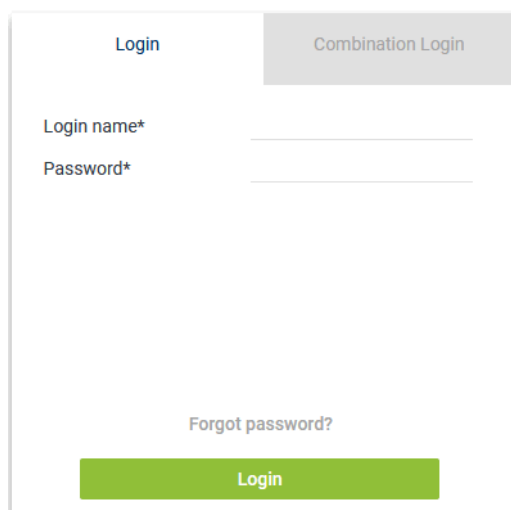


Fig. 24: System Configuration - Web interface

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

Tab. 9: Login data - system provider

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

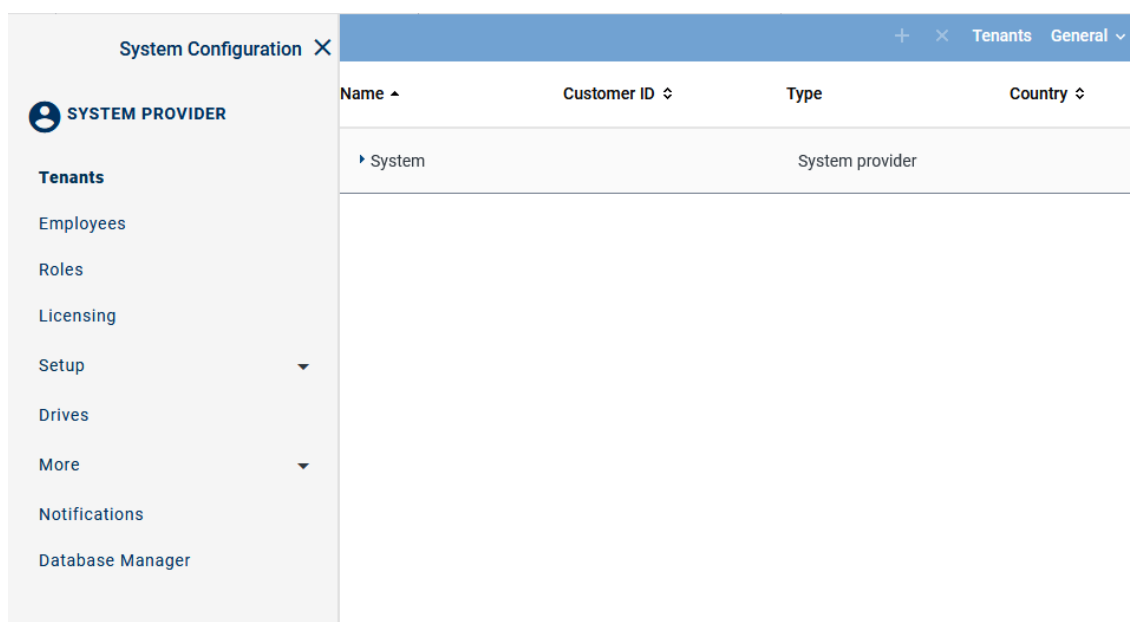


Fig. 25: System Configuration - main view

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:

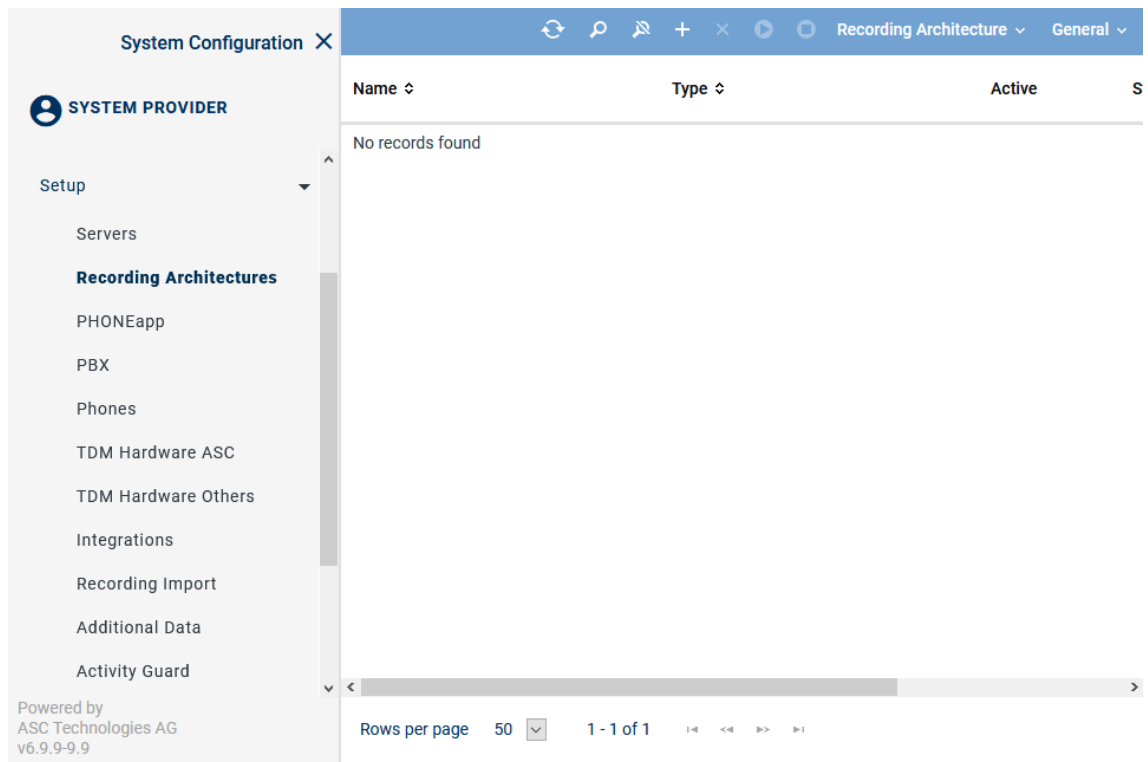




Fig. 26: Recording architectures - main view

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



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








Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 27: Toolbar Recording Architectures module

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


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



For detailed 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.

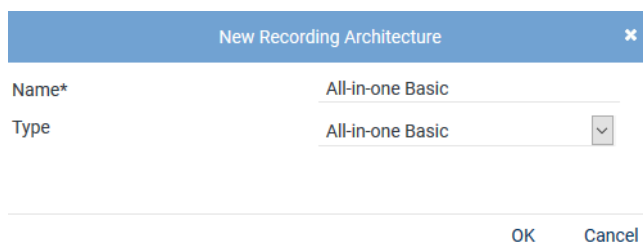
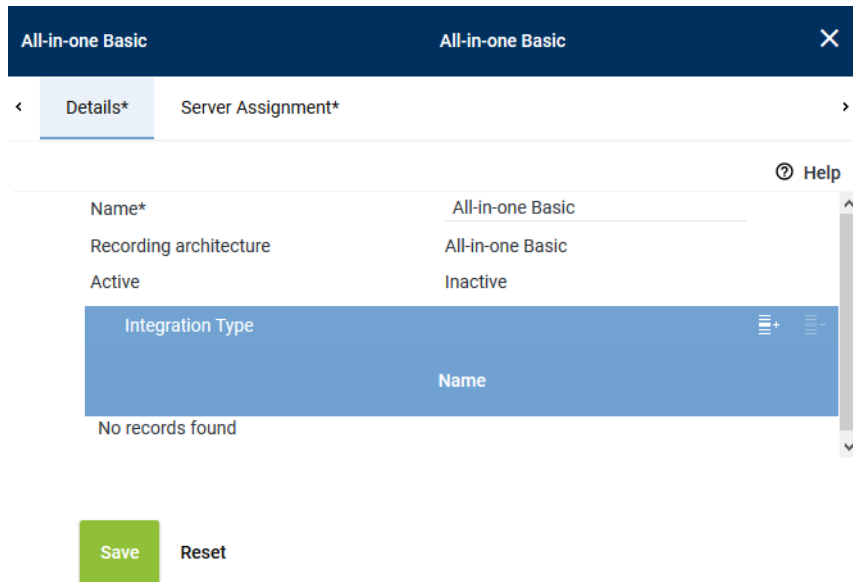


Fig. 28: Create recording architecture - All-in-one Basic Recording

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



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

< Details* Server Assignment* >

Help

Name* All-in-one Basic

Recording architecture All-in-one Basic

Active Inactive


Integration Type

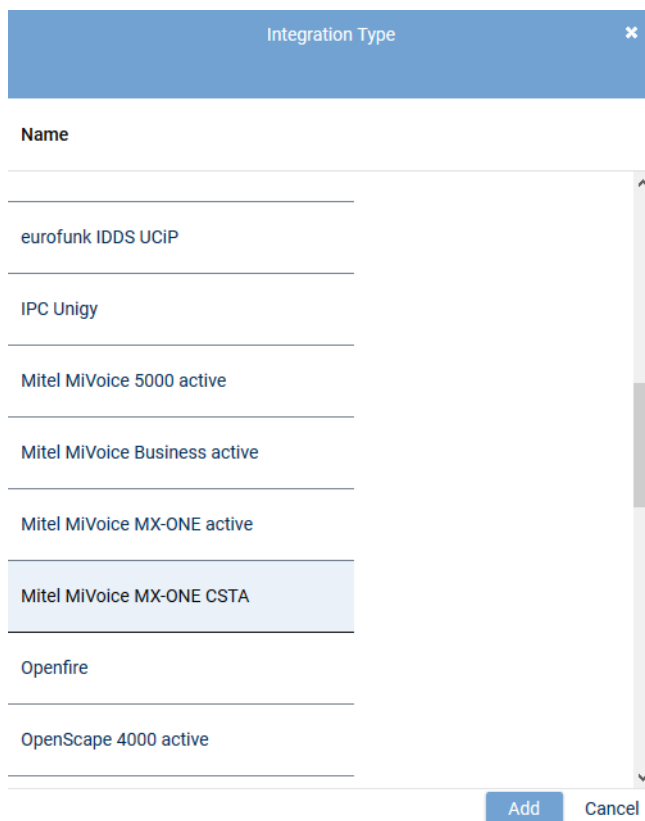
Name
No records found

Save Reset

Fig. 29: Recording architecture - tab Details

Add integration type

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



Integration Type X

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

Add Cancel

Fig. 30: Select integration type



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

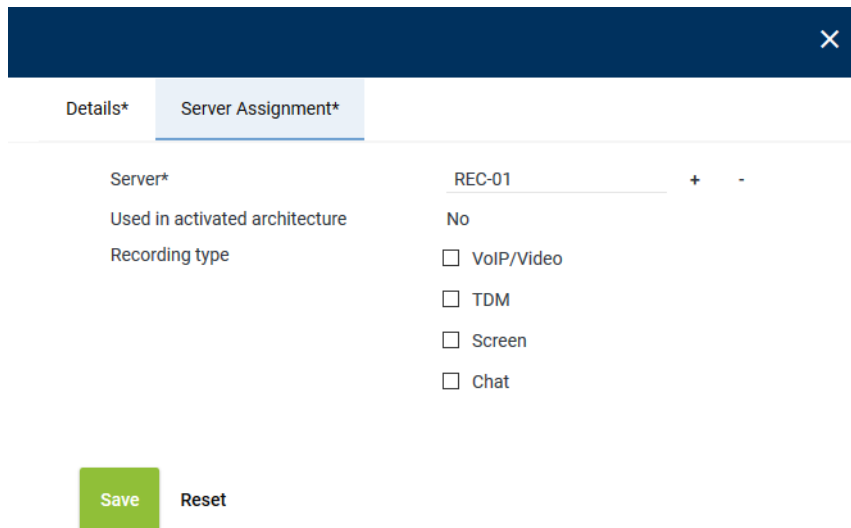


Any number of integration types can be assigned to a recording architecture.

- 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 Basic

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



Details* Server Assignment*

Server* REC-01 + -

Used in activated architecture No

Recording type

☐ VoIP/Video

☐ TDM

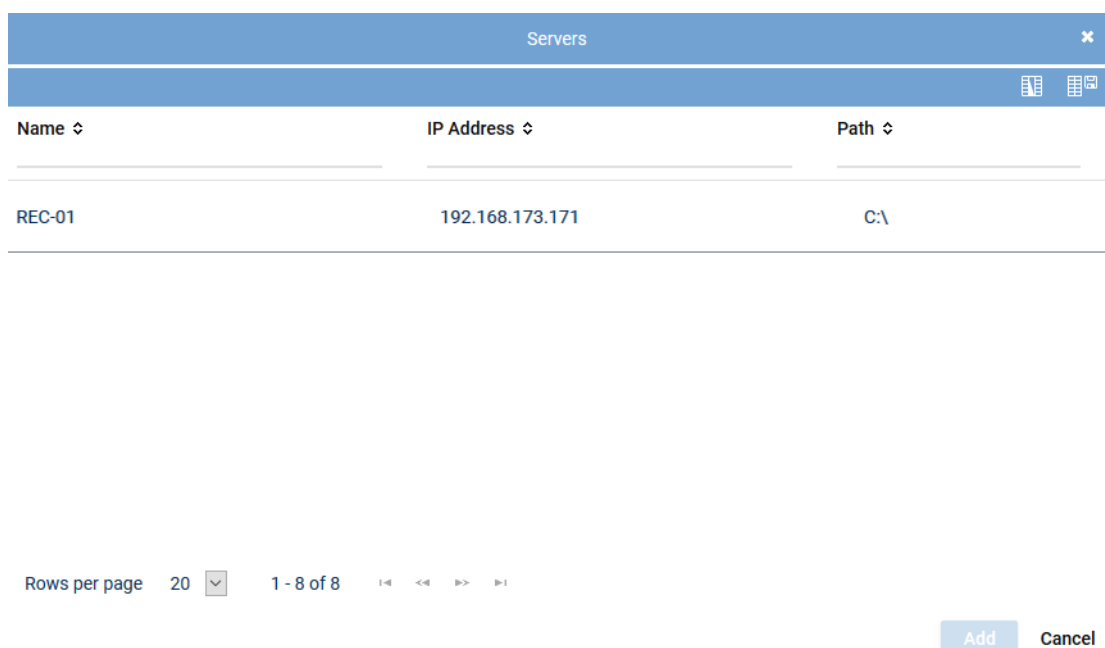
☐ Screen

☐ Chat

Save Reset

Fig. 31: Recording architecture - tab Server Assignment

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



Servers

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

Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 32: Recording architecture - assign server

- Select the respective server.



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

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

Fig. 33: 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. 34: 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:

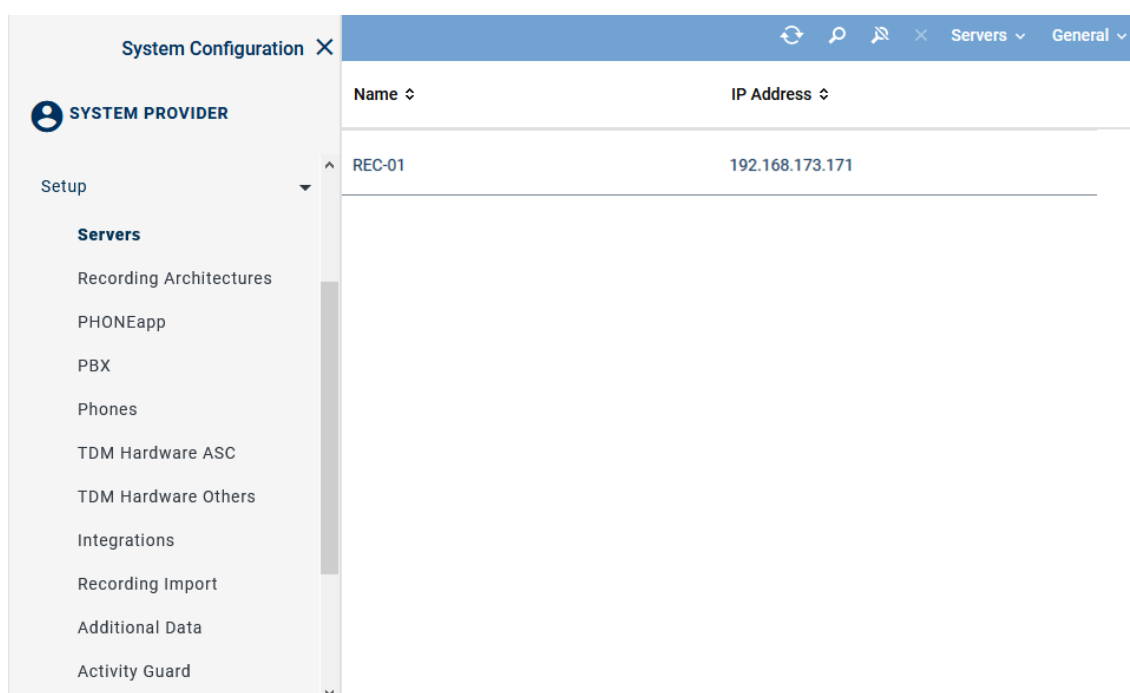


Fig. 35: Servers - main view

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

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

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

Toolbar of the Servers module

The toolbar offers the following functions.

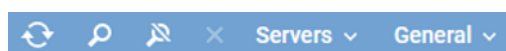







Fig. 36: Toolbar Servers module

	<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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.

<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations", p. 35.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

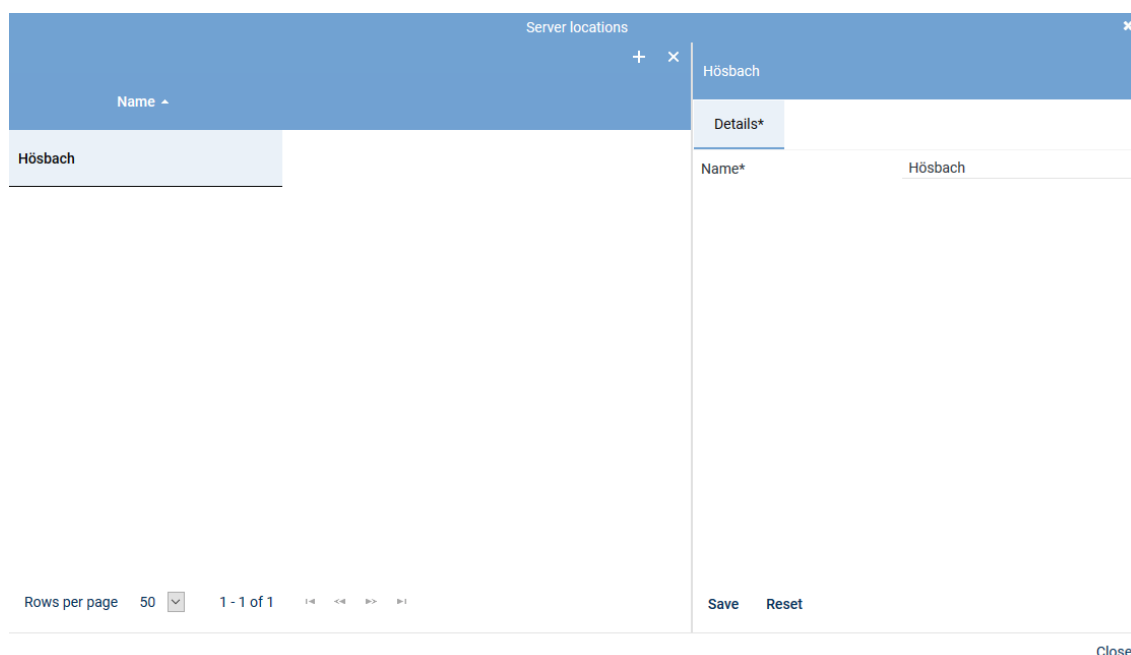



Fig. 37: Add server locations

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

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

Delete server location



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

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

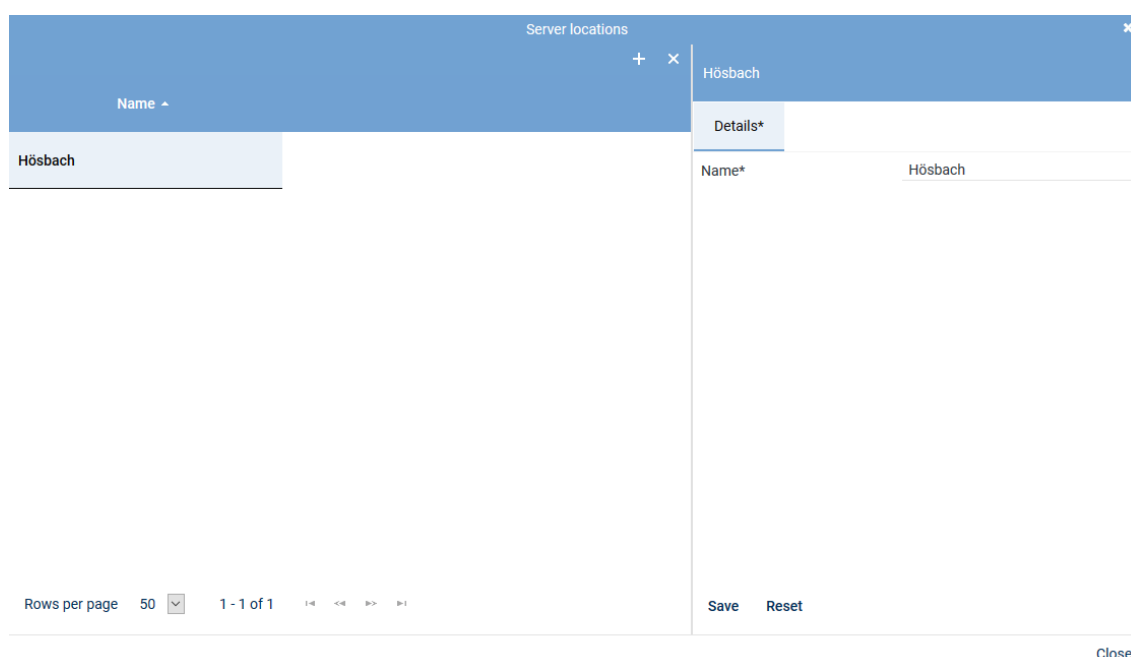



Fig. 38: Delete server location

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. 39: 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. 40: Servers - tab usage

Group field API Server

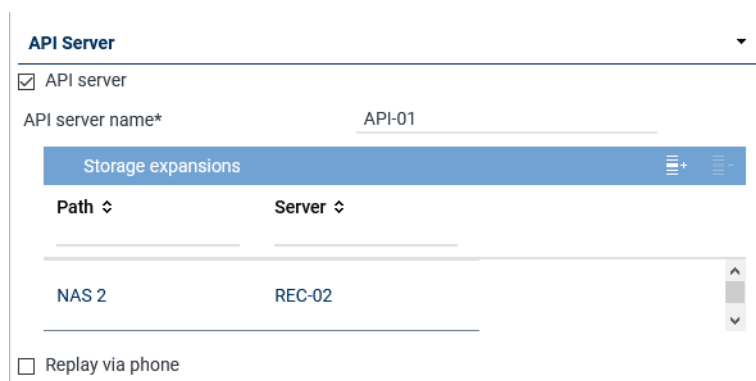




Fig. 41: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 48.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List</i> <i>Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 39. By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.

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>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWER<u>play</u> Pro • Application POWER<u>play</u> Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 46. 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. 42: 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. 43: Group field Audio Analysis

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

Tab. 10: Configure audio analysis

Emotion Detection ×

+

Name ↕

REC-01

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

Add Cancel

Fig. 44: 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/Live Streaming

Recording architecture Please choose... ▼

☐ Neo key management

Fig. 45: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/ Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 46: 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</p>

Parameter	Value/Description
	<p><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"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 43. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 43. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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>

Parameter	Value/Description
	<ul style="list-style-type: none"> Replay server 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. <p>NOTICE! For the export from Neo to Neo, 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"> Recording architecture 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. <p>NOTICE! 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

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

Target Server		
Name ↕	IP Address ↕	
RC-02	192.168.173.176	
REC-04	192.168.173.174	
RC-01	192.168.173.175	
REC-02	192.168.173.172	
CTI-01	192.168.173.177	
REC-03	192.168.173.173	
Rows per page 20 ▾ 1 - 6 of 6		
		 

Fig. 47: 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. 48: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 45.

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

Tab. 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. 49: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 38](#).

- 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. 50: Group field Virtualization

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

Tab. 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* <small>(max. 18 characters)</small>	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. 51: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<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>NOTICE! The port range must not have less than 64 ports.</p>

<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

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

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 52: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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. 53: Servers module - tab Key Management

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

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

In case of an error ... automatically

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

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

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



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



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

Tab Keystore/Virtualization

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

In this tab, you can configure the connection data 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*

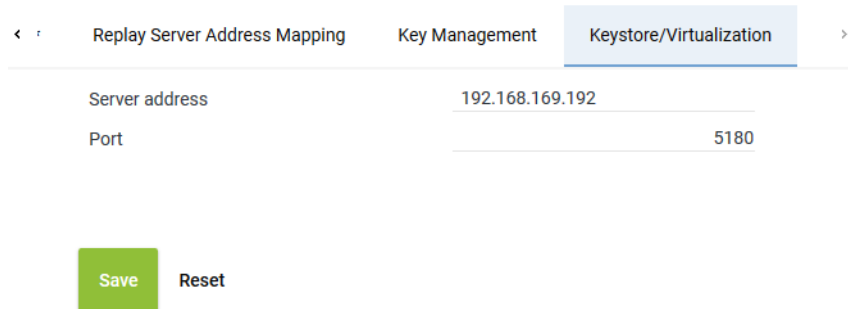
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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

Fig. 54: Servers module - tab Keystore/Virtualization

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

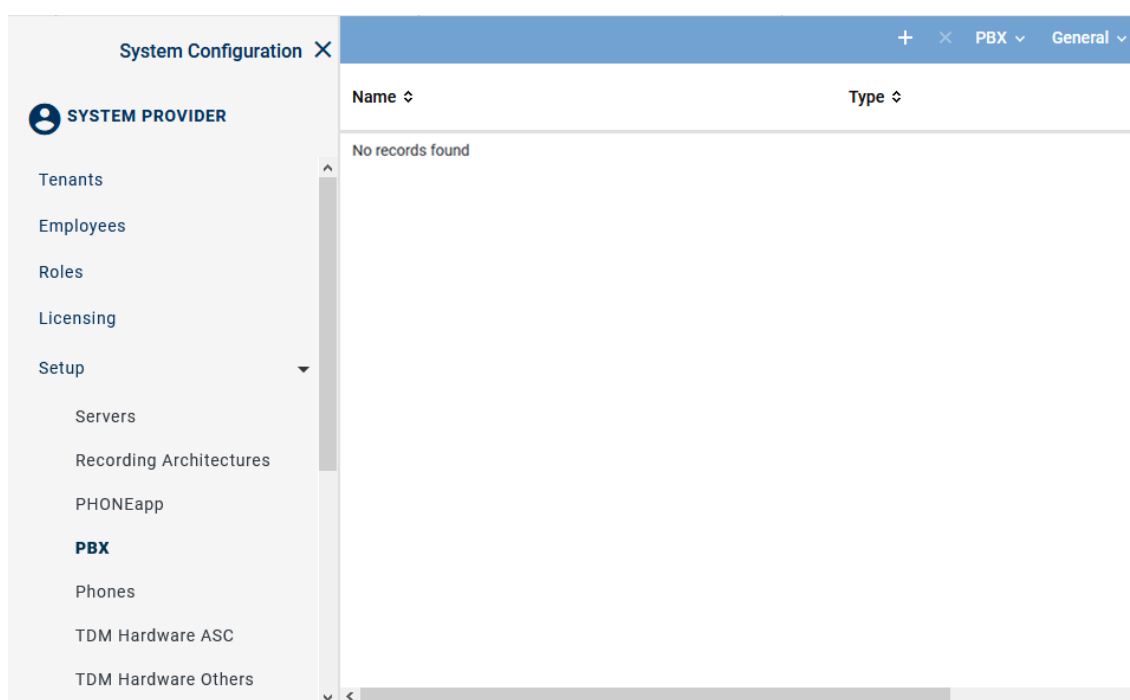




Fig. 55: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 56: 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>Administratre Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

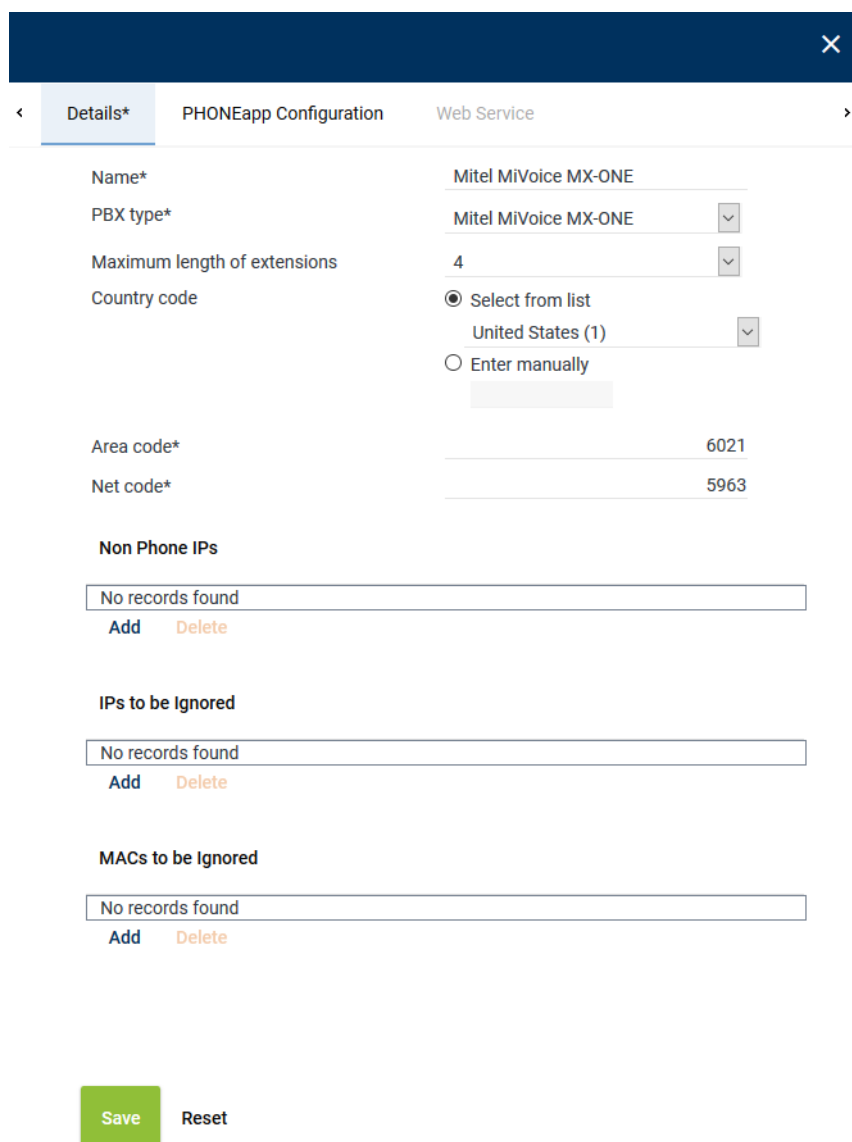


Fig. 57: Create new PBX - tab Details

- 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 PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka <i>094</i>.

Parameter	Value/Description
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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

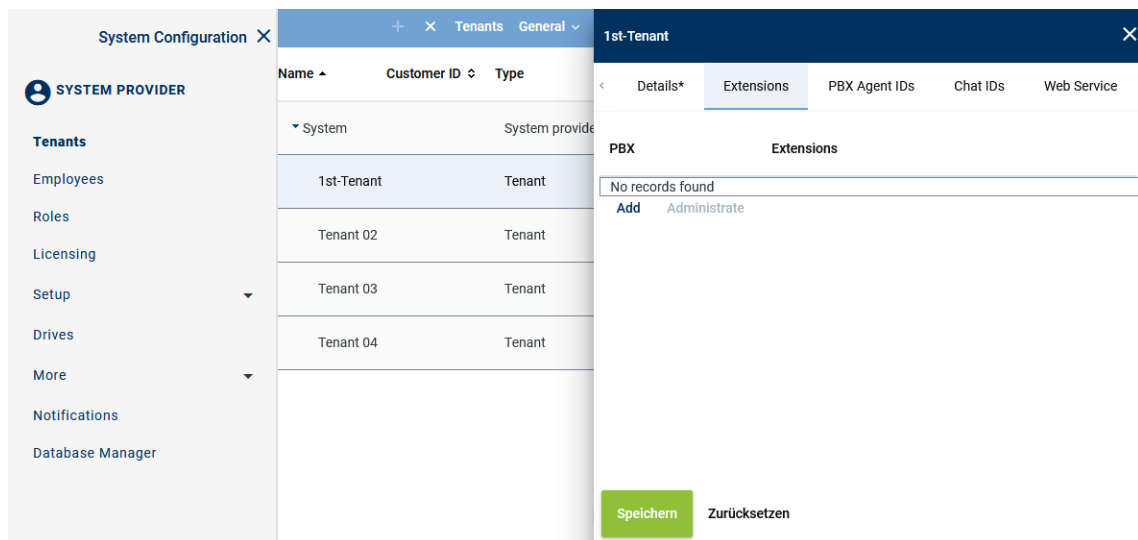


Fig. 58: Tenants - main view - tab Extensions

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. 59: 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"> ZIP TXT CSV <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA3) - Neo 7.x Rev. 2

56 / 474

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.

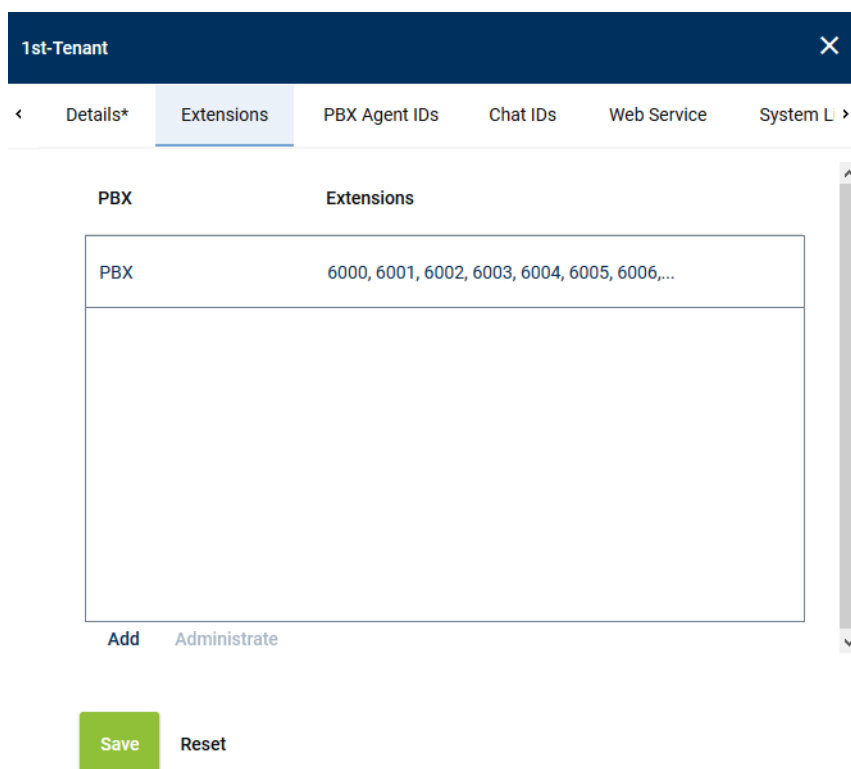


Fig. 60: Remove extensions

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. 61: 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.

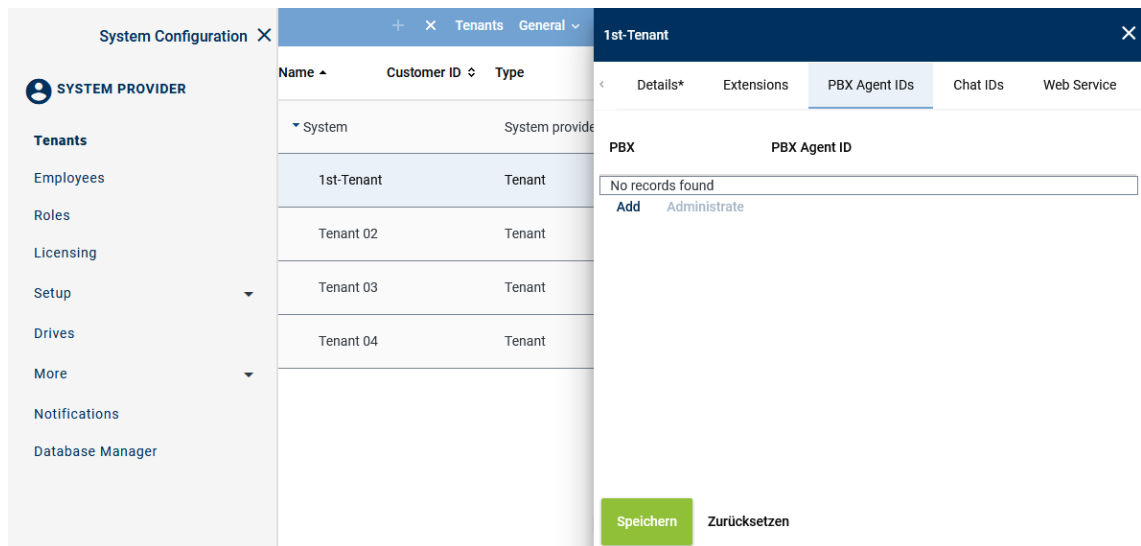


Fig. 62: Tenants - main view - tab PBX Agent ID

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:

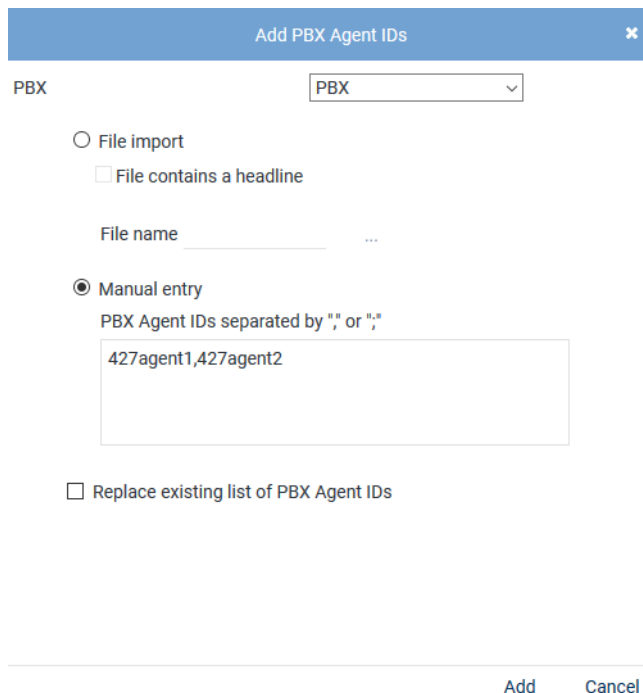




Fig. 63: Assign PBX Agent IDs to tenants

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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 64: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 65: Additional Data module main view

2. Select a data set

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

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. 66: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 67: Additional data - configure availability

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



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

7.3.2.1.6 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:

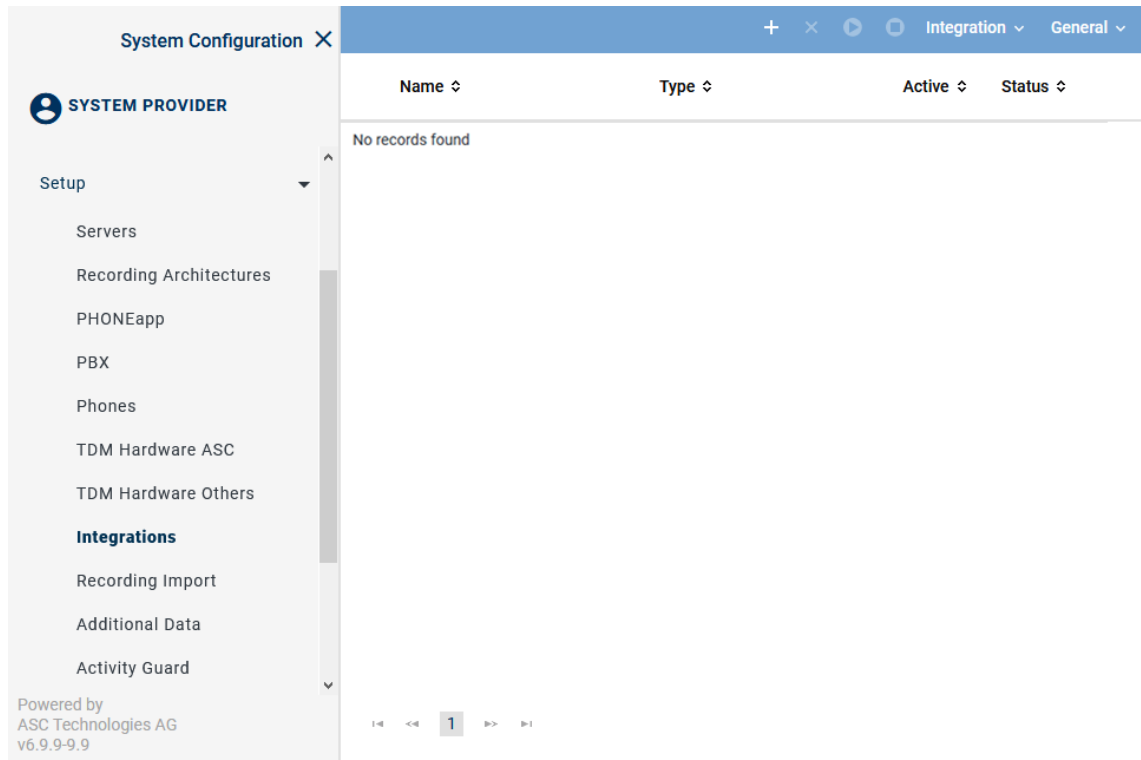




Fig. 68: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 69: Toolbar Integrations module

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

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

Import grammar

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

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

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

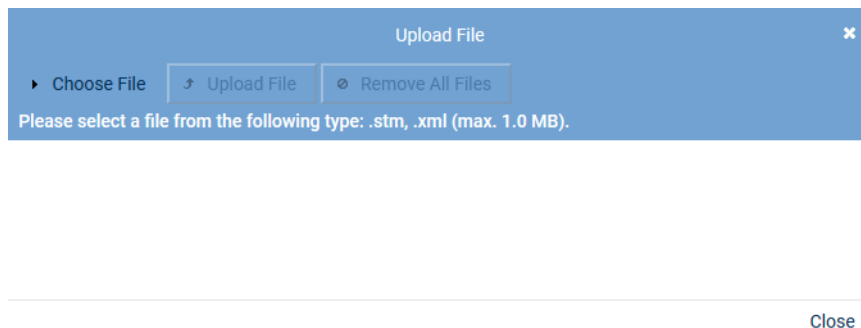


Fig. 70: Choose file

- 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*.

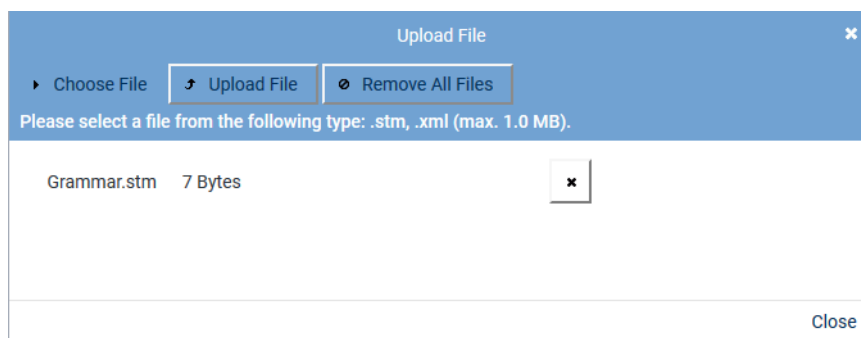



Fig. 71: Upload grammar

- 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. 72: Create integration type

2. Enter the following parameters:

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

Tab. 16: Create integration type

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

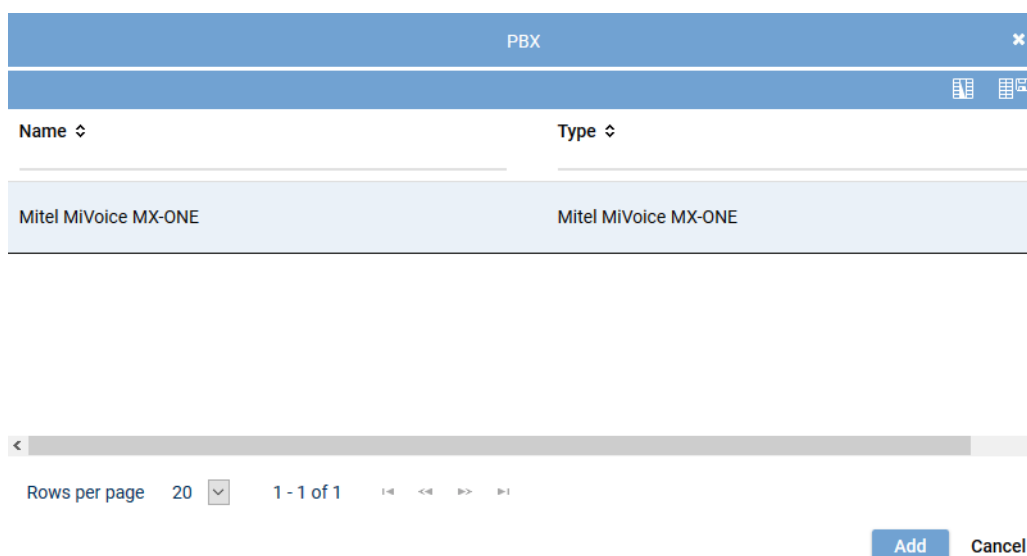


Fig. 73: Integrations - select PBX

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

Assign recording architecture for All-in-one Basic

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



Fig. 74: 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. 75: 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.

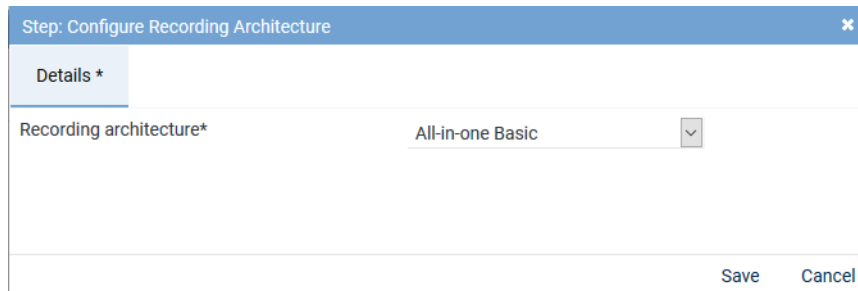



Fig. 76: Configuration step - Configure Recording Architecture

- 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. 77: 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. 78: 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. 79: Configure connection data

Configure Connection
✕

PBX IP address*	<input type="text" value="192.168.170.219"/>
PBX CSTA port*	<input type="text" value="8882"/>
Transport Layer Security (TLS)	<input type="checkbox"/>
<input checked="" type="checkbox"/> Activate authentication	
Application ID*	<input type="text" value="1234"/>
Password*	<input type="password" value="••••••••••••••"/>

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

Fig. 80: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .
<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 chapter "Configure CSTA server", p. 14 .
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See chapter "Configure CSTA server", p. 14 .

Tab. 18: Configure connection data

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

Group field Additional Data

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

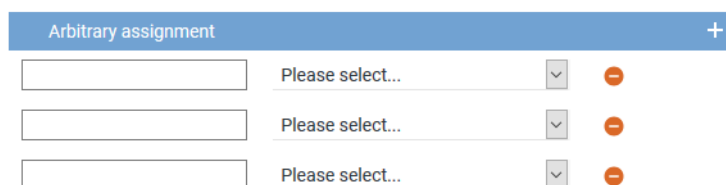



Fig. 81: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 82: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an MBG or if the regular expression does not apply for the respective phone type, recording runs via the MBG/SRC.

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 83: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

1. Select the tab **MBG** to configure the connection data for recording by means of MiVoice Border Gateway.

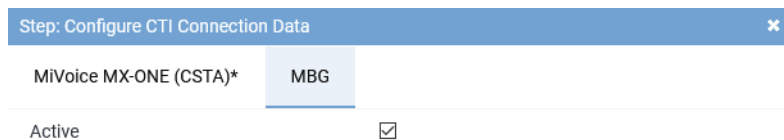


Fig. 84: Activate CTIconnect connection data for MBG

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.

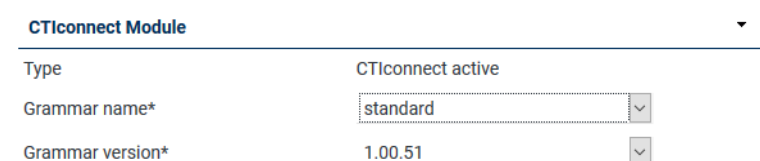


Fig. 85: Configure CTIconnect module

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.




Fig. 86: Group field Connection Data

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

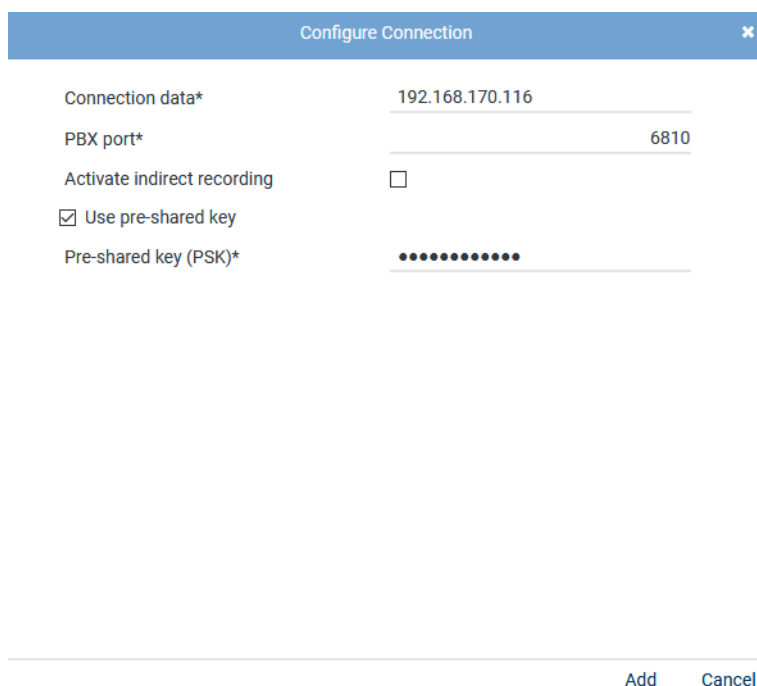


Fig. 87: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , 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 MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

Tab. 20: Configure connection data



A maximum of 20 MBG connections are possible.

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

Group field Additional Data MBG

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

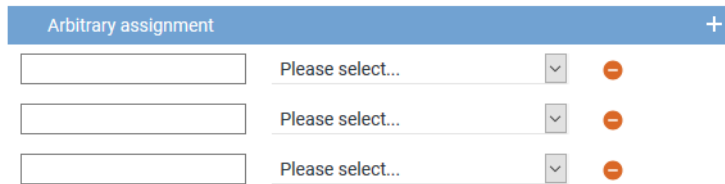



Fig. 88: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.




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



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

Configure monitor points 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.

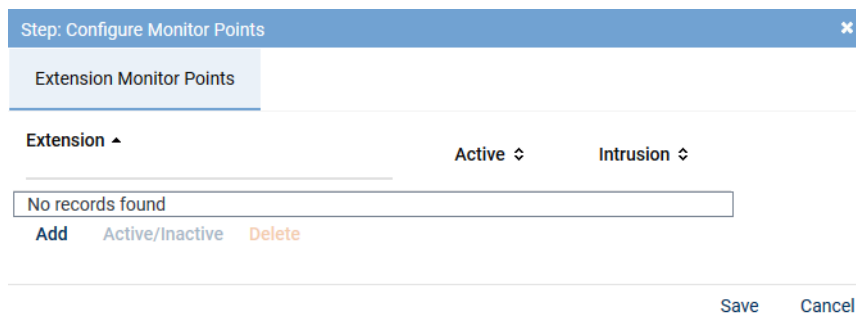


Fig. 89: Configuration step - configure monitor points

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.

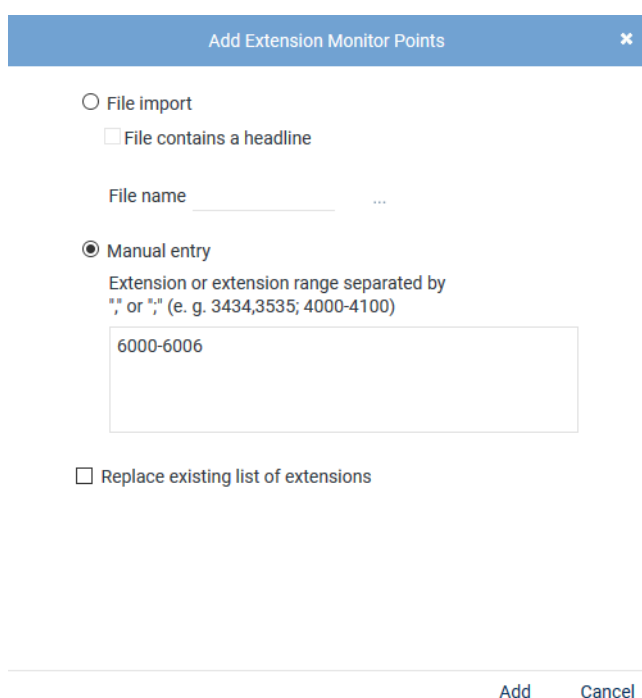






Fig. 90: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button  behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>).
File contains a headline	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.</p>
File name	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button  behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p>

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 ✕		
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. 91: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at

	the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Delete	To delete extension monitor points, select the respective extension in the list and click on the button <i>Delete</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Intrusion	<p>To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column <i>Intrusion</i>.</p> <p><input checked="" type="checkbox"/> = Intrusion feature has been activated.</p> <p><input type="checkbox"/> = Intrusion feature has not been activated.</p>


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



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

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 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. 92: 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. 21: Global recording settings

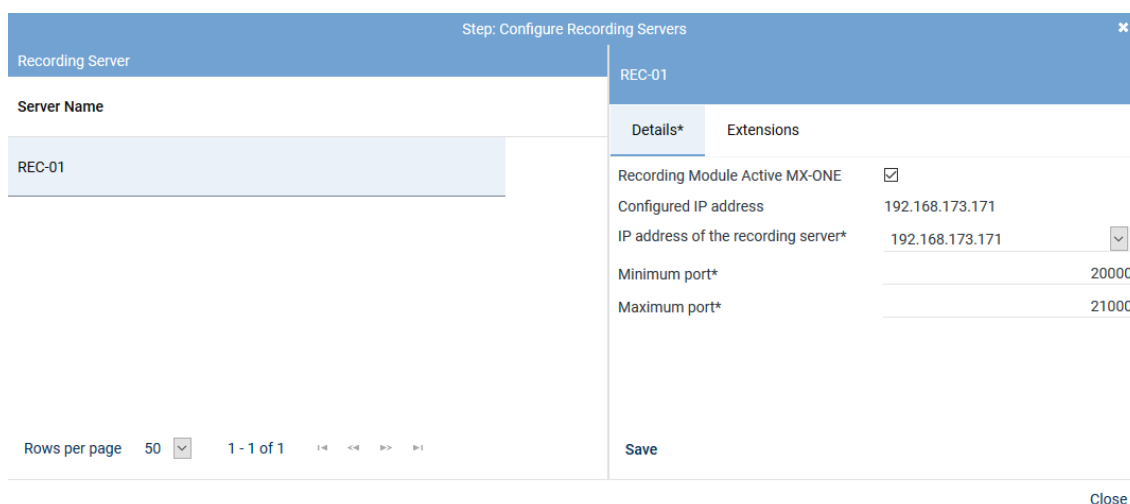
- Click on the button **Save** to apply the settings and to finish this configuration step.



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.



Step: Configure Recording Servers

Recording Server	REC-01
Server Name	REC-01
Details*	Recording Module Active MX-ONE <input checked="" type="checkbox"/> Configured IP address 192.168.173.171 IP address of the recording server* 192.168.173.171 Minimum port* 20000 Maximum port* 21000

Rows per page 50 1 - 1 of 1 Save Close

Fig. 93: Configuration step - Configure recording servers

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

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

Tab. 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 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. 94: 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. 23: Configure CTIconnect module

Group field Connection Data

- 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. 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

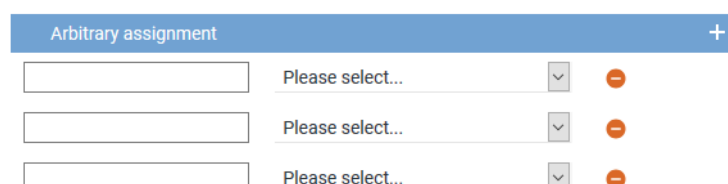



Fig. 95: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

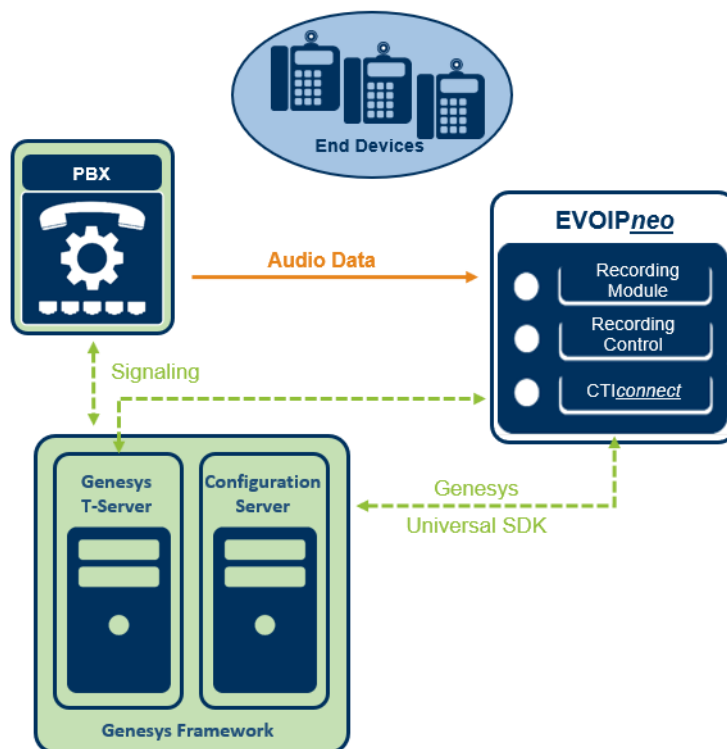


Fig. 96: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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. 97: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

Parameter	Value/Description
<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 CTIconnect 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 CTIconnect 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.

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

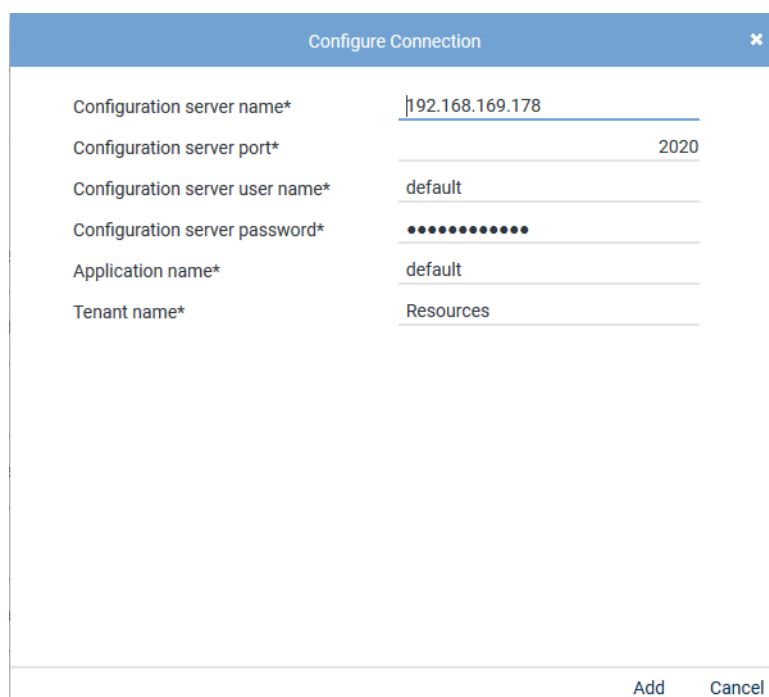


Fig. 98: Configure connection data

- 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.
<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.

Parameter	Value/Description
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

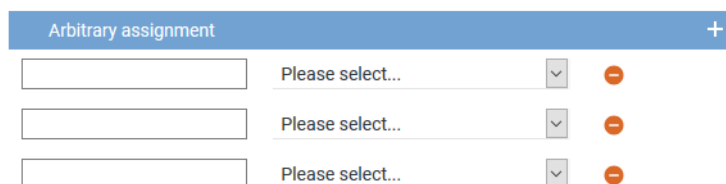




Fig. 99: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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.

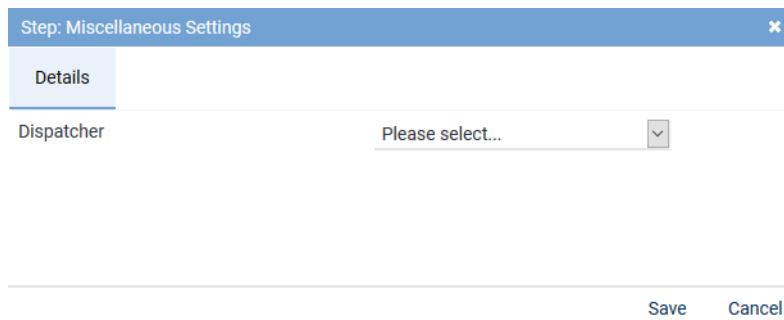


Fig. 100: Configure miscellaneous settings

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. 101: 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. 102: 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.

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







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

Fig. 103: Deactivate integration

2. 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.

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

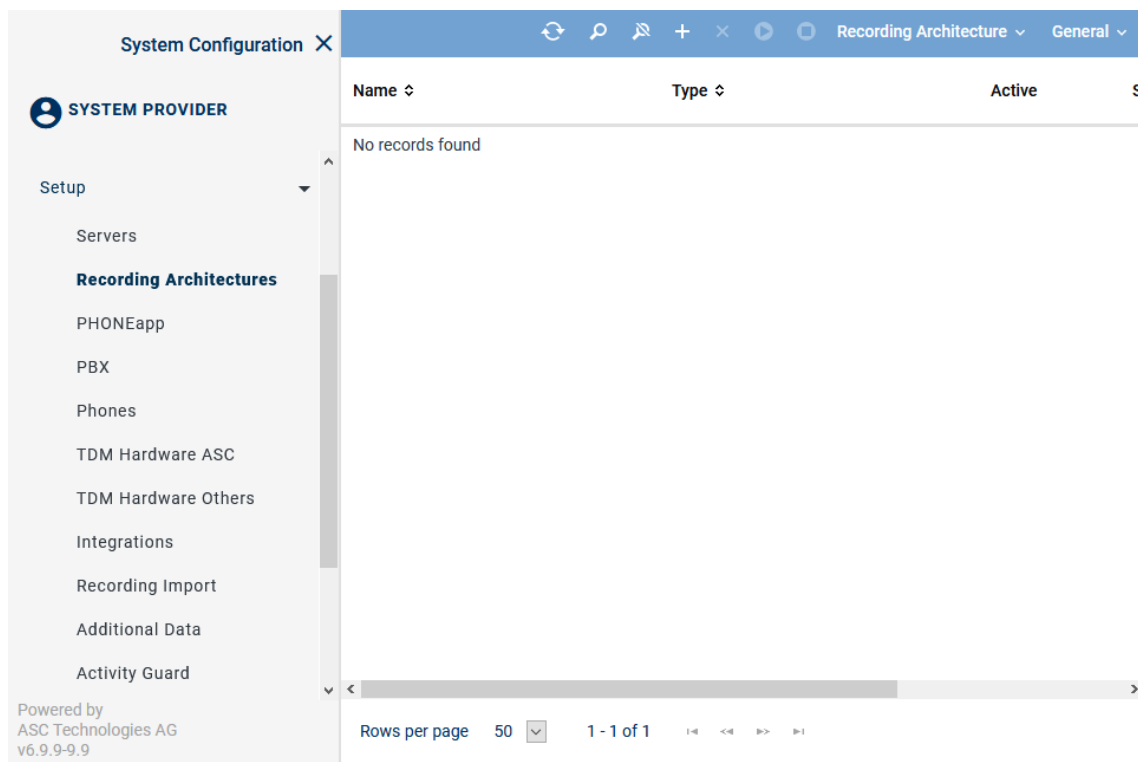




Fig. 104: Recording architectures - main view

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


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








Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 105: Toolbar Recording Architectures module

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

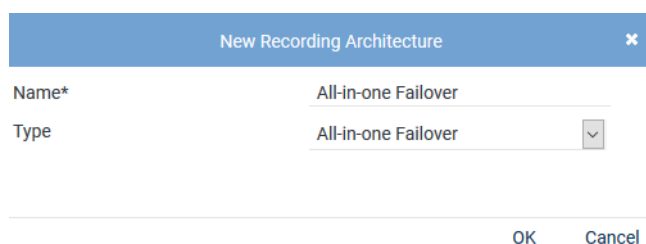


For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

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.



New Recording Architecture

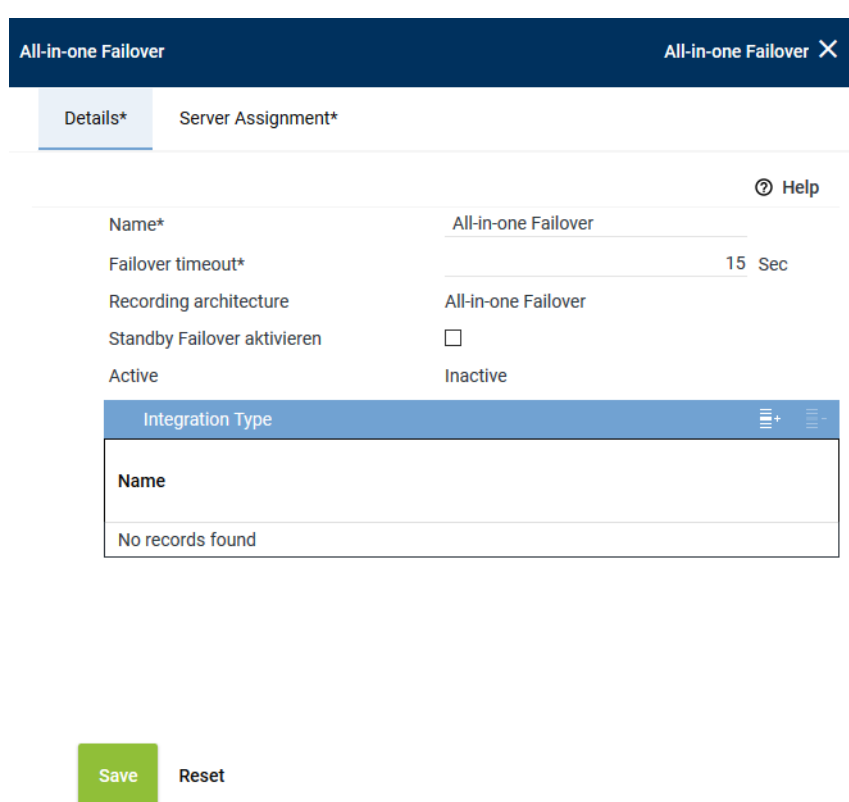
Name* All-in-one Failover

Type All-in-one Failover

OK Cancel

Fig. 106: Create recording architecture - All-in-one Failover

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



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

Details* Server Assignment*

Help

Name* All-in-one Failover

Failover timeout* 15 Sec

Recording architecture All-in-one Failover

Standby Failover aktivieren ☐

Active Inactive

Integration Type

Name
No records found

Save Reset

Fig. 107: 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. 447](#).

Failover timeout	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. NOTICE! Check these parameters after an update and set the timeout to 15 seconds, if required.
Activate standby failover	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.


NOTICE! There is no check whether the primary database is working properly before switching back. As a result it is possible that both databases are in an undefined state.

NOTICE! After switching back to the original primary server from the standby server, this option is deactivated. If the switching process is supposed to be carried out automatically in the event of a new error, you must activate this option again.

Active

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.

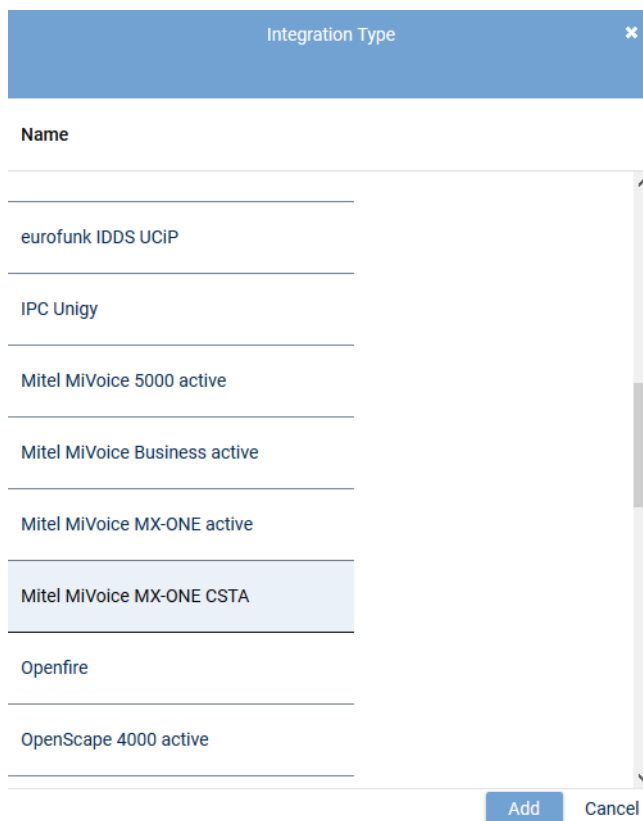


Fig. 108: Select integration type



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	<input type="checkbox"/> VoIP/Video		
	<input type="checkbox"/> TDM		
	<input type="checkbox"/> Screen		
	<input type="checkbox"/> Chat		

Save

Reset

Fig. 109: Recording Architecture - tab Server Assignment

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

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

Fig. 110: Recording Architecture - assign server - example


3. Select the *primary* server.



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

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

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

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

Recording type

☒ VoIP/Video

☒ TDM

☒ Screen

☒ Chat



 




Fig. 111: 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. 112: 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. 447](#).



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:

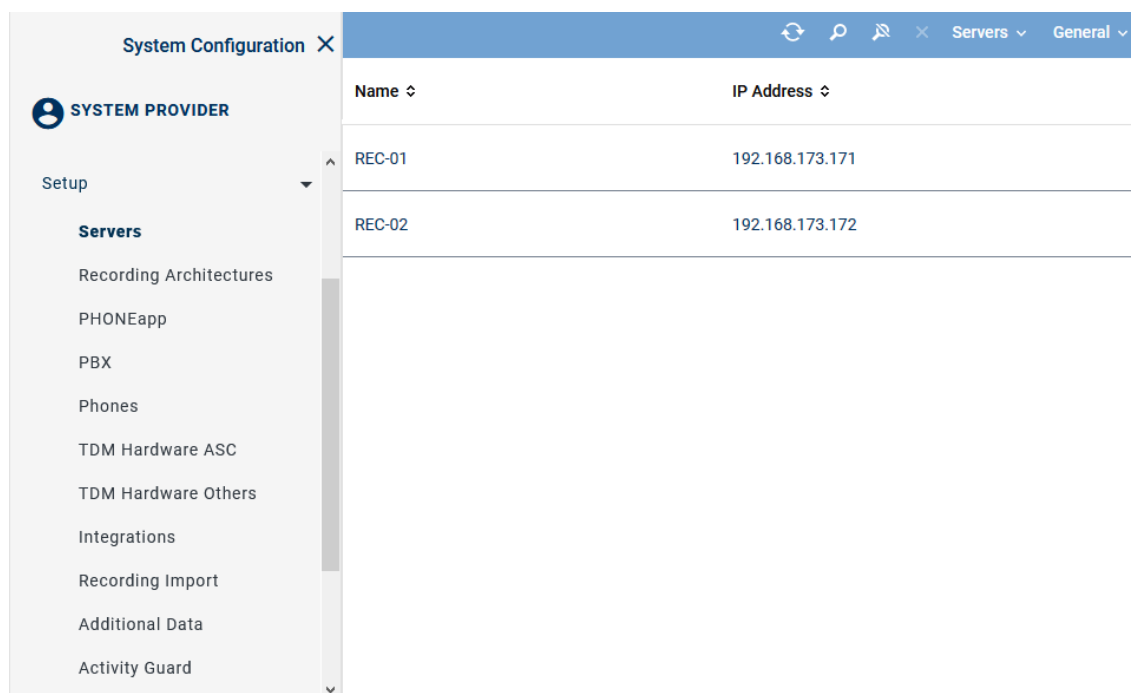


Fig. 113: Servers - main view

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

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

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

Toolbar of the Servers module

The toolbar offers the following functions.

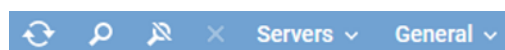








Fig. 114: Toolbar Servers module

	<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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.
<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations", p. 98 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



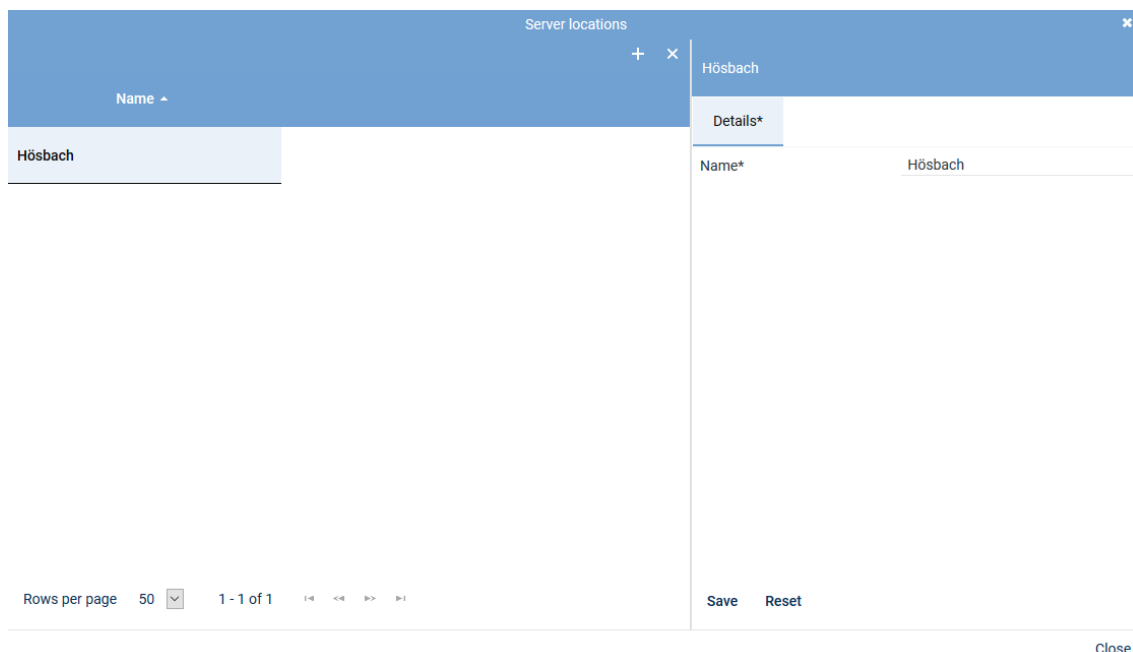
For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

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 "+" icon and a "x" icon. The main area is divided into two panes. The left pane contains a table with a single row: "Hösbach". The right pane has a tab labeled "Details*" and a form field labeled "Name*" with the value "Hösbach". At the bottom of the window, there is a footer area with "Rows per page 50" and "1 - 1 of 1" on the left, and "Save" and "Reset" buttons on the right. A "Close" button is located at the bottom right of the window.

Fig. 115: Add server locations

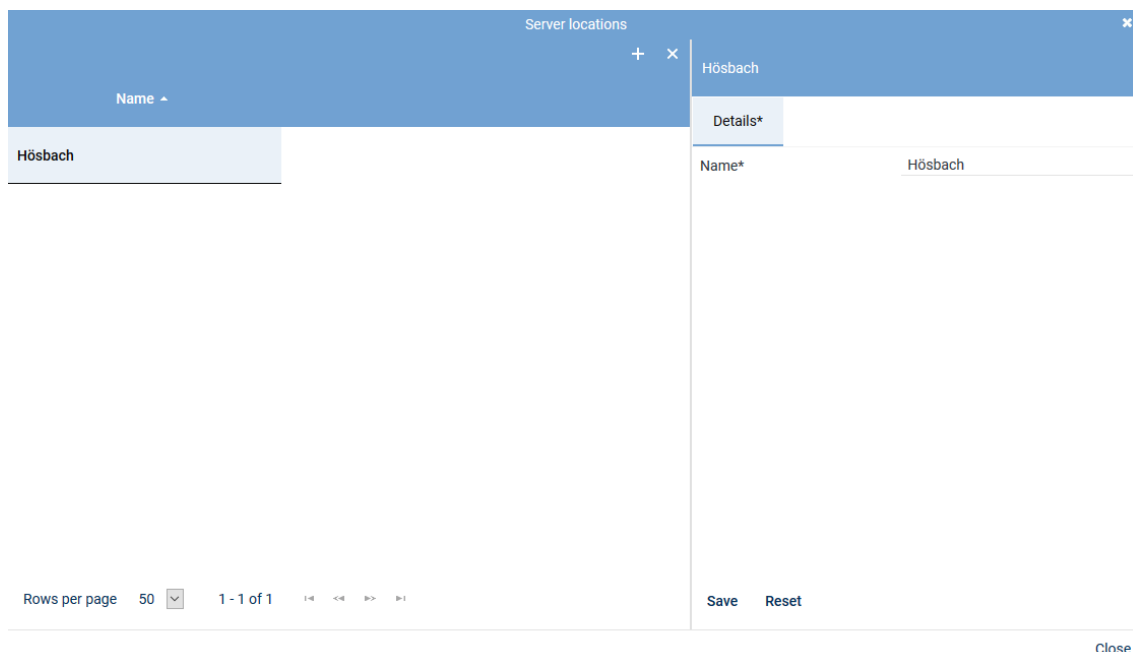
2. Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
3. Enter the name of the location on the right side in the tab *Details*.
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last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



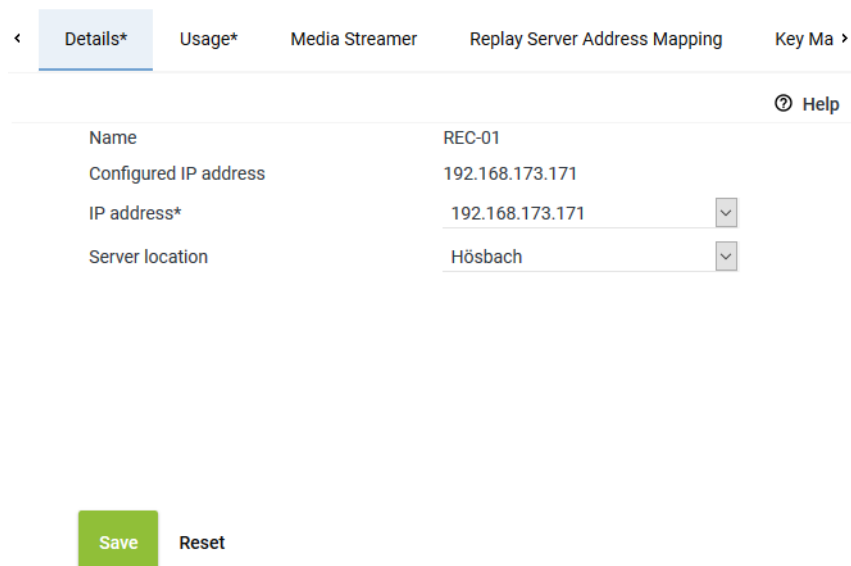
The screenshot shows a window titled "Server locations" with a close button (x) in the top right corner. Below the title bar is a table with one row containing the name "Hörsbach". To the right of the table is a "Details*" tab. Below the tab, there is a form with a label "Name*" and a text input field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

Fig. 116: 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 corner. Below the title bar is a tabbed interface with tabs: "Details*", "Usage*", "Media Streamer", "Replay Server Address Mapping", and "Key Ma". The "Details*" tab is active. Below the tabs is a form with the following fields:

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

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

Fig. 117: 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.

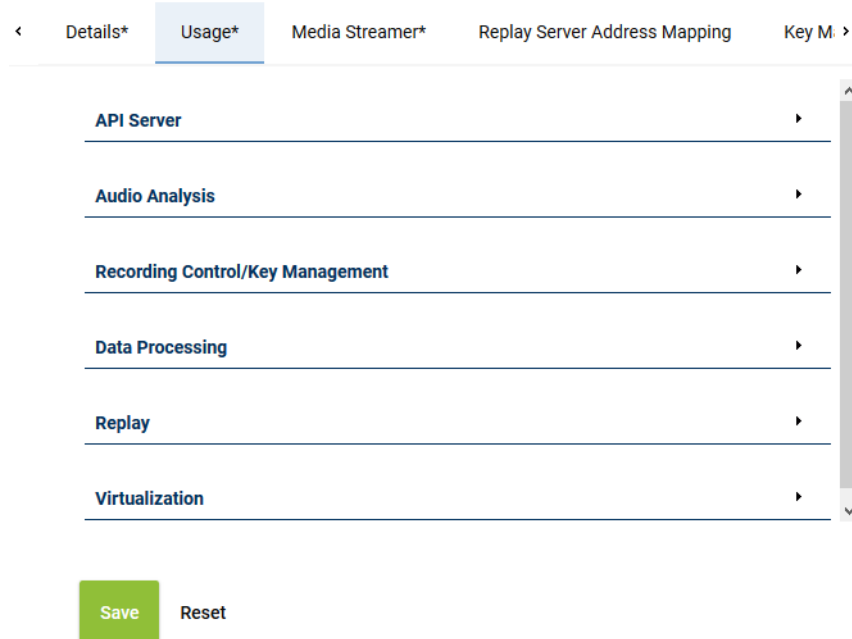


Fig. 118: Servers - tab usage

Group field API Server

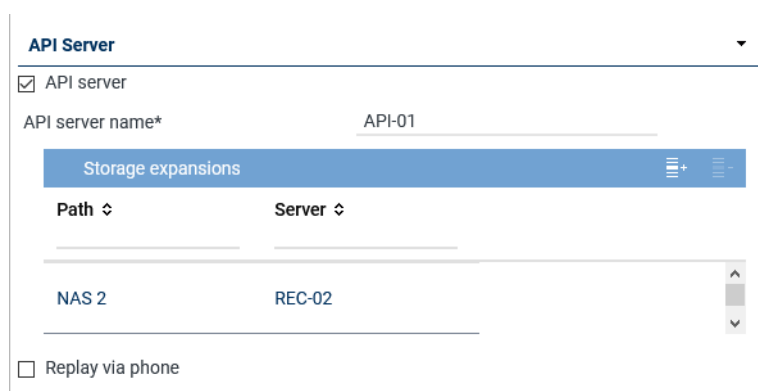




Fig. 119: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 111.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 103. • By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 110. 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. 120: 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

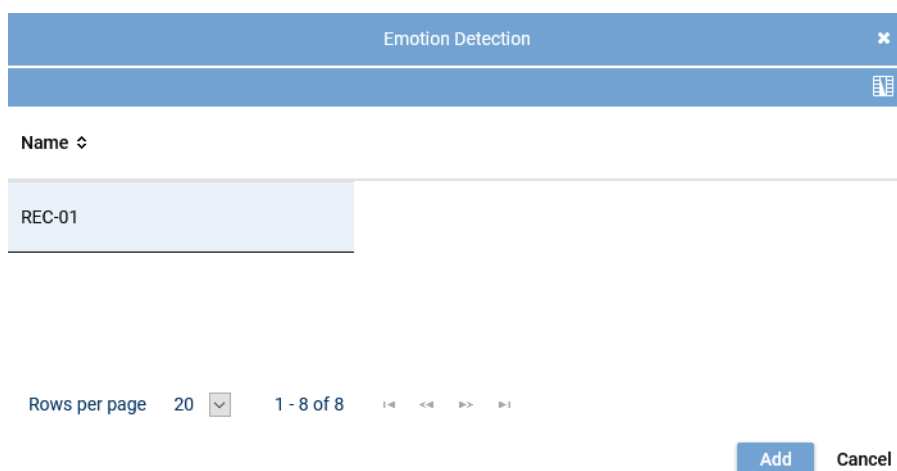
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 121: Group field Audio Analysis

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

Tab. 27: Configure audio analysis



Emotion Detection

Name ↕

REC-01

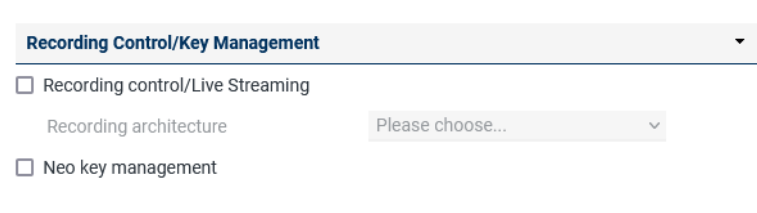
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 122: 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/Live Streaming

Recording architecture Please choose...

☐ Neo key management

Fig. 123: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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 0:00 ▼

End 4:00 ▼

Receives data from

Only Replay

Name	Only Replay
No records found	

☐ Archiving



☒ Export





Replay server Please choose... ▼

☒ Import

Recording architecture All-in-one Basic ▼

Fig. 124: 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"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 107. By clicking on the icon  (Remove), you can remove target servers from the list. <p>NOTICE! 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"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 107. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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"> <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. <p>NOTICE! For the export from Neo to Neo, 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"> <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.

Parameter	Value/Description
	NOTICE! 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

Rows per page: 20 1 - 6 of 6

Add Cancel

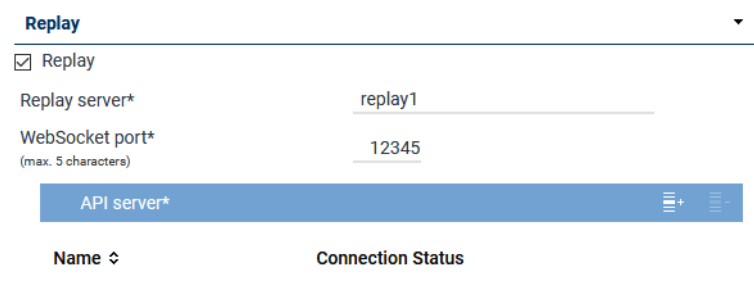
Fig. 125: Select server



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. 126: 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 API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 108. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

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. 127: 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. 128: 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"> • <code>licensing.asc.de</code> If you enter this domain, there is no key management.

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

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 <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. 129: Servers module - tab Media Streamer

- Enter the following parameters:

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

	If no PBX has been created in the system yet, you can create a PBX via the blue bar <i>PBX</i> .
<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 8000.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</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>NOTICE! The port range must not have less than 64 ports.</p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered. <input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

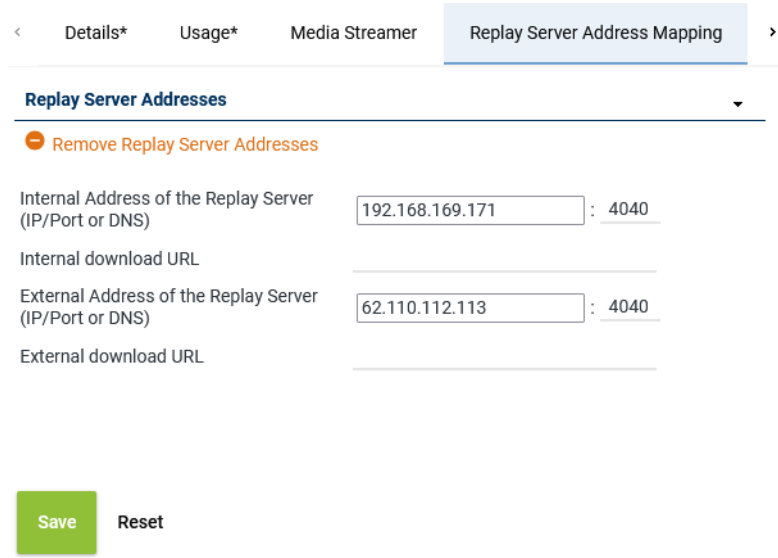



Fig. 130: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

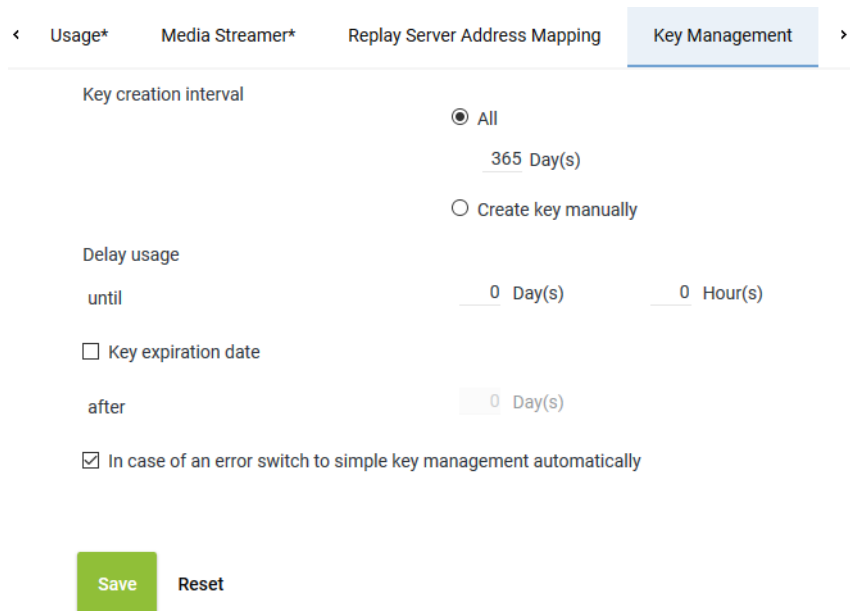


Fig. 131: Servers module - tab Key Management

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>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo 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 Neo 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 Neo 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*

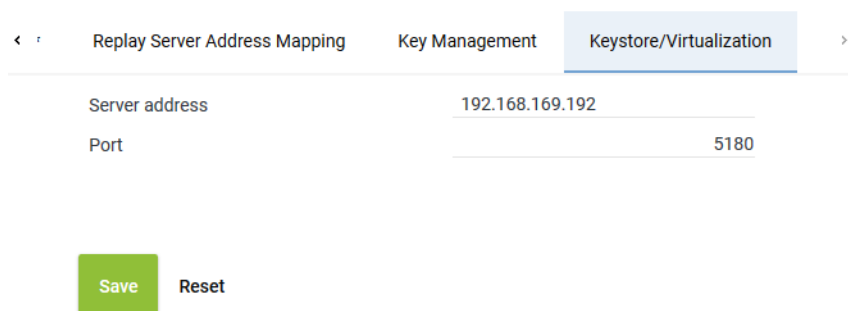
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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' (which is selected). Below the tabs, there are two input fields: 'Server address' with the value '192.168.169.192' and 'Port' with the value '5180'. At the bottom, there are two buttons: 'Save' (green) and 'Reset' (gray).

Fig. 132: Servers module - tab Keystore/Virtualization

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

	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*.

7.3.2.2.3 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.

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

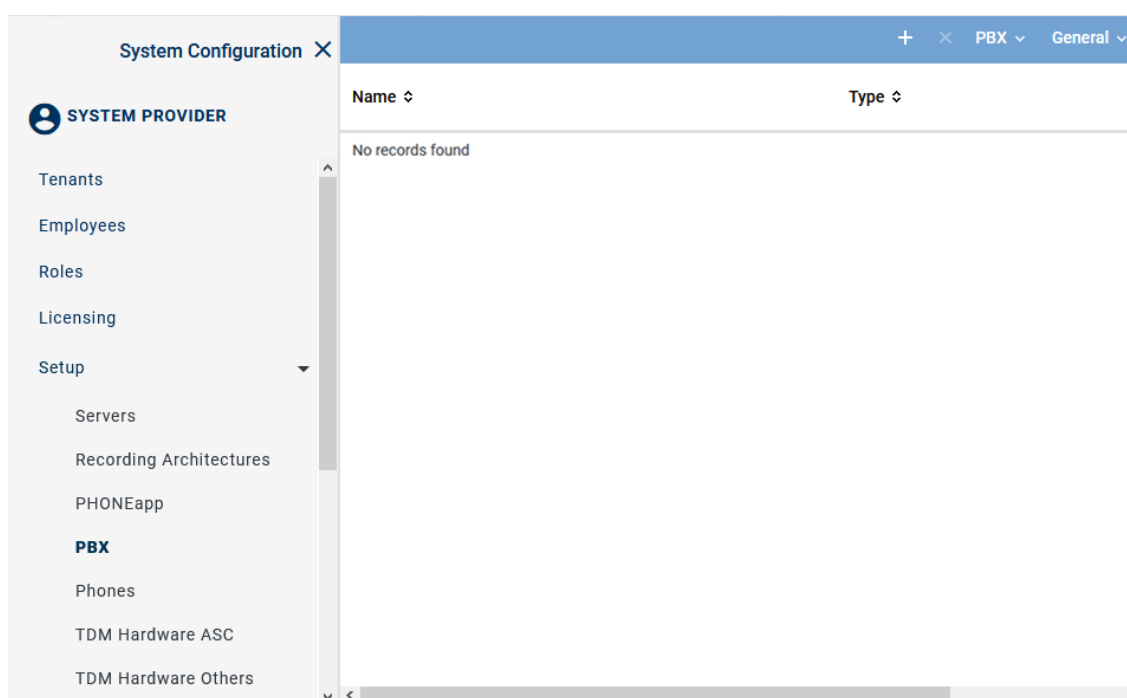


Fig. 133: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

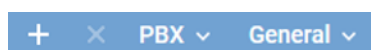




Fig. 134: Toolbar PBX module


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

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



For detailed 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. 135: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

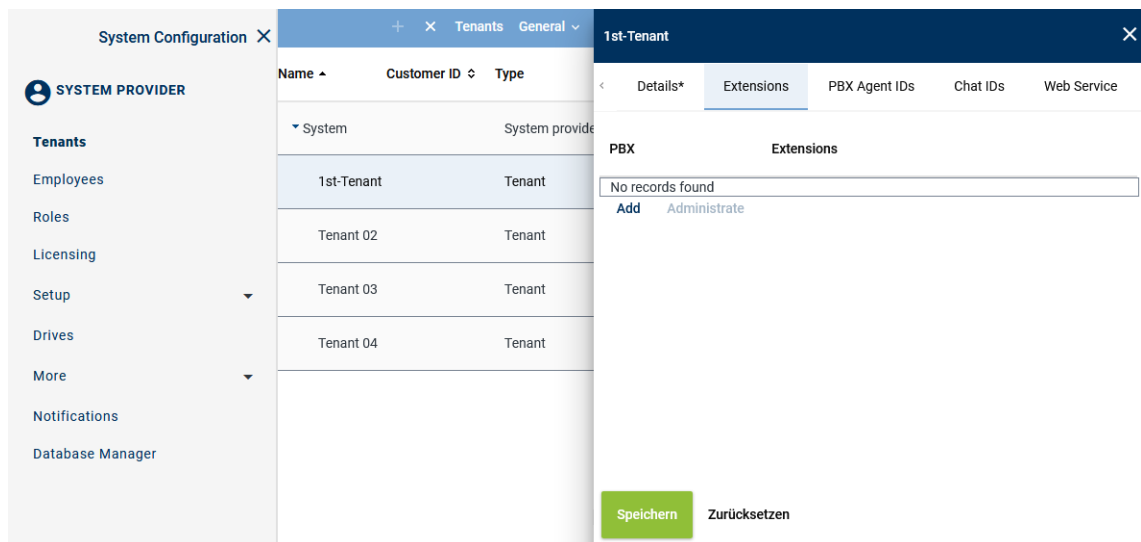


Fig. 136: Tenants - main view - tab Extensions

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. 137: 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"> ZIP TXT CSV <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

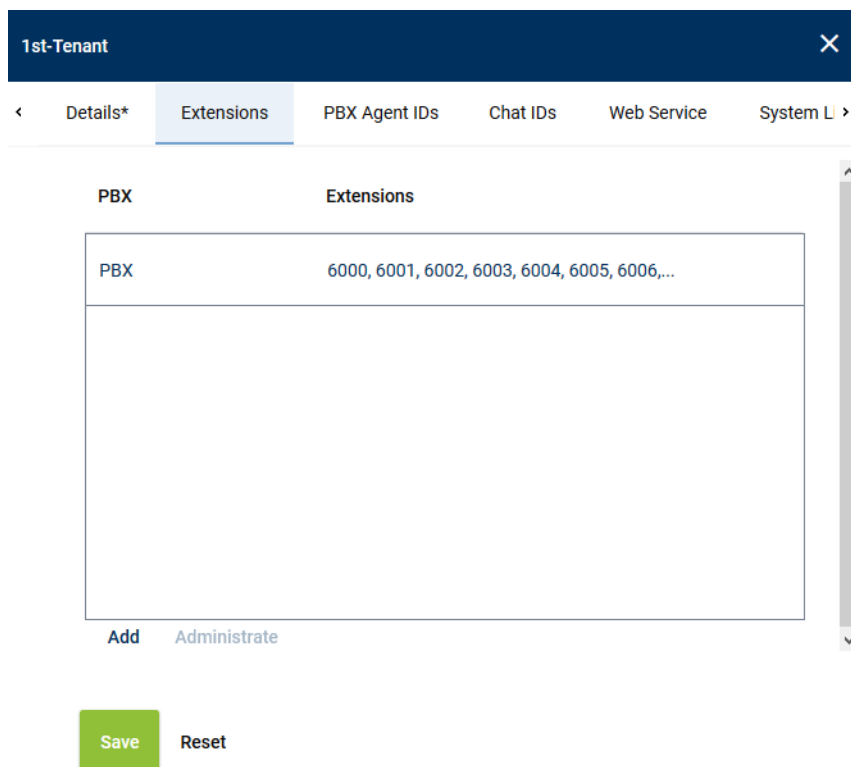


Fig. 138: Remove extensions

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. 139: 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.

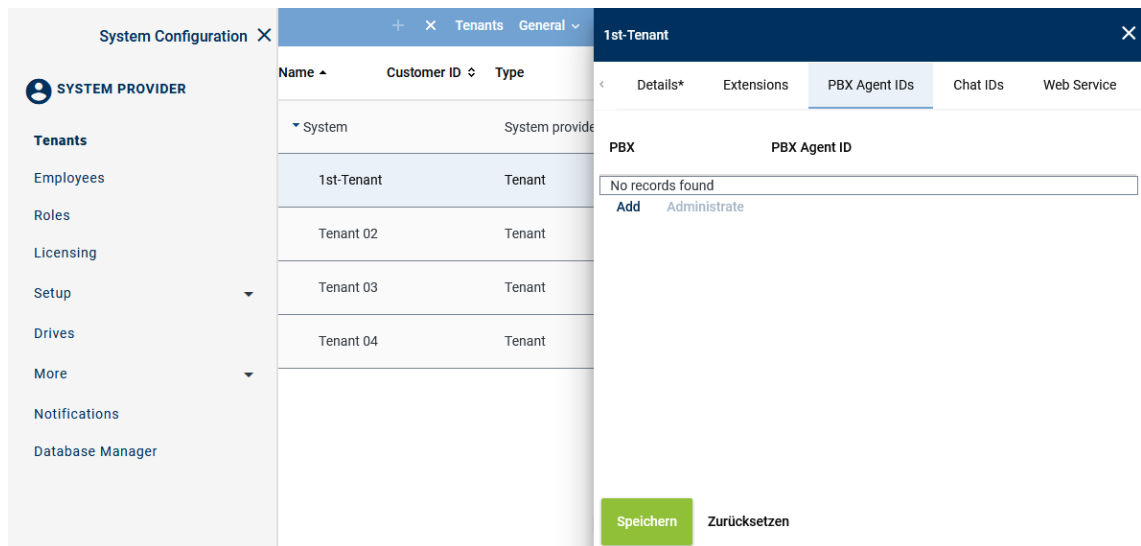
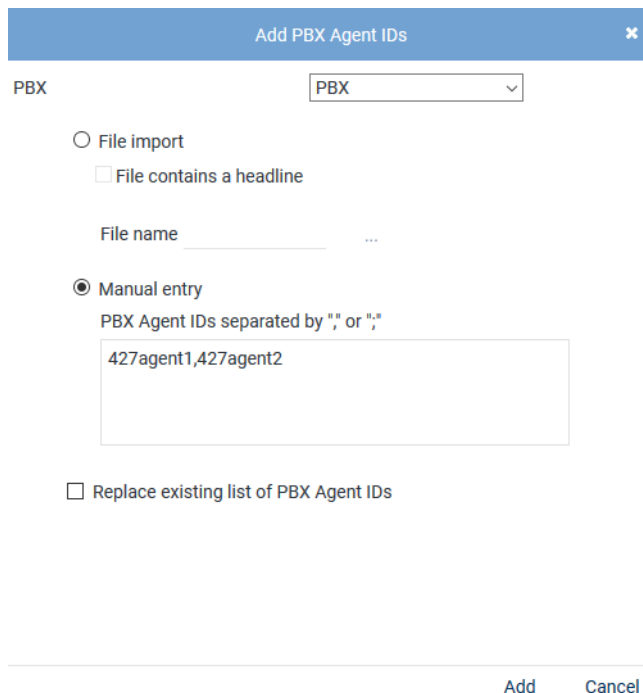


Fig. 140: Tenants - main view - tab PBX Agent ID

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 methods: 'File import' (with a checkbox for 'File contains a headline' and a 'File name' field) and 'Manual entry' (selected, with a text area containing '427agent1,427agent2' and a note 'PBX Agent IDs separated by ";" or ","'). A checkbox for 'Replace existing list of PBX Agent IDs' is at the bottom. 'Add' and 'Cancel' buttons are at the bottom right.

Fig. 141: 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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
Manual entry	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
Replace existing list of PBX Agent IDs	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 142: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 143: Additional Data module main view

2. Select a data set

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

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. 144: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 145: Additional data - configure availability

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



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

7.3.2.2.6 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:

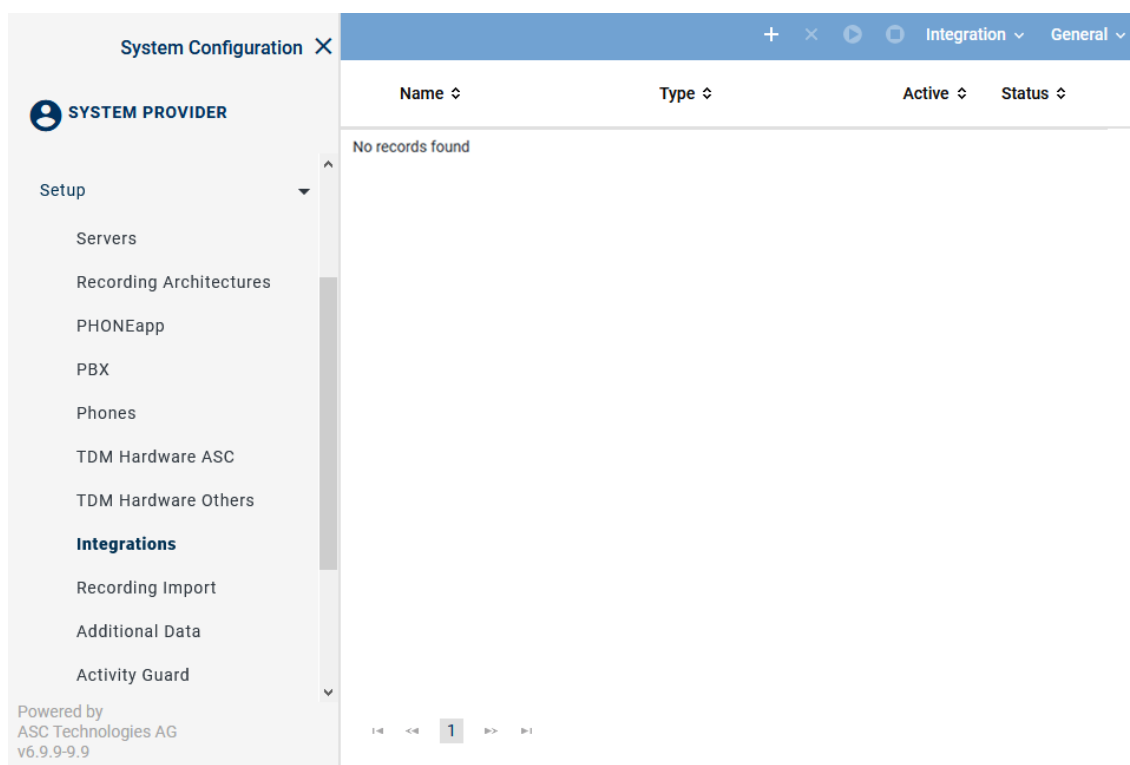




Fig. 146: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 147: Toolbar Integrations module

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

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

Import grammar

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

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

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

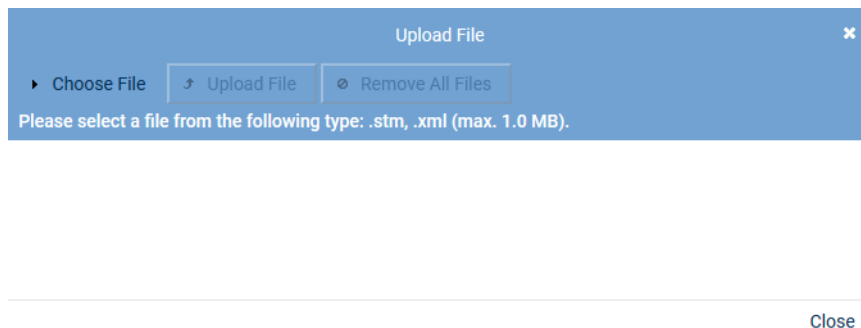


Fig. 148: Choose file

- 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*.

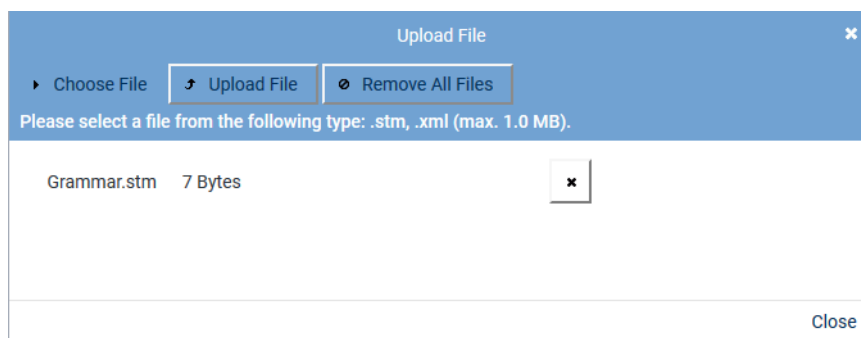



Fig. 149: Upload grammar

- 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. 150: Create integration type

2. Enter the following parameters:

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

Tab. 33: Create integration type

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

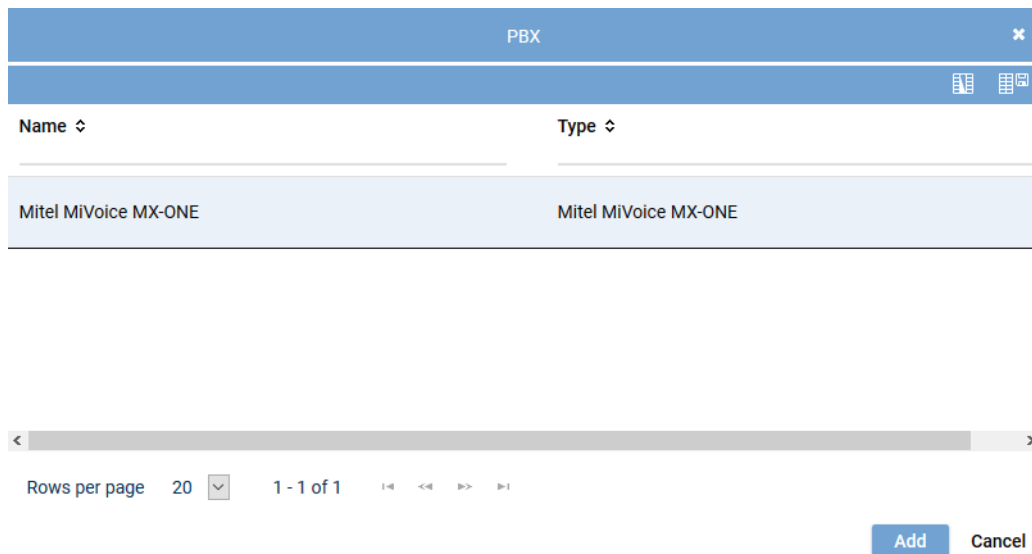


Fig. 151: Integrations - select PBX

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

Assign recording architecture for All-in-one Failover

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Failover

Save Cancel Back Next

Fig. 152: Assign recording architecture - All-in-one Failover


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

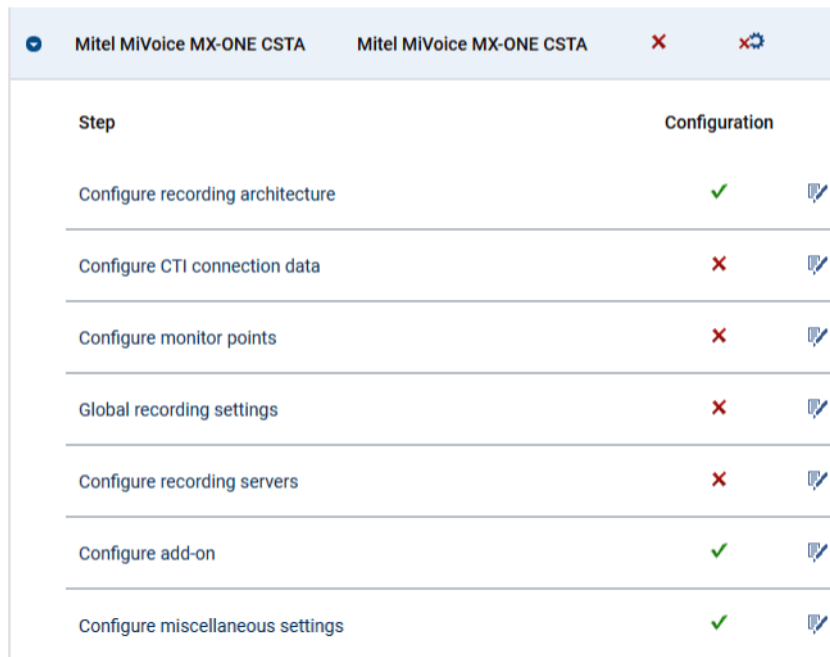


Only activated recording architectures in which the appropriate integration type has been configured appear in the drop-down list.

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			
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. 153: 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. 154: 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*
^[A-Za-z]*\s[0-9]{4}[a-zA-Z]?\$|^[0-9]{4}[a-zA-Z]?\$|^DBC[0-9]{5}\$

Save
Cancel

Fig. 155: 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. 156: 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~~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. 157: Configure connection data

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. 158: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .
<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 chapter "Configure CSTA server", p. 14 .
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See chapter "Configure CSTA server", p. 14 .

Tab. 35: Configure connection data

2. 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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

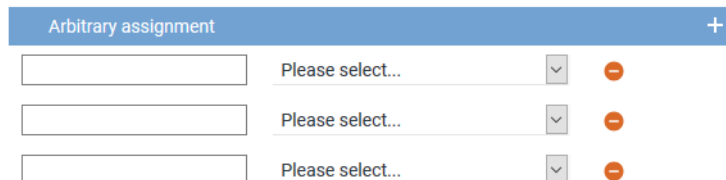



Fig. 159: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information read out of the protocol is displayed in the columns in the players.
- 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.
- To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.
⇒ An additional line to add another additional data type appears.
- Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 160: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an MBG or if the regular expression does not apply for the respective phone type, recording runs via the MBG/SRC.

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 161: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

1. Select the tab **MBG** to configure the connection data for recording by means of MiVoice Border Gateway.

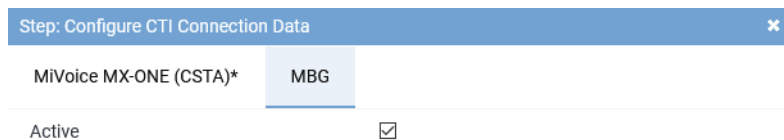


Fig. 162: Activate CTIconnect connection data for MBG

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.

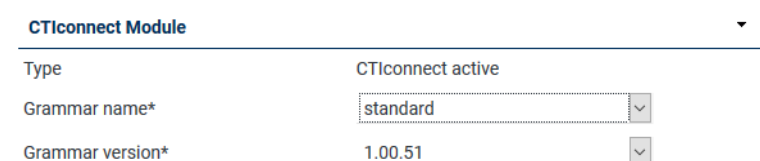


Fig. 163: Configure CTIconnect module

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.

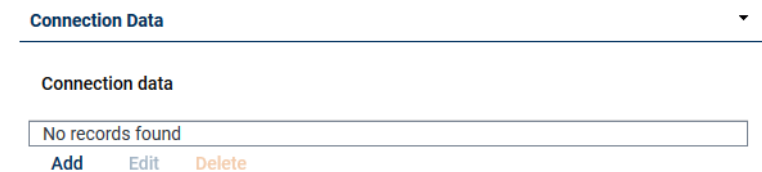


Fig. 164: Group field Connection Data

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

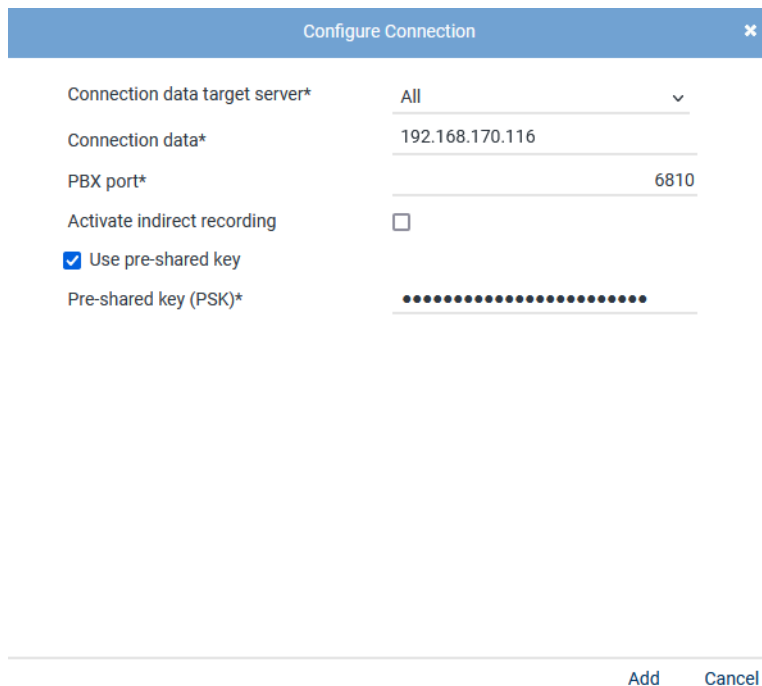


Fig. 165: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Configure target server</i>	From the drop-down list, select the option for which server the connection is intended. Select the option <i>All</i> if the connection is supposed to apply for all servers.
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , default <i>6810</i> .
<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 MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

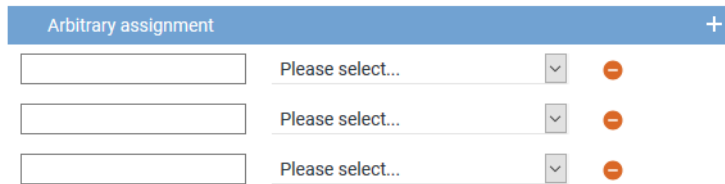



Fig. 166: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.




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



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

Configure monitor points 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.

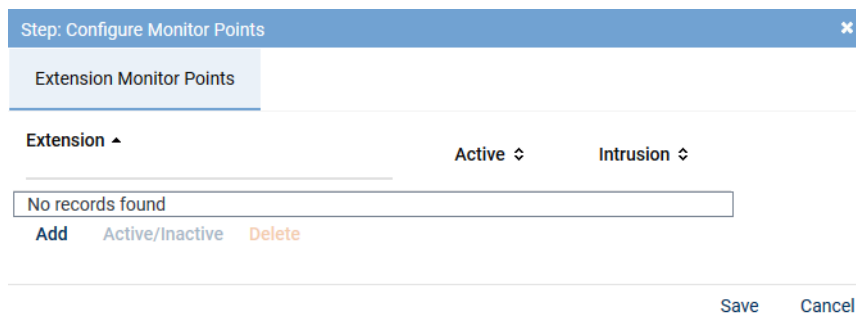


Fig. 167: Configuration step - configure monitor points

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.

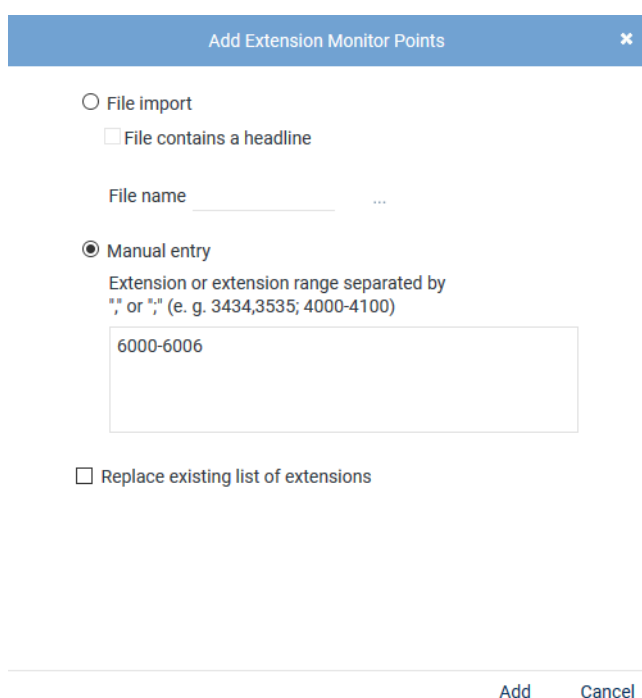






Fig. 168: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
File contains a headline	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.</p>
File name	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p>

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 ✕		
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. 169: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at

	the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Delete	To delete extension monitor points, select the respective extension in the list and click on the button <i>Delete</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Intrusion	<p>To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column <i>Intrusion</i>.</p> <p><input checked="" type="checkbox"/> = Intrusion feature has been activated.</p> <p><input type="checkbox"/> = Intrusion feature has not been activated.</p>


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



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

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 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. 170: 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	REC-01
	<div>Details*</div> <div>Extensions</div> <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>

Rows per page 50 1 - 1 of 1

Save

Close

Fig. 171: Configuration step - Configure recording servers

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

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

Tab. 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*.

Step: Configure Recording Servers

Recording Server

REC-01

REC-03

Details*

Extensions*

☐ Don't configure extensions for recording servers
 ☒ Configure extensions for recording servers

Extensions ▾

No records found

Add

Delete

Save

Rows per page 50 ▾

1 - 2 of 2

◀

<<

>>

▶

Close

Fig. 172: 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. 173: Add extensions

- In the window *Add Extensions*, enter either a single extension or an extension range that the recording server is to use when registering on the PBX.

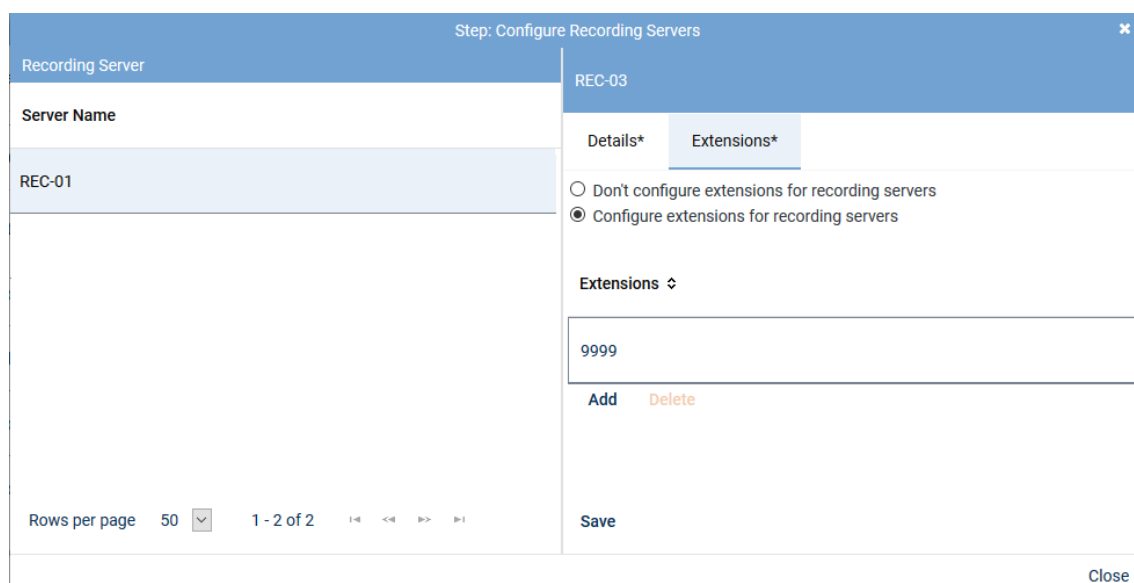



Fig. 174: Added extensions

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

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.

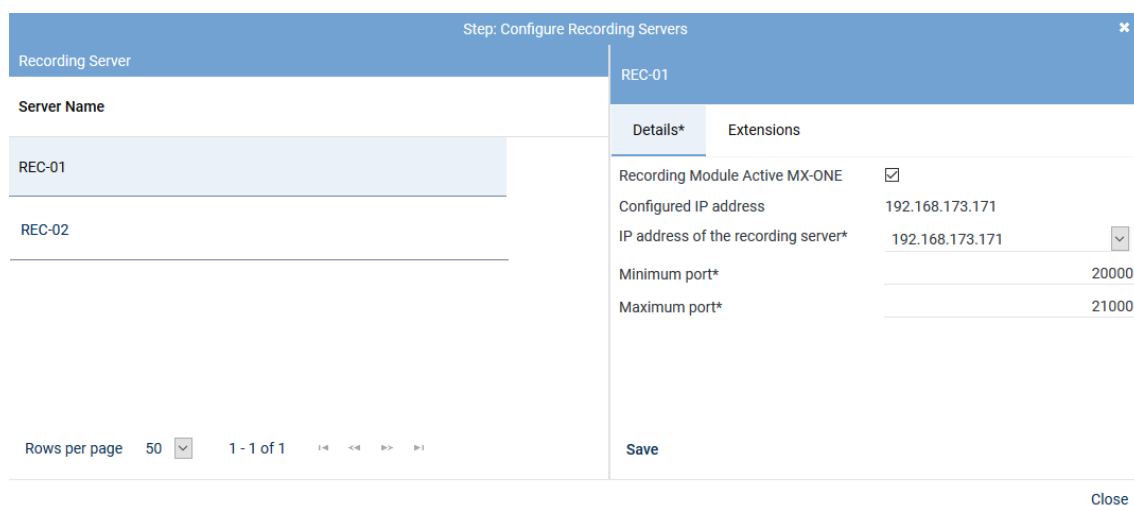


Fig. 175: Configuration step - Configure recording servers

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

Tab. 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*.

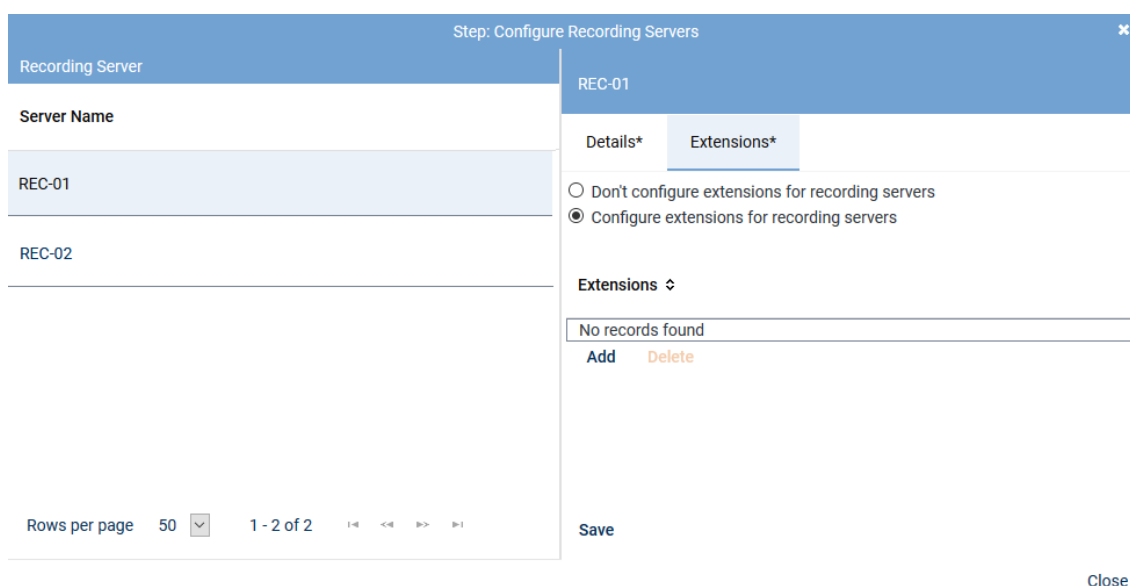


Fig. 176: Tab Extensions

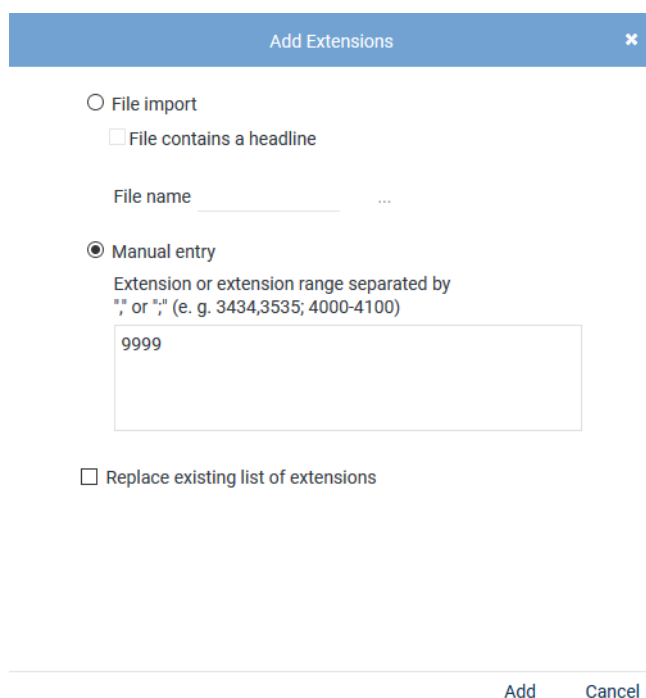
Configure extensions of the recording server Activate this option if you would like to configure extensions for the recording server so make the feature call intrusion work.

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.

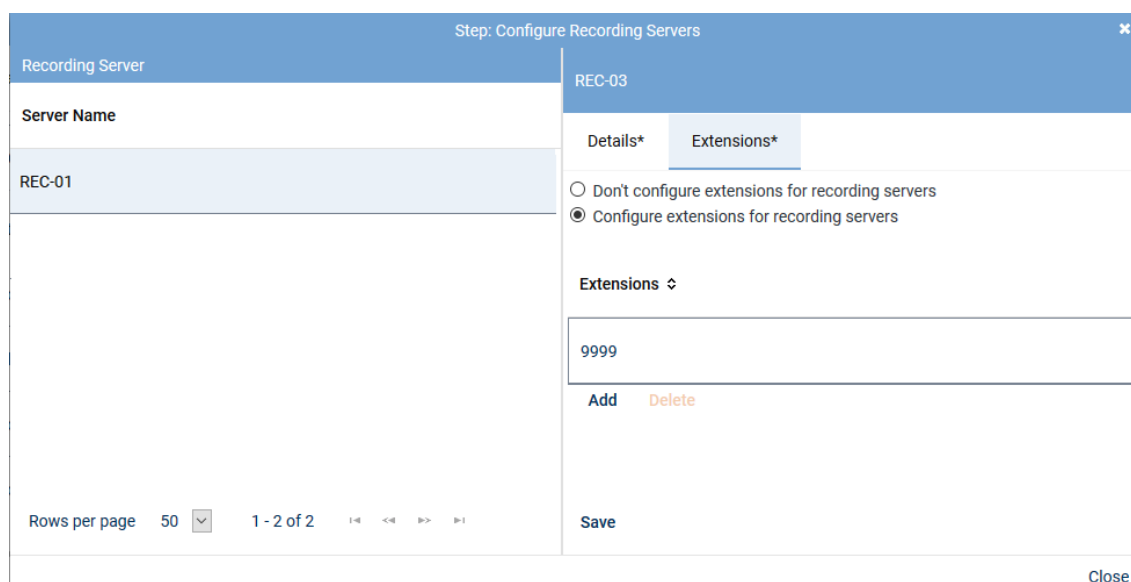


The **Add Extensions** dialog box contains the following elements:

- File import** (radio button):
 - ☐ File contains a headline
 - File name: _____
- Manual entry** (radio button, selected):
 - Extension or extension range separated by " " or ";", (e. g. 3434,3535; 4000-4100)
 - Input field containing: 9999
- ☐ Replace existing list of extensions
- Buttons: **Add** and **Cancel**

Fig. 177: 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 displays a table of recording servers and a configuration panel for the selected server.

Step: Configure Recording Servers	
Recording Server	REC-03
Server Name	Details* Extensions*
REC-01	<input type="radio"/> Don't configure extensions for recording servers <input checked="" type="radio"/> Configure extensions for recording servers
	Extensions ▾ 9999 Add Delete
Rows per page 50 ▾ 1 - 2 of 2 < << >> >	Save

Close

Fig. 178: 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. 179: 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

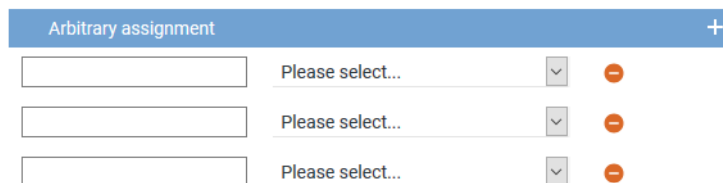



Fig. 180: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

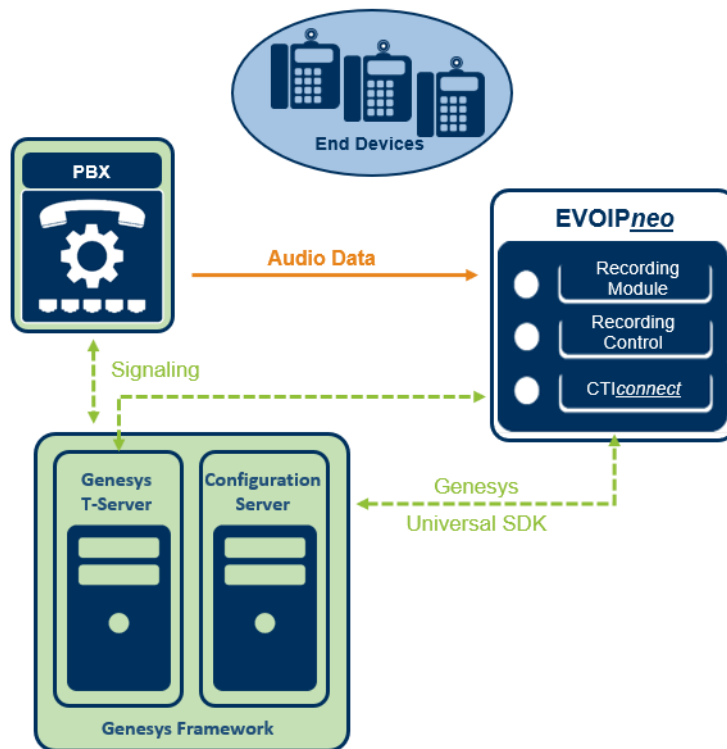


Fig. 181: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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*.

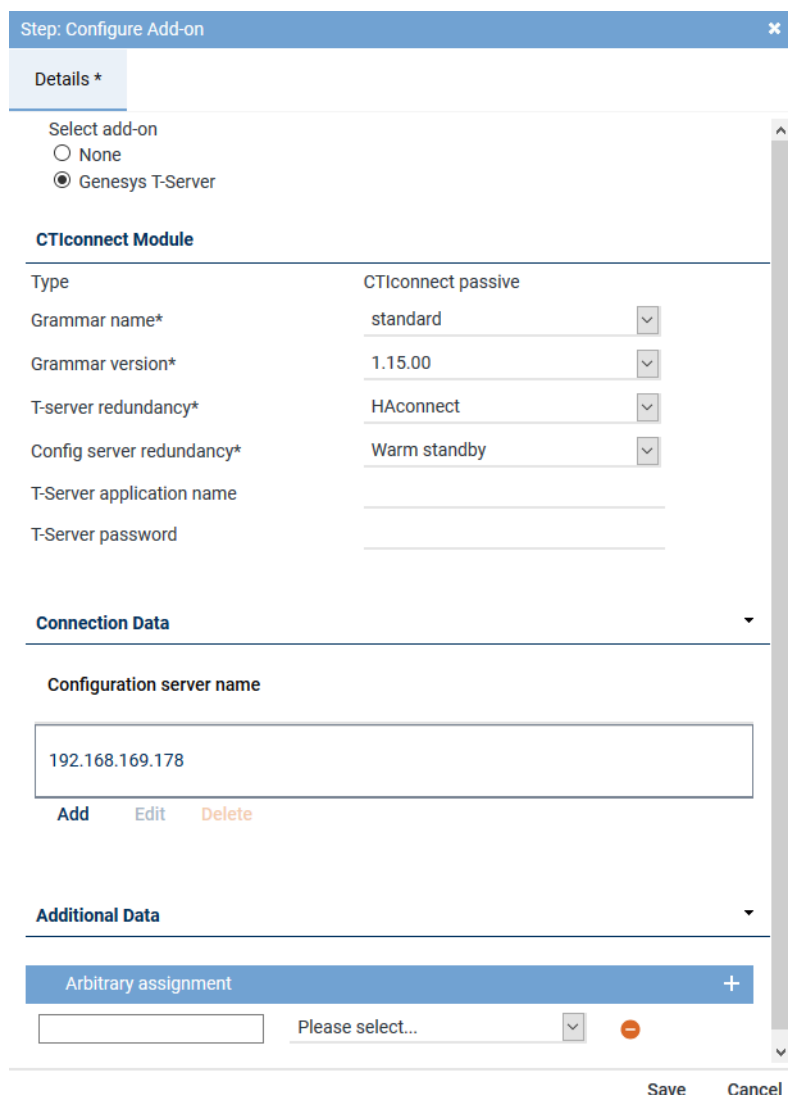


Fig. 182: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

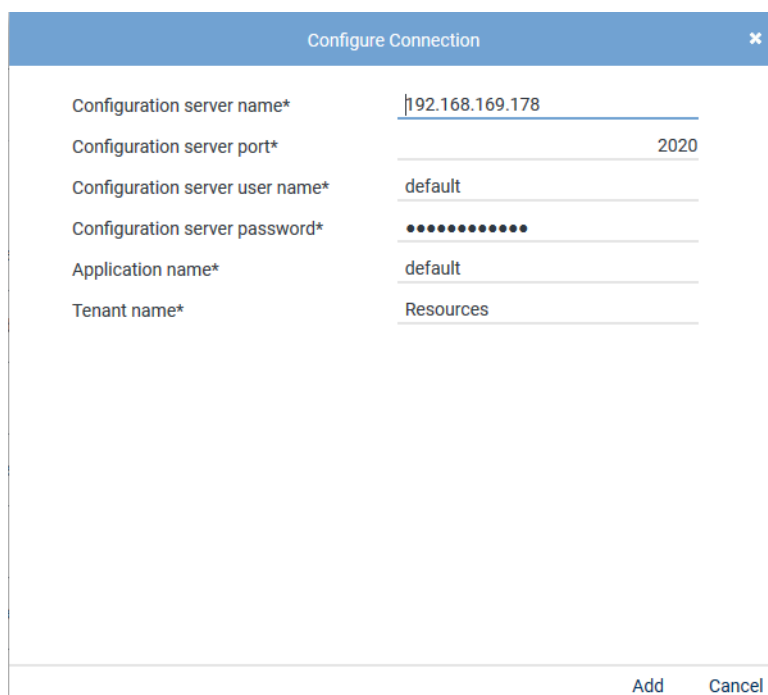
Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	<p>From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.</p> <ul style="list-style-type: none"> • <i>No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

Tab. 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.

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



Configure Connection

Configuration server name*

Configuration server port*

Configuration server user name*

Configuration server password*

Application name*

Tenant name*

Add Cancel

Fig. 183: 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.
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

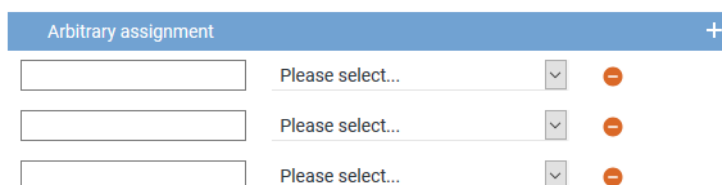




Fig. 184: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.

- Click on the button **Save** in the detail view to save the settings and complete this configuration step.

Configure miscellaneous settings

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

⇒ The window *Step: Miscellaneous Settings* appears.

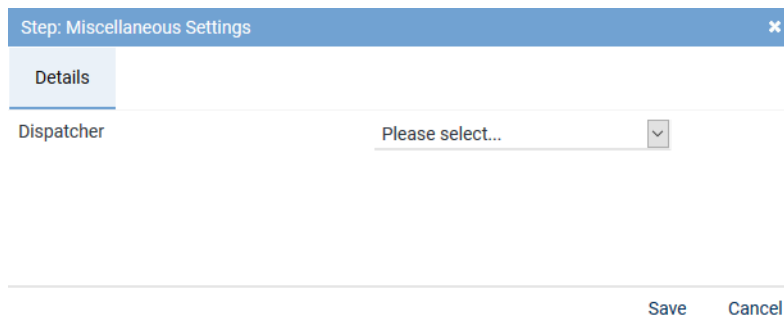


Fig. 185: Configure miscellaneous settings

- 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. 186: 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.

Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA	✓	✓
Name ↕	Type ↕	Active ↕	Status ↕	
Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	✓	✓	

Fig. 187: 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.

1. To deactivate the integration, click on the icon  (*Deactivate*) in the toolbar.

- ⇒ In the column *Active*, the icon  (*Inactive*) appears.
- ⇒ The icon  (*Delete*) becomes active in the toolbar.





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

Fig. 188: Deactivate integration

2. 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.

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

System Configuration X ⌂ 🔍 ⌂ + × ⏮ ⏭ Recording Architecture ▾ General ▾			
Name ↕	Type ↕	Active	S
No records found			
<div> <div> SYSTEM PROVIDER Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard </div> <div> Powered by ASC Technologies AG v6.9.9-9.9 </div> </div>			
<div> <div> Rows per page 50 ▾ 1 - 1 of 1 < << >> > </div> </div>			

Fig. 189: Recording architectures - main view

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

	<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. 190: 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>NOTICE! 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>NOTICE! 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"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>


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



For detailed 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*.

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

⇒ The window *New Recording Architecture* appears.



Fig. 191: Create recording architecture - All-in-one Parallel Recording

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

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

4. Click on the button *OK*.

⇒ Your entries now appear in the detail view.

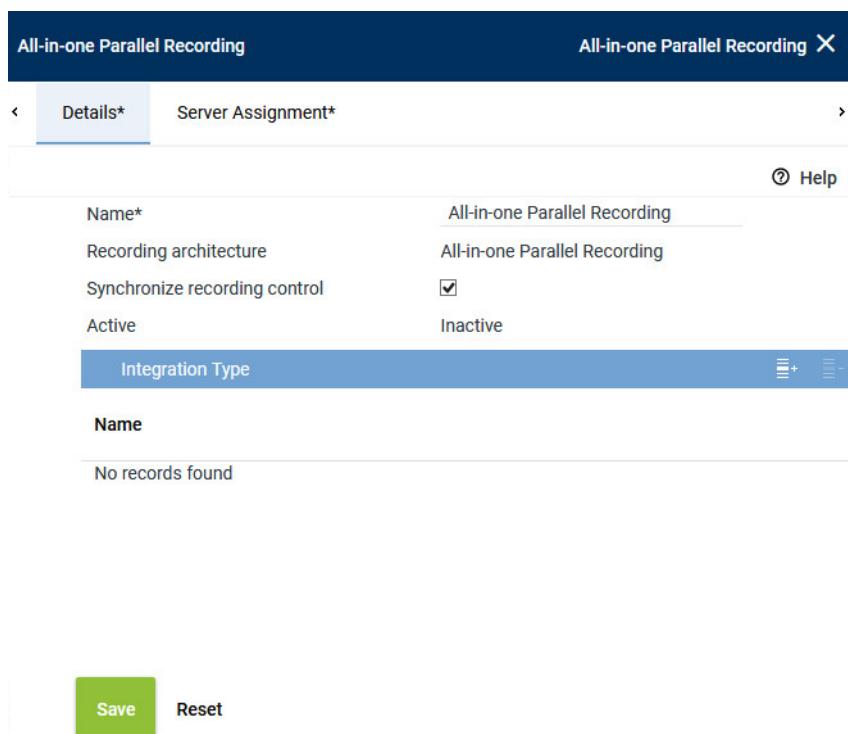



Fig. 192: Recording architecture - tab Details - All-in-one Parallel Recording

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. 439](#).

Add integration type

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

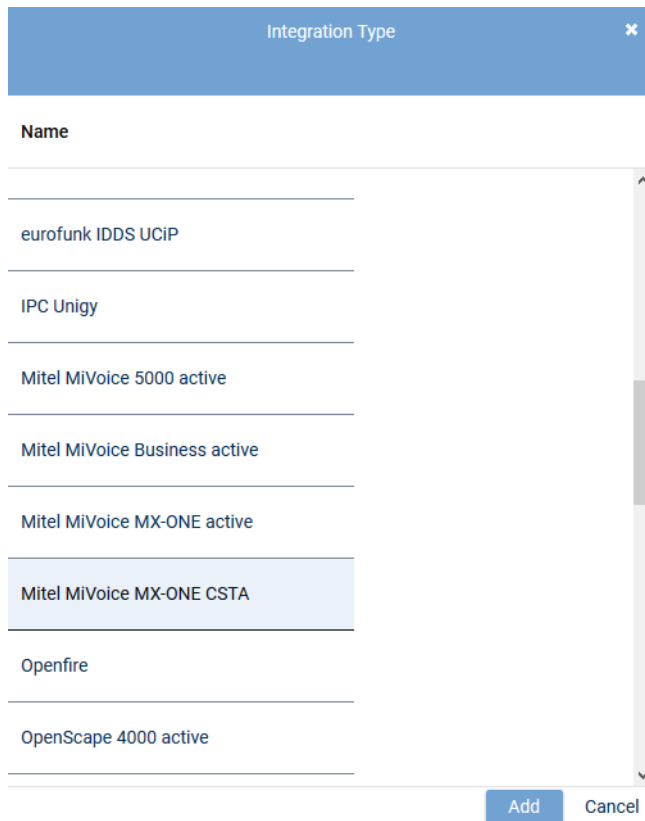


Fig. 193: Select integration type



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

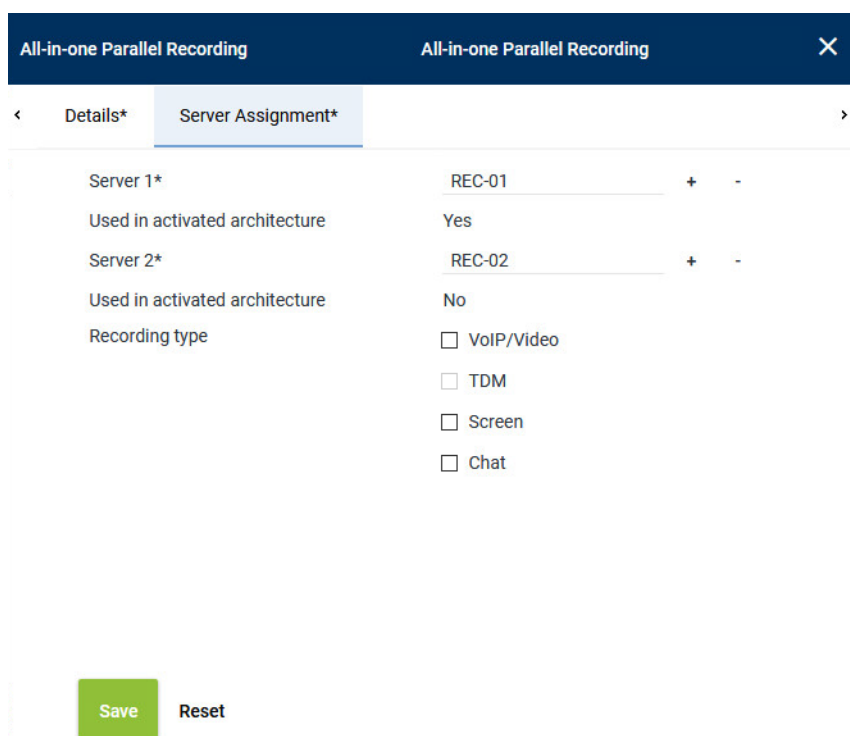


Any number of integration types can be assigned to a recording architecture.

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 X

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

Server 1*	REC-01	+	-
Used in activated architecture	Yes		
Server 2*	REC-02	+	-
Used in activated architecture	No		
Recording type	<input type="checkbox"/> VoIP/Video <input type="checkbox"/> TDM <input type="checkbox"/> Screen <input type="checkbox"/> Chat		

Save **Reset**

Fig. 194: Recording Architecture - tab Server Assignment

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



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

Rows per page 20 1 - 8 of 8

Add **Cancel**

Fig. 195: 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. 196: 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. 197: 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.

7.3.2.3.2 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:

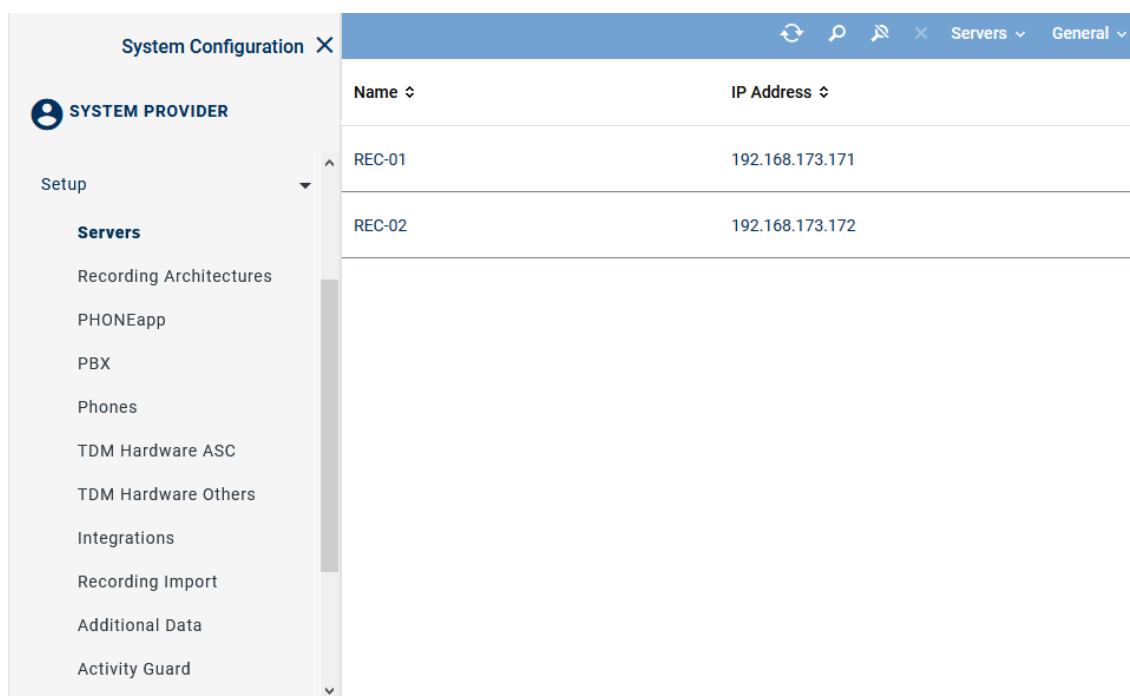


Fig. 198: Servers - main view

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

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

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

Toolbar of the Servers module

The toolbar offers the following functions.

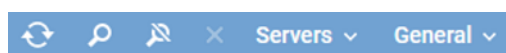







Fig. 199: Toolbar Servers module

	<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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.

<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations" , p. 166.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

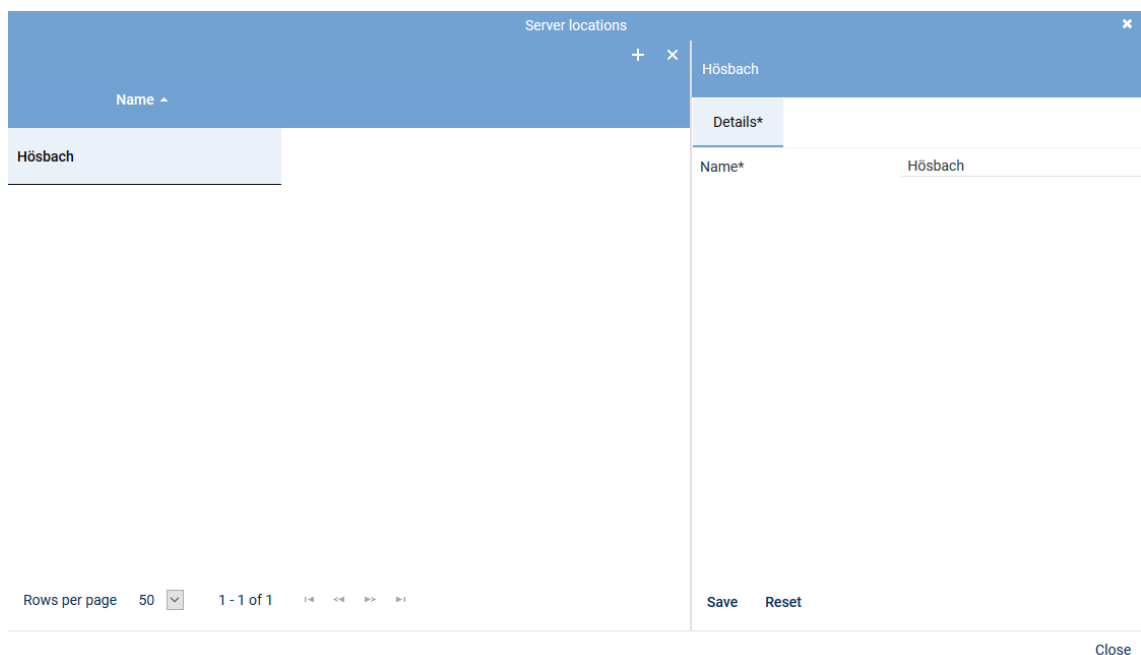



Fig. 200: Add server locations

- 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*.

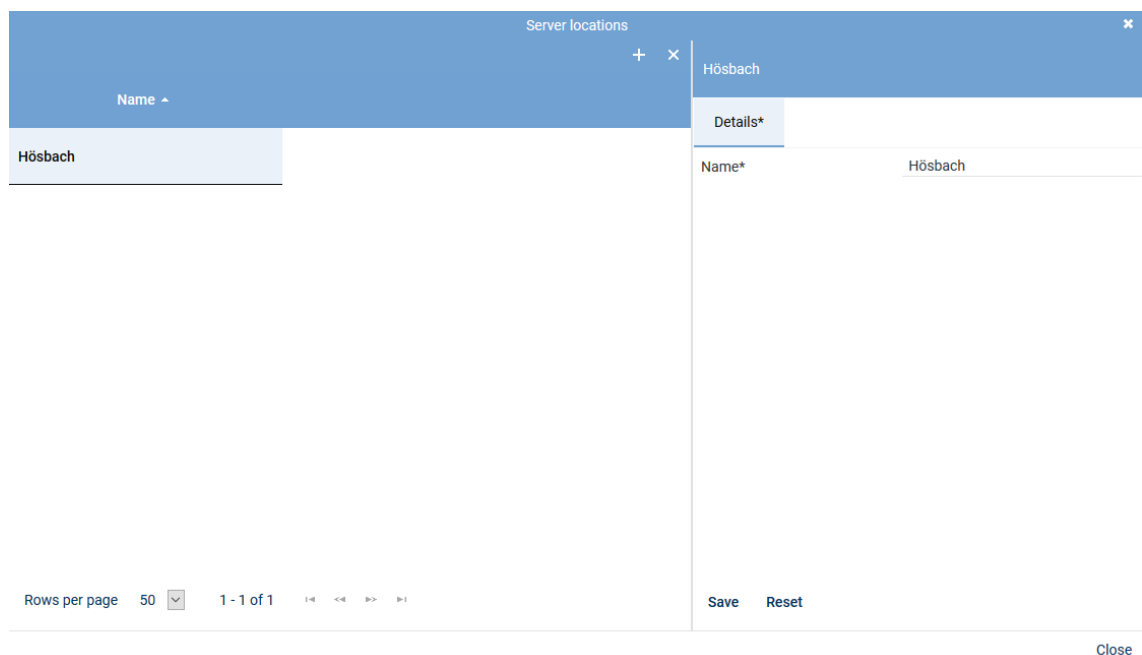
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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 header "Name" and a dropdown arrow. The table contains one row with the value "Hösbach". To the right of the table is a "Details*" tab. Below the table, there is a "Rows per page" dropdown set to "50", a "1 - 1 of 1" indicator, and navigation buttons. At the bottom right of the window, there are "Save" and "Reset" buttons, and a "Close" button at the very bottom right.

Fig. 201: 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. 202: 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. 203: Servers - tab usage

Group field API Server

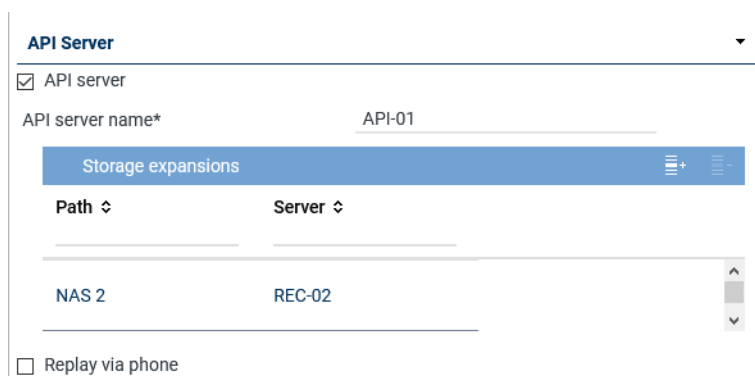




Fig. 204: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 179.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 170. By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.

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>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 177. 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. 205: 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. 206: Group field Audio Analysis

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

Tab. 45: Configure audio analysis

Emotion Detection ✕

📄

Name ↕

REC-01

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

Add **Cancel**

Fig. 207: 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/Live Streaming

Recording architecture Please choose... ▼

☐ Neo key management

Fig. 208: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/ Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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. 209: 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</p>

Parameter	Value/Description
	<p><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"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 174. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 174. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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>

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*


(max. 5 characters)


API server*

+
 -

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

Fig. 211: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 176.

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

Tab. 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.
- 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. 212: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 169](#).

- 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. 213: Group field Virtualization

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

Tab. 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.

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. 214: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<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>NOTICE! The port range must not have less than 64 ports.</p>

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

Tab Replay Server Address Mapping

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

In this tab, you can configure the replay server address mapping. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

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

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 215: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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. 216: Servers module - tab Key Management

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

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

In case of an error ... automatically

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

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

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



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



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

Tab Keystore/Virtualization

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

In this tab, you can configure the connection data 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*

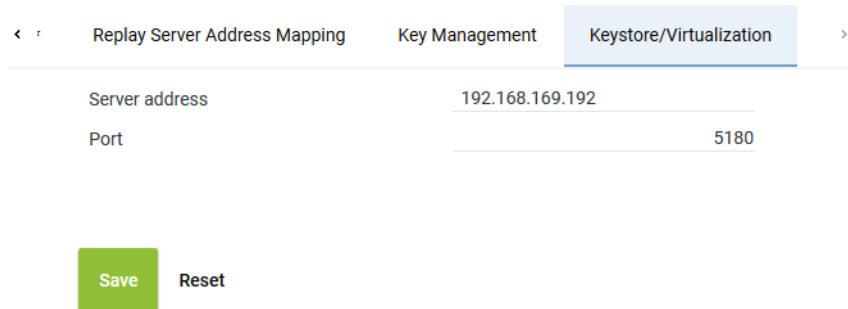
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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

Fig. 217: Servers module - tab Keystore/Virtualization

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

7.3.2.3.3 Create PBX

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

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

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

⇒ The following window appears:

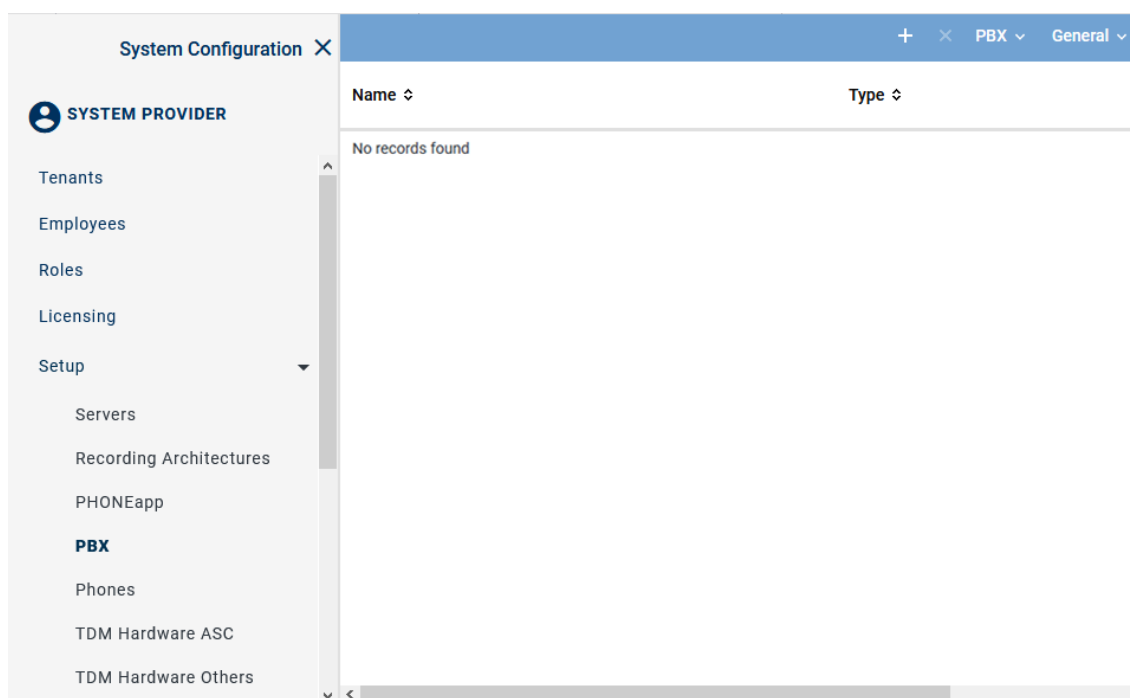




Fig. 218: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 219: Toolbar PBX module

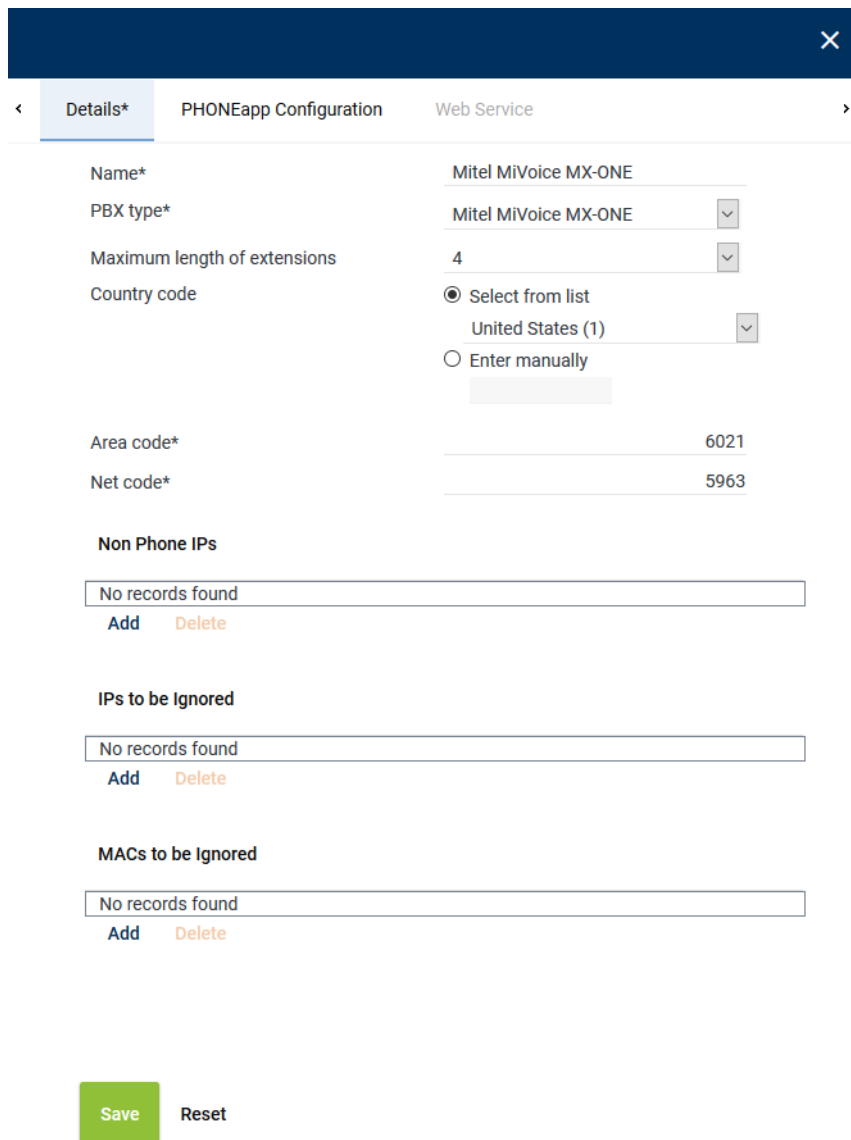
	<i>Create</i>	In the detail view, you can enter the parameters of the new PBX.
	<i>Delete</i>	Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration.
<i>PBX</i>	<i>Phone Configuration</i>	Opens a window in which you can create and configure phones.
	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



For detailed 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. 220: 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 PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka 094.

Parameter	Value/Description
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. 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

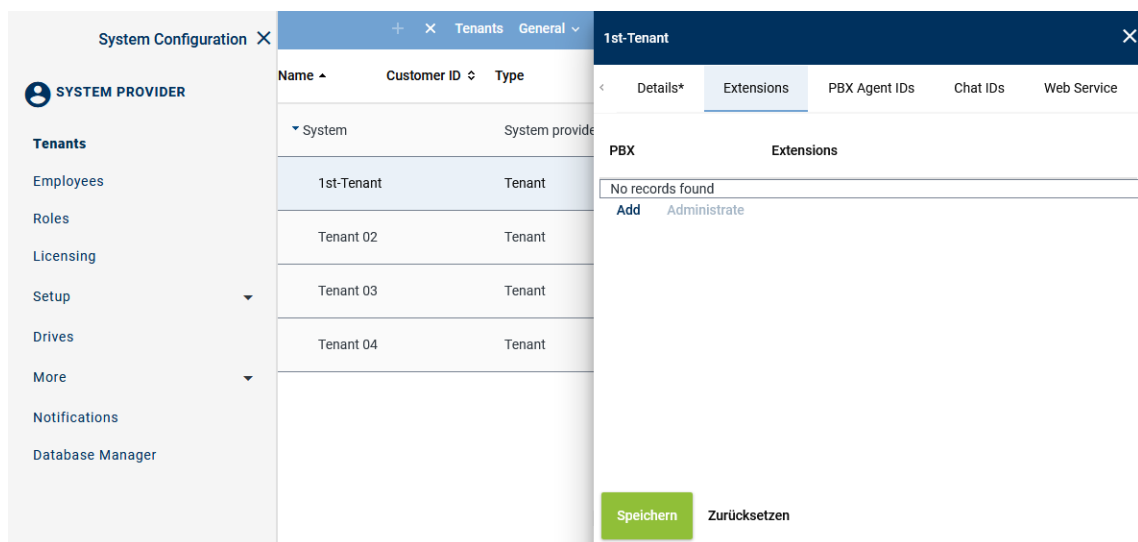


Fig. 221: Tenants - main view - tab Extensions

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. 222: 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"> • <i>ZIP</i> • <i>TXT</i> • <i>CSV</i> <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

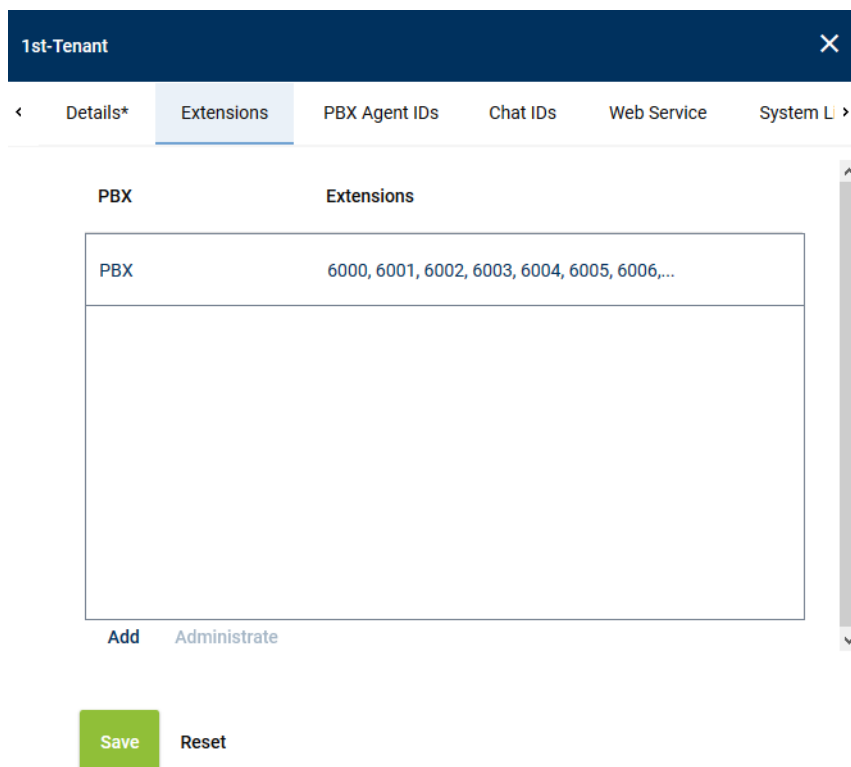


Fig. 223: Remove extensions

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.

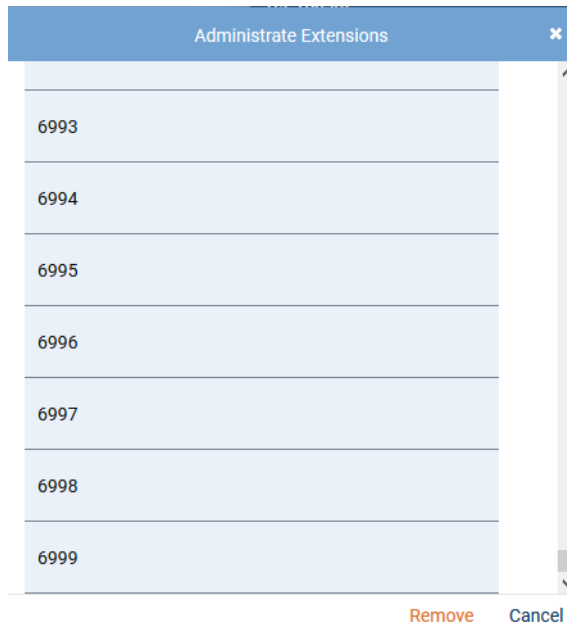


Fig. 224: Select extensions

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.

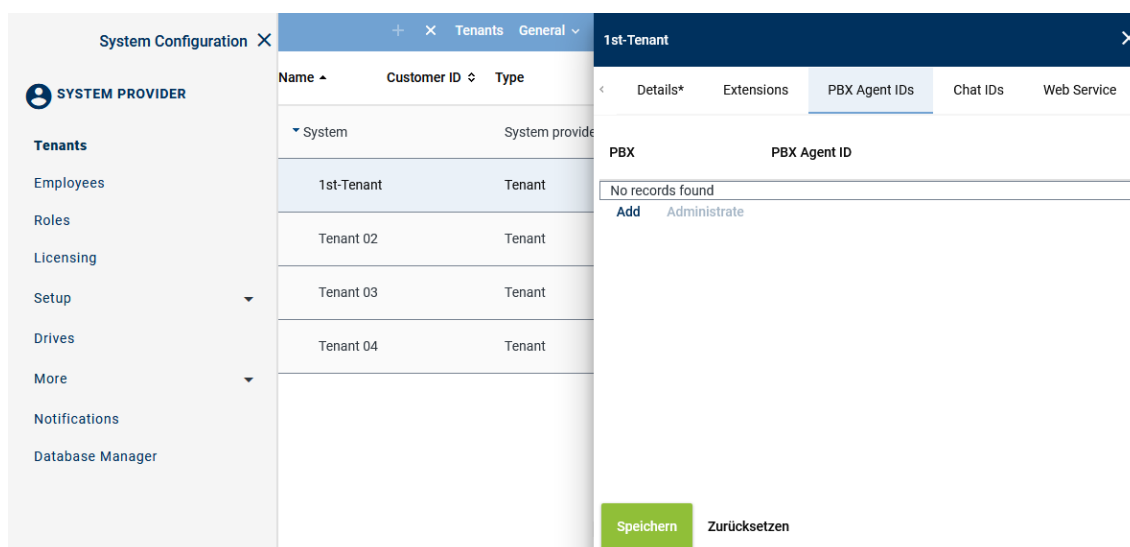
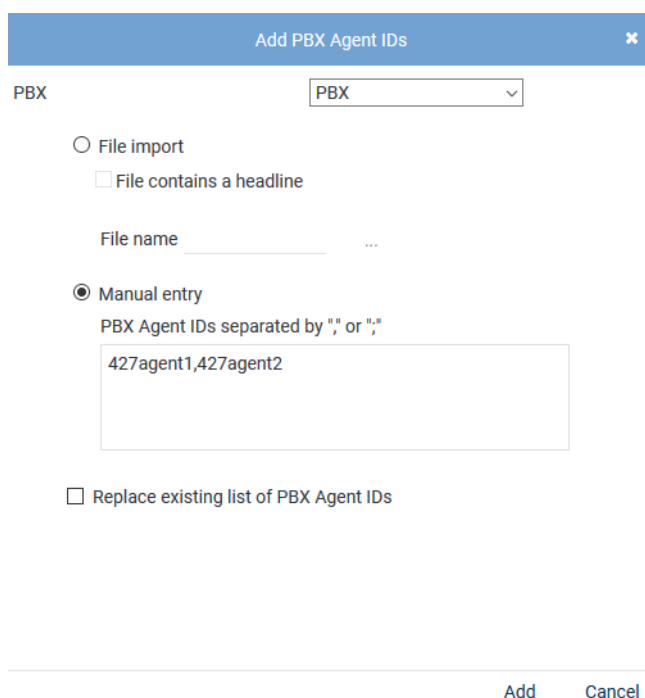


Fig. 225: Tenants - main view - tab PBX Agent ID

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 set to 'PBX'. Under 'File import', there is an unchecked checkbox for 'File contains a headline' and a text field for 'File name'. Under 'Manual entry', which is selected, there is a text field containing '427agent1,427agent2' and a note 'PBX Agent IDs separated by ";" or ","'. At the bottom, there is an unchecked checkbox for 'Replace existing list of PBX Agent IDs'. 'Add' and 'Cancel' buttons are at the bottom right.

Fig. 226: 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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
Manual entry	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
Replace existing list of PBX Agent IDs	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 227: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 228: Additional Data module main view

2. Select a data set

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

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. 229: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 230: Additional data - configure availability

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



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

7.3.2.3.6 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:

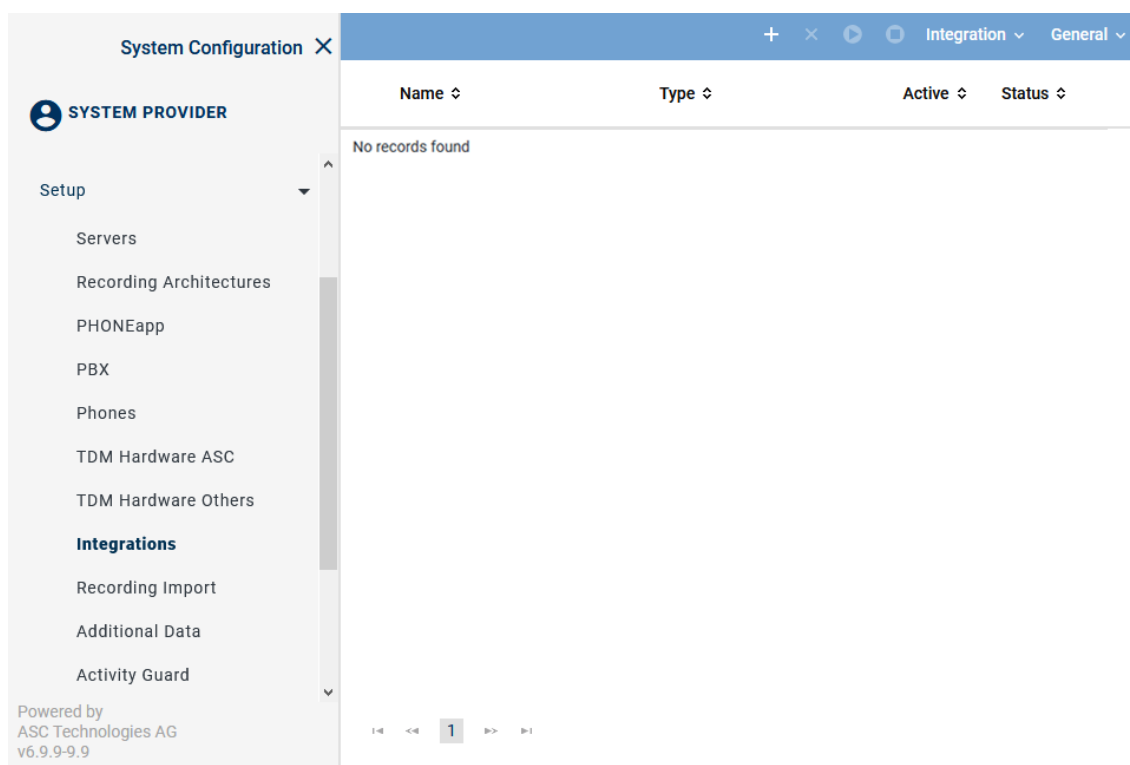




Fig. 231: Integrations - main view

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

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

Toolbar of the Integrations module

The toolbar offers the following functions.

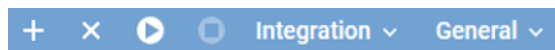






Fig. 232: Toolbar Integrations module

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

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

Import grammar

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

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

1. To import a new grammar, click on the menu item *Integration > Import Grammar* in the toolbar of the main view.

⇒ The window *Upload File* appears.

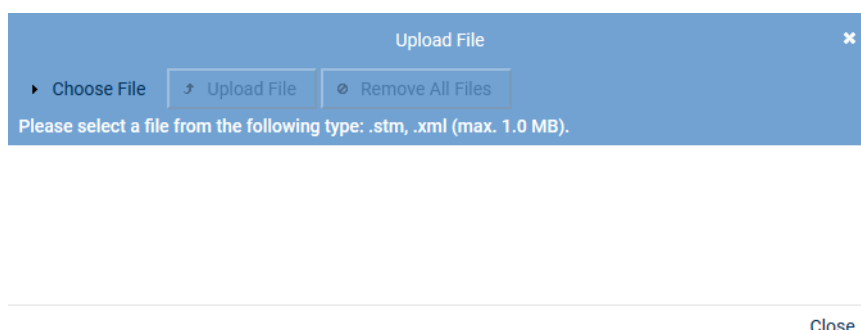


Fig. 233: Choose file

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*.

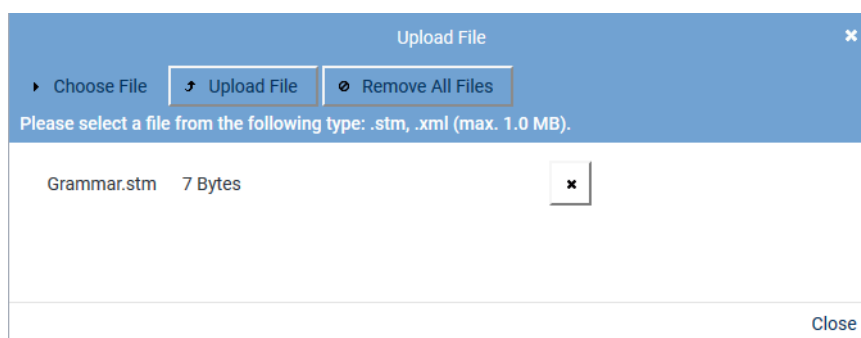



Fig. 234: Upload grammar

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

Assign integration type


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



Fig. 235: Create integration type

2. Enter the following parameters:

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

Tab. 51: Create integration type

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

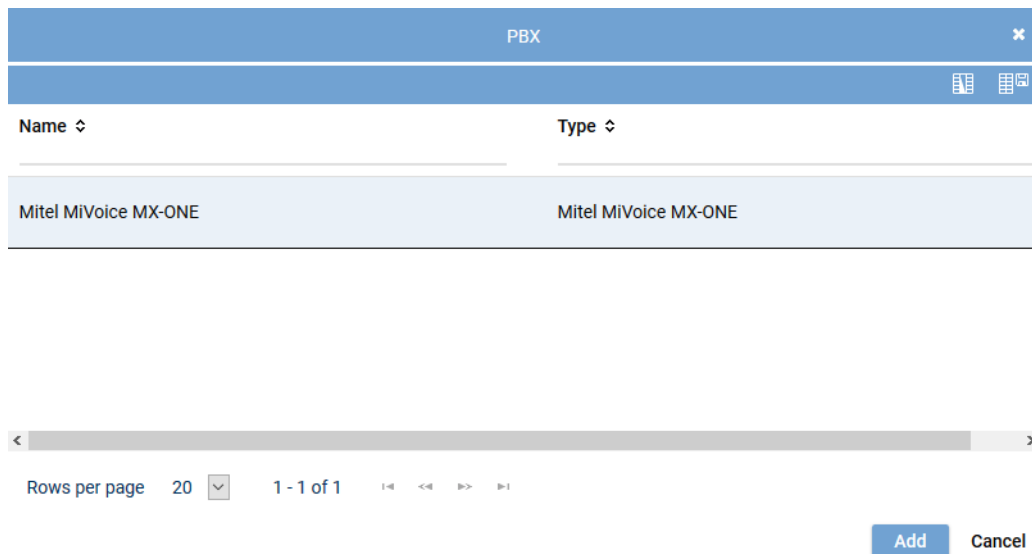


Fig. 236: Integrations - select PBX

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

Assign recording architecture for All-in-one Parallel Recording

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

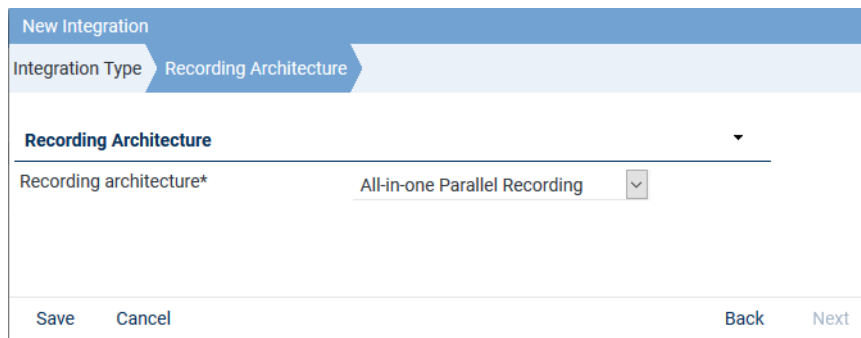


Fig. 237: Assign recording architecture - All-in-one Parallel


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.

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. 238: 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.

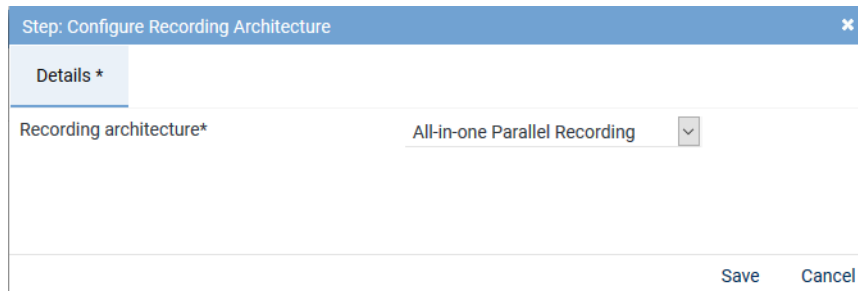



Fig. 239: Configuration step - Configure Recording Architecture

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)*

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 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

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. 240: 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. 241: 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. 242: Configure connection data

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. 243: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .

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

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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

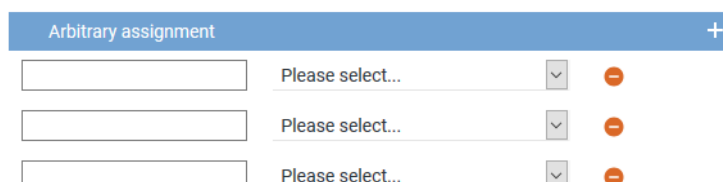



Fig. 244: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 245: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- *Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- *MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an [MBG](#) or if the regular expression does not apply for the respective phone type, recording runs via the [MBG/SRC](#).

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 246: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

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

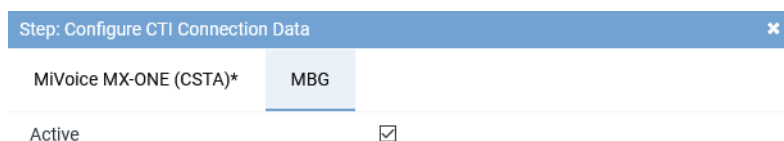


Fig. 247: Activate CTIconnect connection data for [MBG](#)

Active	<p>Activate the check box to display the configuration parameters and to activate the connection to the MBG.</p> <p><input checked="" type="checkbox"/> = Connection has been activated.</p> <p><input type="checkbox"/> = Connection has not been activated.</p>
--------	---



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.

CTIconnect Module ▼

Type	CTIconnect active
Grammar name*	standard ▼
Grammar version*	1.00.51 ▼

Fig. 248: 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.

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. 249: Group field Connection Data

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

⇒ The following window appears:

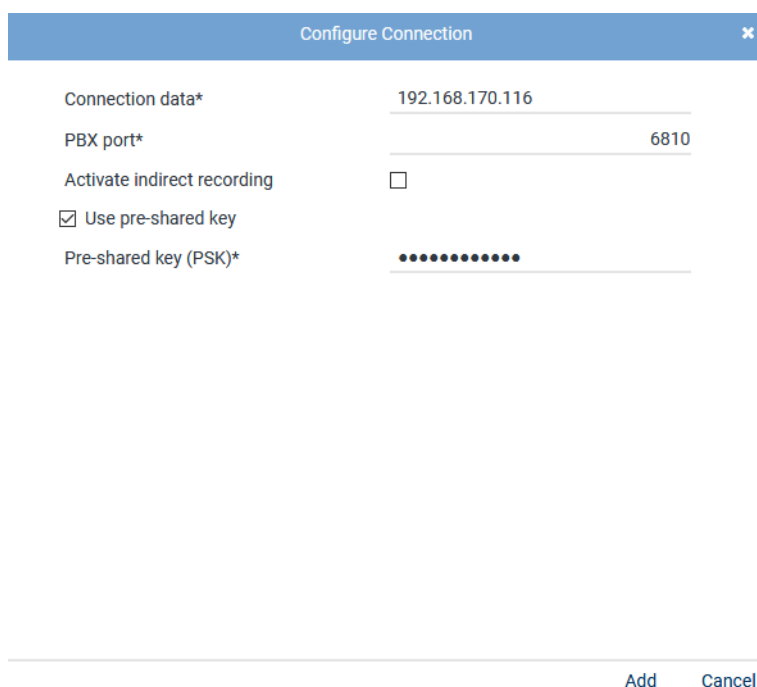


Fig. 250: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , default <i>6810</i> .
<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 MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

Tab. 55: 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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

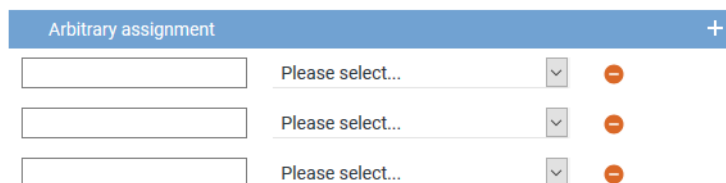


Fig. 251: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.



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



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

Configure monitor points 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.

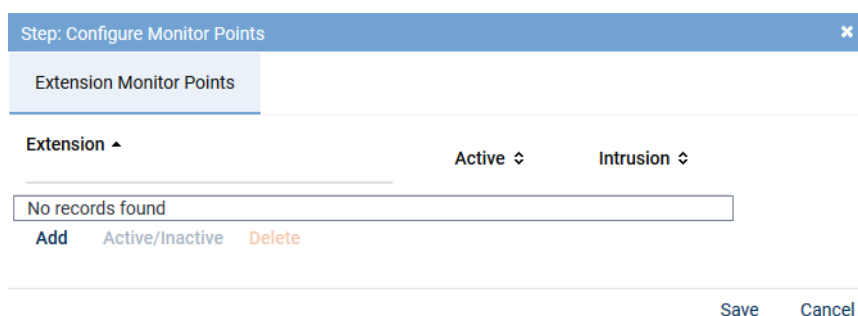


Fig. 252: Configuration step - configure monitor points

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.

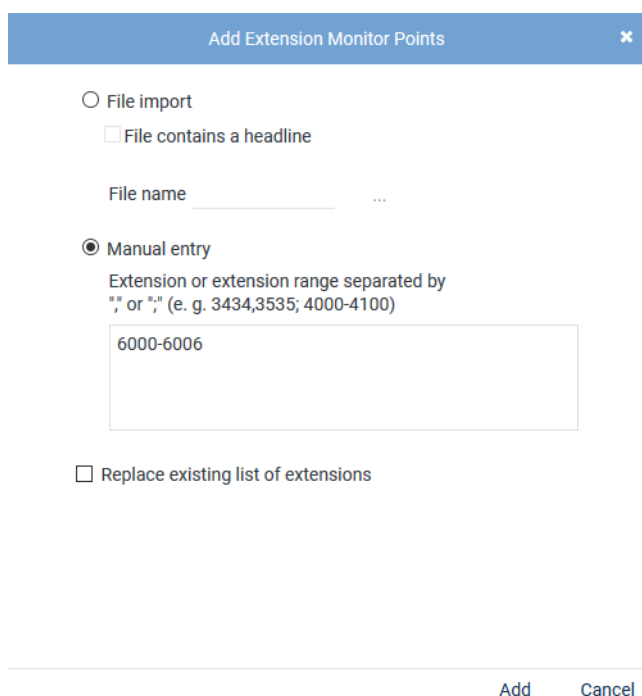




Fig. 253: Add extension monitor points

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 CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; all assignments of the PBXs which are listed in the detail view are overwritten and only the new assignment is applied.</p> <p><input type="checkbox"/> = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.</p>

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

Step: Configure Monitor Points ✕

Extension Monitor Points

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

Add
Active/Inactive
Delete

Save
Cancel

Fig. 254: Configured extension monitor points

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



In parallel recording, you cannot use the Intrusion feature.

Intrusion	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^{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. 255: 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> .

Parameter	Value/Description
<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. 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.

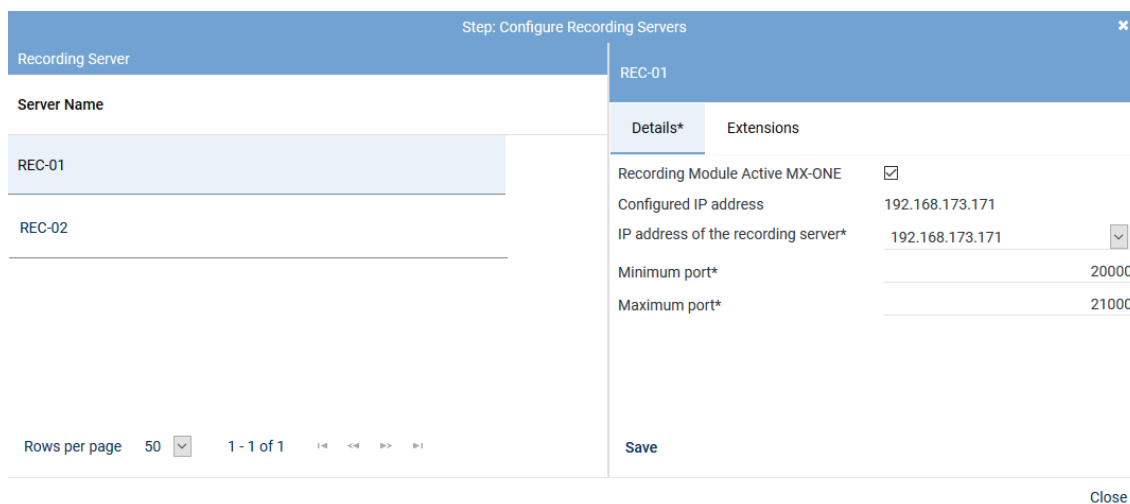


Fig. 256: Configuration step - Configure recording servers

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

Tab. 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*.

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

Type CTIconnect passive

Grammar name* standard ▼

Grammar version* 2.00.01 ▼

Connection Data ▼

Server name* 192.168.170.205

Port* 2601

Additional Data ▼

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

Arbitrary assignment
+

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

Save Cancel

Fig. 257: 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. 58: 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. 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

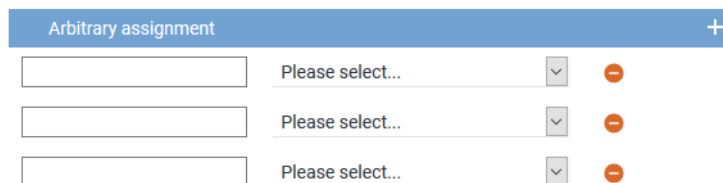



Fig. 258: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

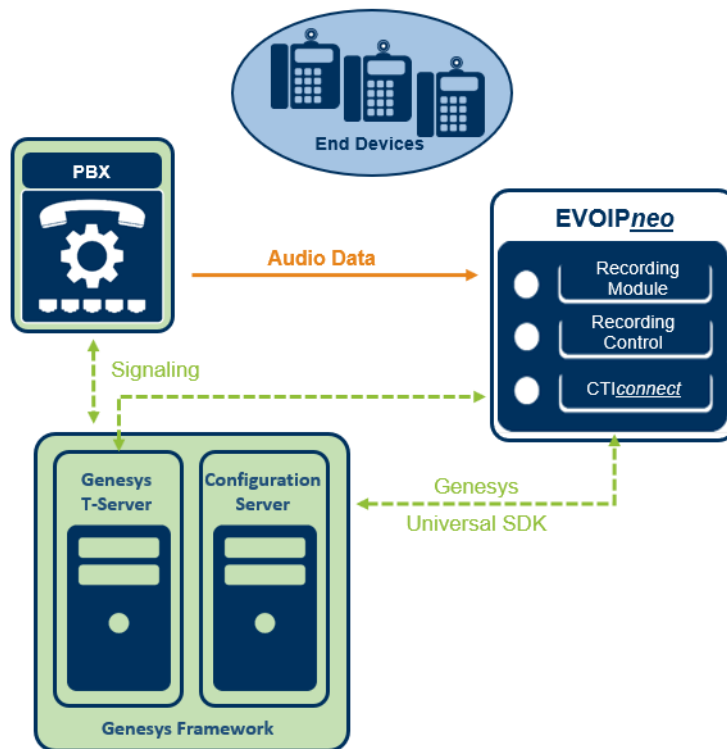


Fig. 259: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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*.

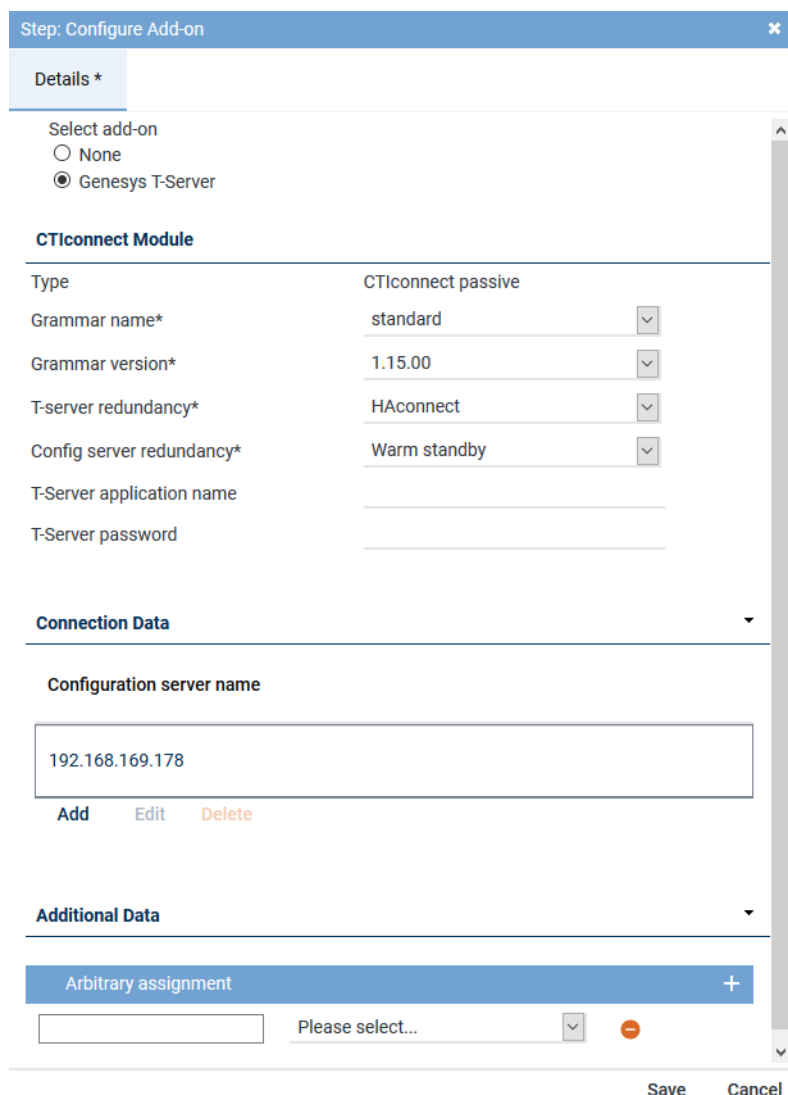


Fig. 260: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

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

Tab. 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:

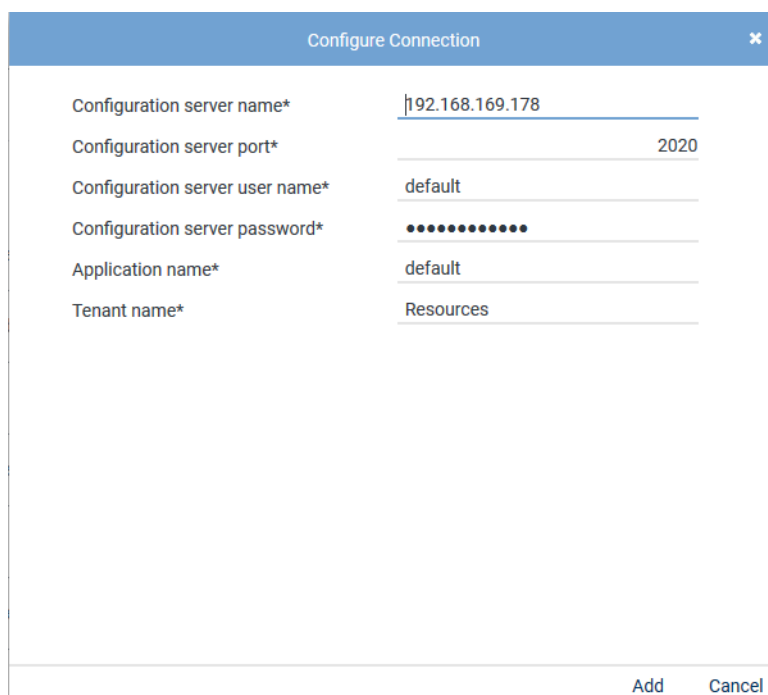


Fig. 261: Configure connection data

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.
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

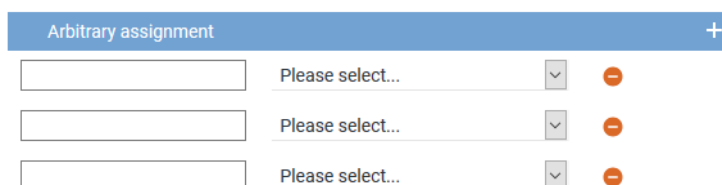




Fig. 262: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.

- Click on the button **Save** in the detail view to save the settings and complete this configuration step.

Configure miscellaneous settings

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

⇒ The window *Step: Miscellaneous Settings* appears.

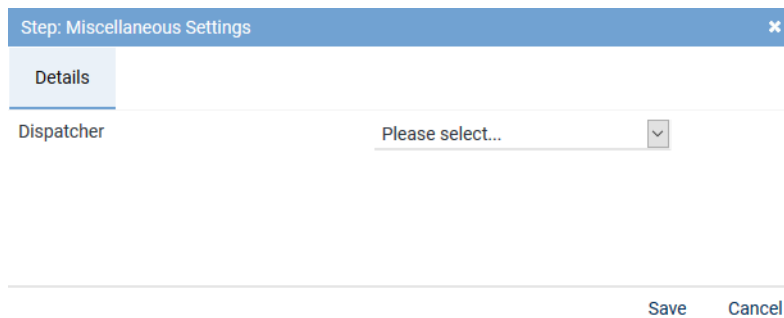


Fig. 263: Configure miscellaneous settings

- 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. 264: 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.

Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA	✔	✔
Name ↕	Type ↕	Active ↕	Status ↕	
Mitel MiVoice MX-ONE CSTA	Mitel MiVoice MX-ONE CSTA	✔	✔	

Fig. 265: 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.

1. To deactivate the integration, click on the icon  (*Deactivate*) in the toolbar.

- ⇒ In the column *Active*, the icon  (*Inactive*) appears.
- ⇒ The icon  (*Delete*) becomes active in the toolbar.





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

Fig. 266: Deactivate integration

2. 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.

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

System Configuration X		⏮ 🔍 ⏭ + × ⏮ ⏭ Recording Architecture ▾ General ▾			
SYSTEM PROVIDER		Name ↕	Type ↕	Active	S
Setup		No records found			
Servers					
Recording Architectures					
PHONEapp					
PBX					
Phones					
TDM Hardware ASC					
TDM Hardware Others					
Integrations					
Recording Import					
Additional Data					
Activity Guard					
Powered by ASC Technologies AG v6.9.9-9.9		Rows per page 50 ▾ 1 - 1 of 1 < << >> >			

Fig. 267: Recording architectures - main view


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

	<p>✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar.</p>
<i>Standby Active</i>	<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>
<i>Creation Date</i>	Date on which the recording architecture was installed.
<i>Updated</i>	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.

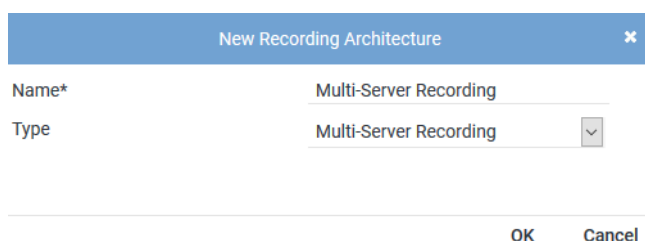
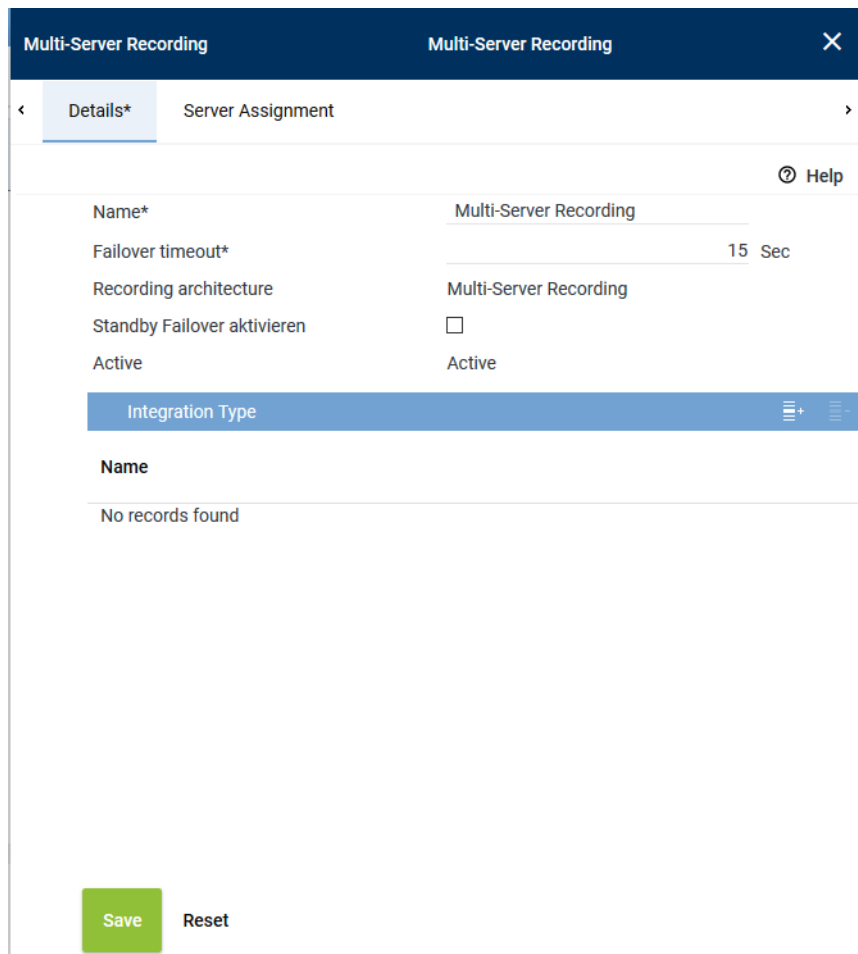


Fig. 268: Create recording architecture - Multi-Server Recording

- 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.



The screenshot shows the 'Multi-Server Recording' configuration window with the 'Details*' tab selected. The window has a dark blue header with the title 'Multi-Server Recording' and a close button. Below the header, there are two tabs: 'Details*' and 'Server Assignment'. The 'Details*' tab is active, showing a form with the following fields:

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

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


Fig. 269: Recording architecture - tab Details - Multi-Server Recording

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



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

Add integration type

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

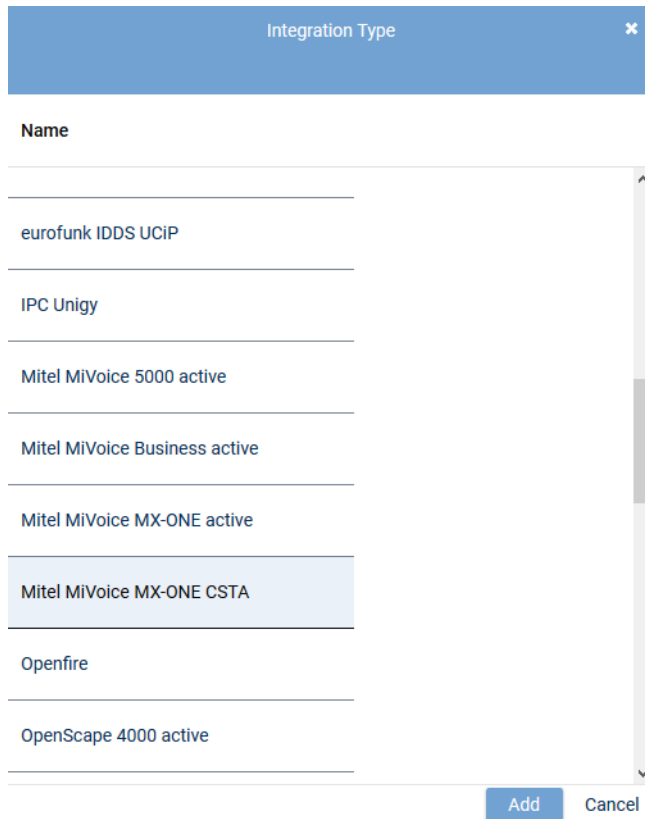


Fig. 270: Select integration type



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 Recording

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

Group field Recording Control and CTIconnect

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

Multi-Server Recording
Multi-Server Recording

Details*
Server Assignment*

Recording Control and CTIconnect

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

Recording Server


Recording Server

Server
Standby

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

Save
Reset

Fig. 271: 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. 272: 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:

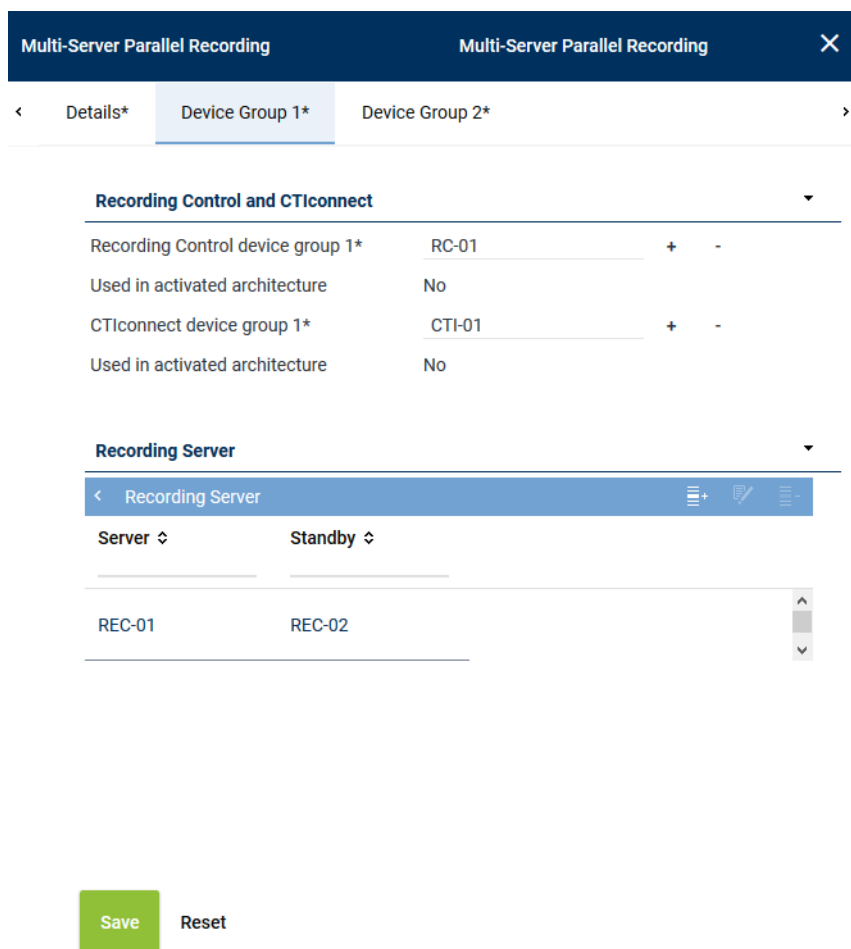









Fig. 273: Add recording server

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. 274: 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

SYSTEM PROVIDER

Setup

Servers

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. 275: Servers - main view

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

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

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

Toolbar of the Servers module

The toolbar offers the following functions.

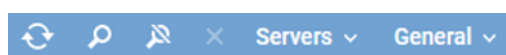







Fig. 276: Toolbar Servers module

	<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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.

<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations" , p. 230.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

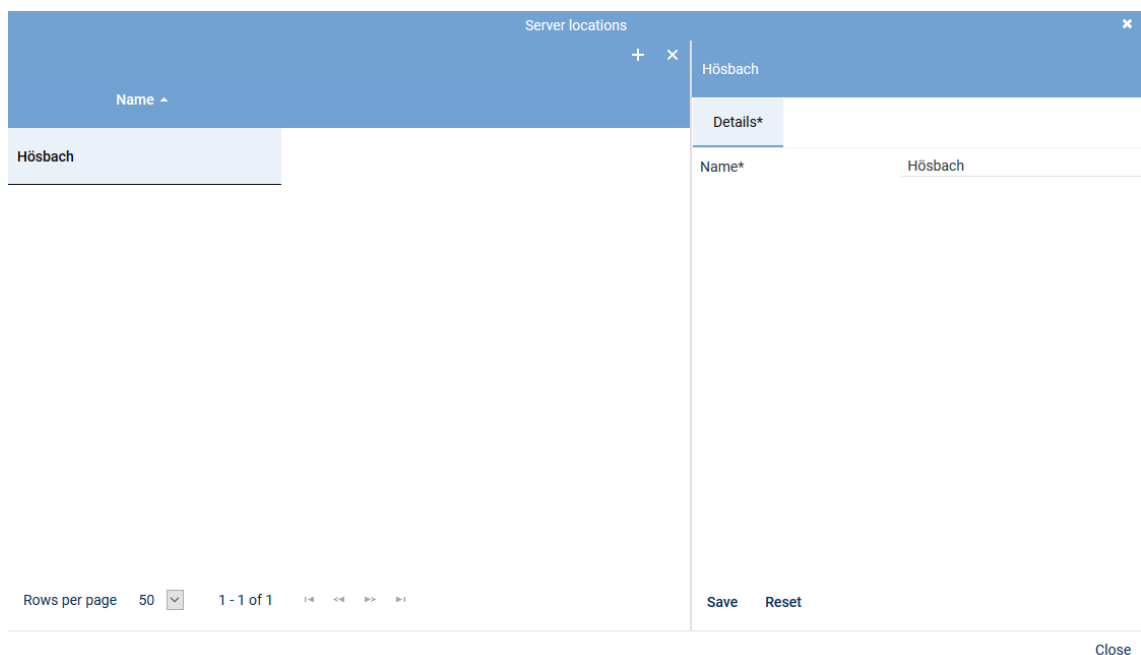



Fig. 277: Add server locations

- 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*.

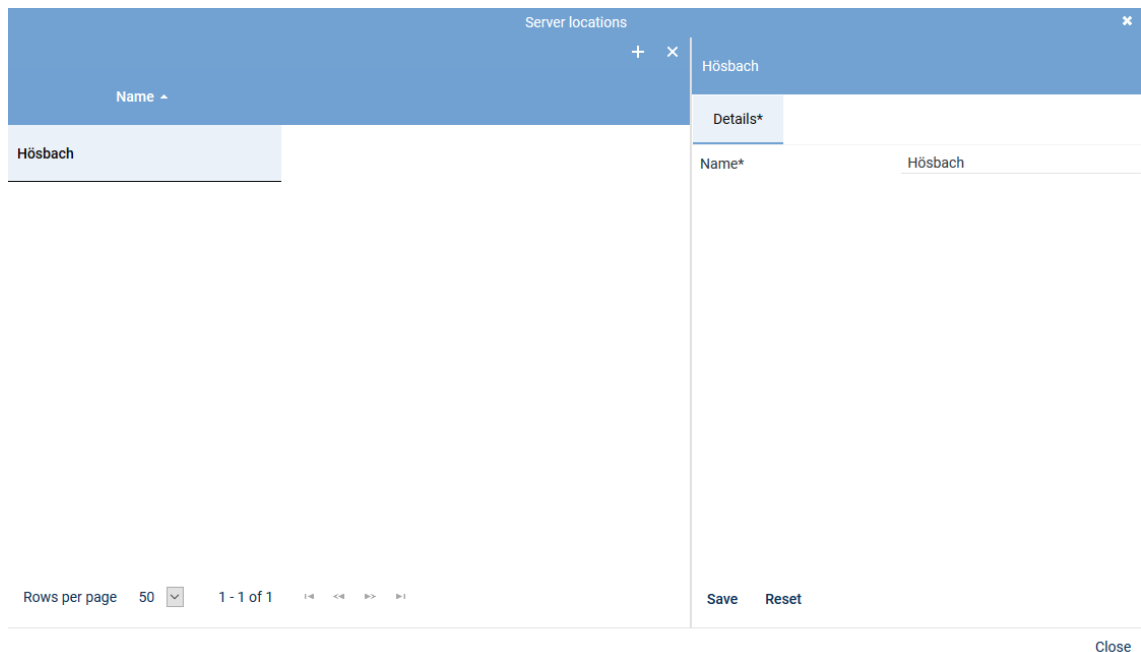
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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 details panel with a tab labeled "Details*". Inside the details panel, there is a field labeled "Name*" with the value "Hösbach". At the bottom of the window, there is a footer area with "Rows per page" set to 50, "1 - 1 of 1", and navigation icons. On the right side of the footer, there are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the window.

Fig. 278: 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. 279: 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. 280: Servers - tab usage

Group field API Server

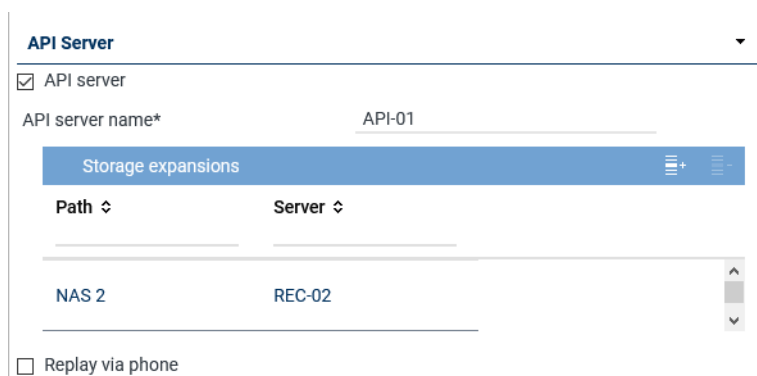




Fig. 281: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 243.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 234. By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.

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>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 241. 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. 282: 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. 283: Group field Audio Analysis

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

Tab. 62: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

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

Add Cancel

Fig. 284: 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/Live Streaming

Recording architecture Please choose... ▼

☐ Neo key management

Fig. 285: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/ Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 286: 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</p>

Parameter	Value/Description
	<p><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"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 238. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 238. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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>

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*


(max. 5 characters)


API server*

+
 -

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

Fig. 288: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	<p>Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.</p>
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 240.

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

Tab. 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.

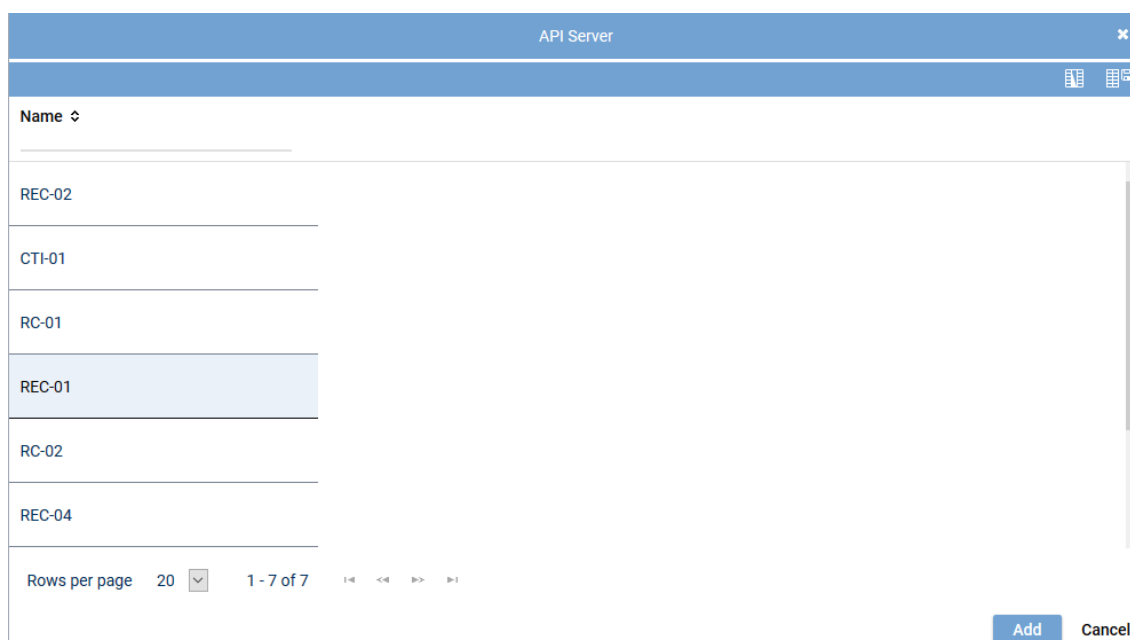


Fig. 289: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 233](#).

- 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. 290: Group field Virtualization

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

Tab. 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. 291: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<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>NOTICE! The port range must not have less than 64 ports.</p>

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

Tab Replay Server Address Mapping

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

In this tab, you can configure the replay server address mapping. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

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

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 292: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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. 293: Servers module - tab Key Management

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

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

In case of an error ... automatically

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

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

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



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



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

Tab Keystore/Virtualization

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

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

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

For key management there are the following options:

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

For licensing, there are the following options:

Without Internet access:

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

- *Trusted Virtualization License*

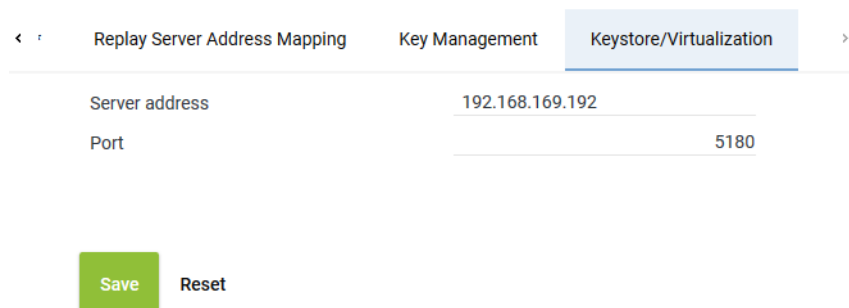
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*

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



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

Server address 192.168.169.192

Port 5180

Save Reset

Fig. 294: Servers module - tab Keystore/Virtualization

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

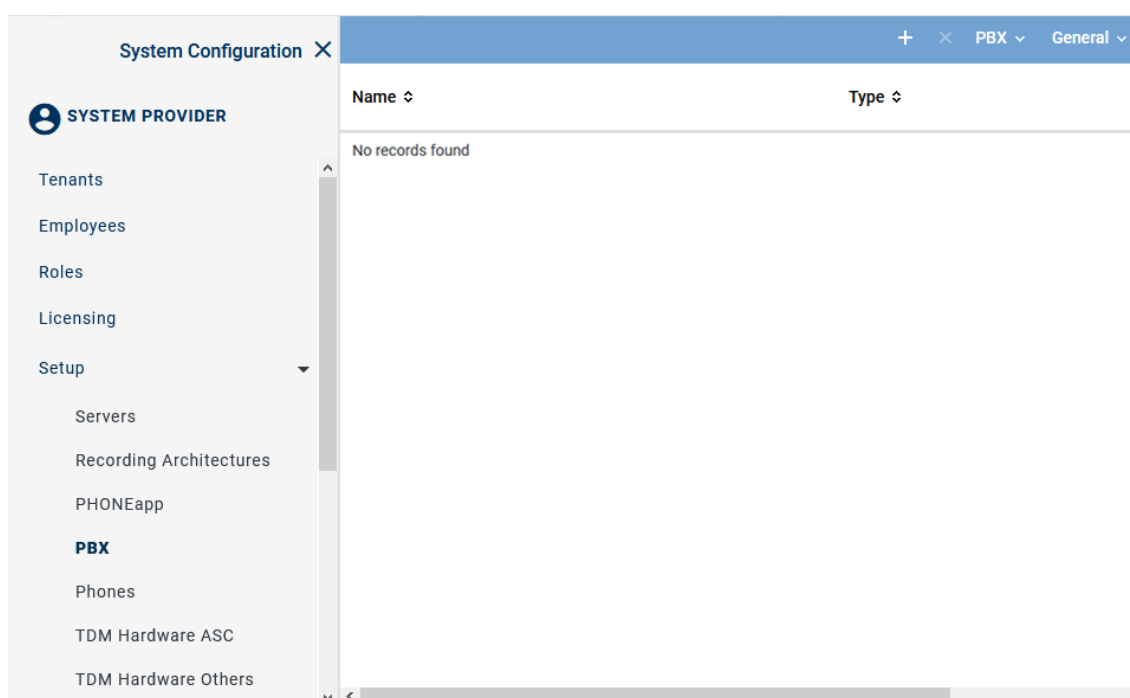


Fig. 295: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

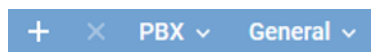





Fig. 296: Toolbar PBX module

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



For detailed 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.

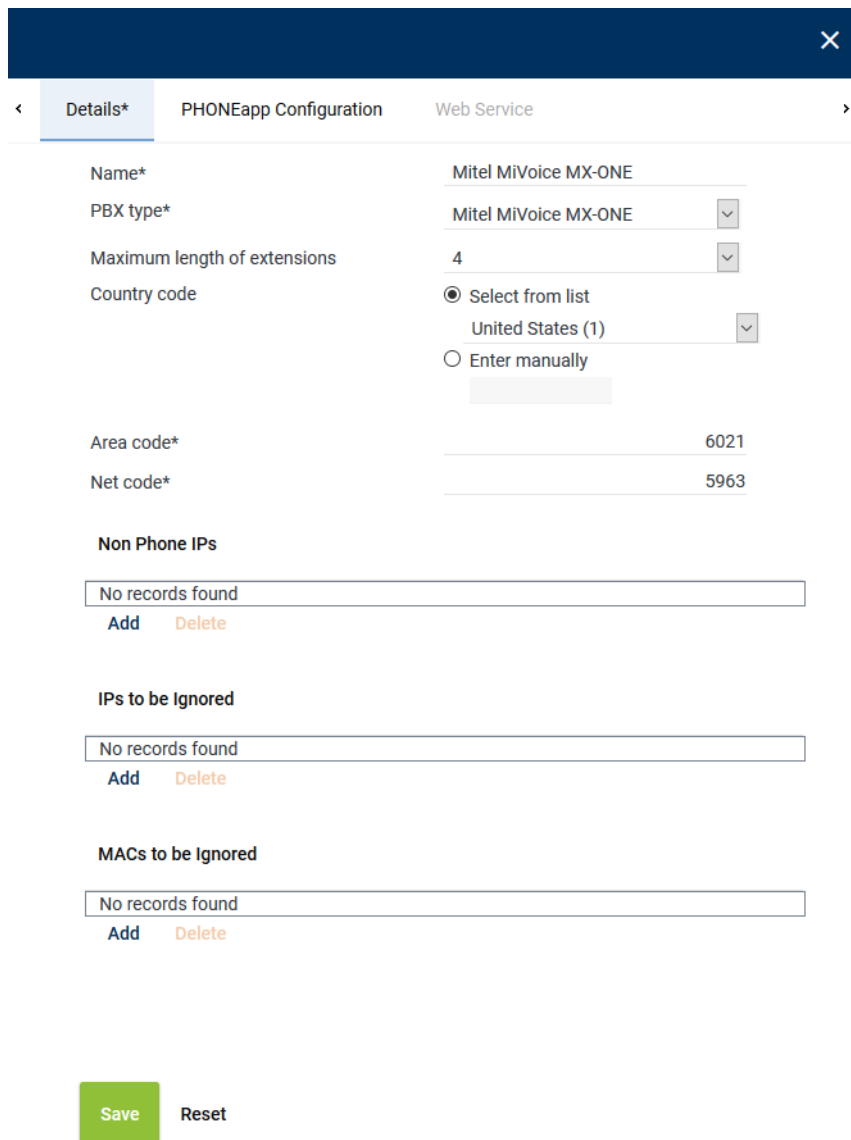


Fig. 297: Create new PBX - tab Details

- 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 PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka 094.

Parameter	Value/Description
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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

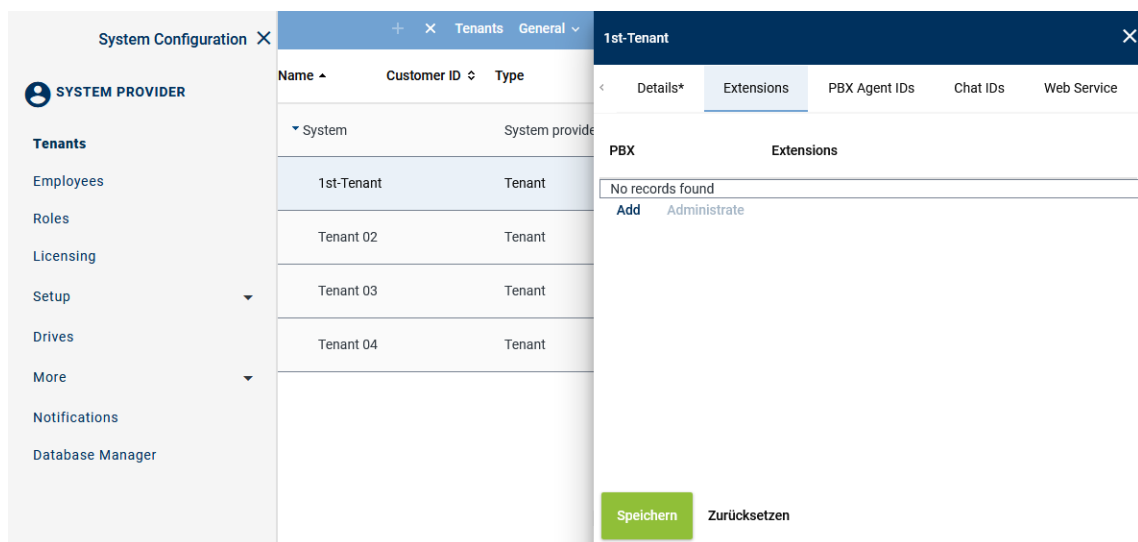


Fig. 298: Tenants - main view - tab Extensions

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. 299: 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"> ZIP TXT CSV <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> Click on the button ... behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective file in the Explorer and click on the button <i>Open</i>. Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA3) - Neo 7.x Rev. 2

251 / 474

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.

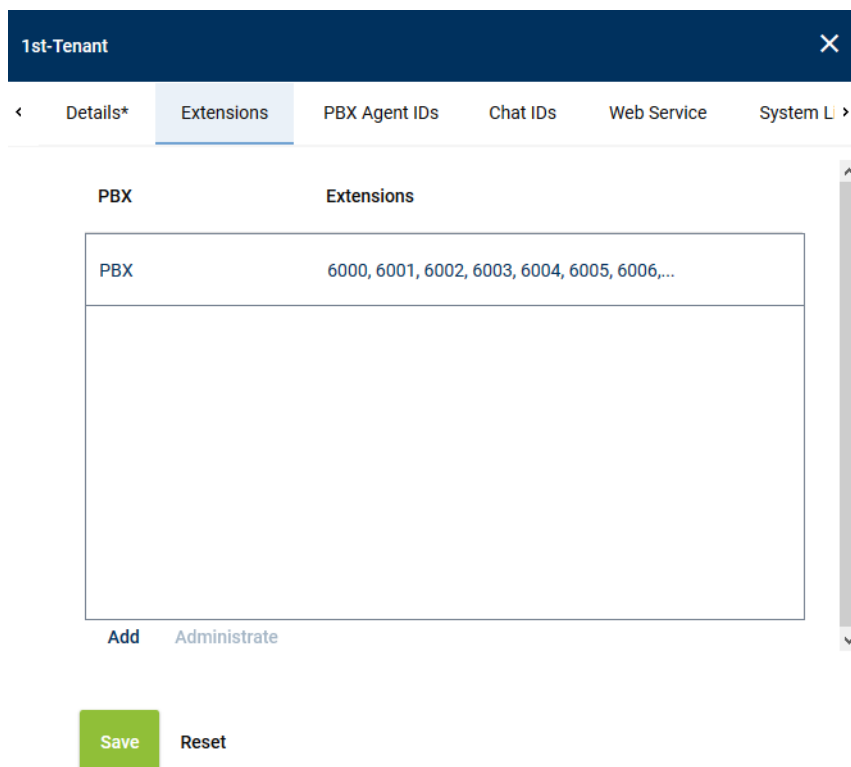


Fig. 300: Remove extensions

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.

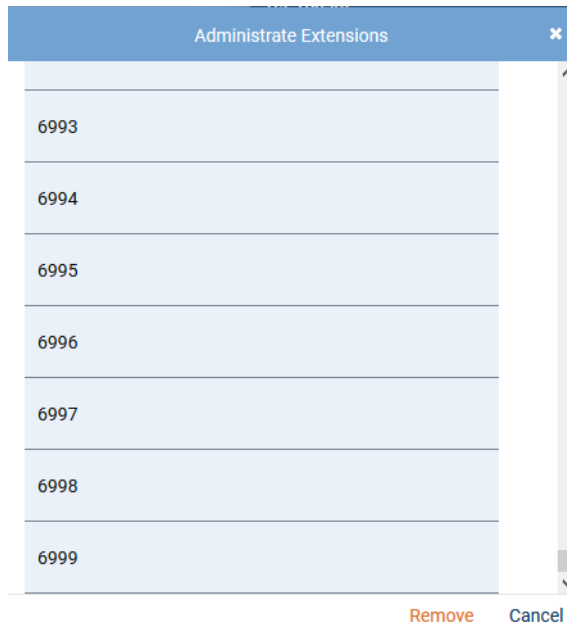


Fig. 301: Select extensions

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.

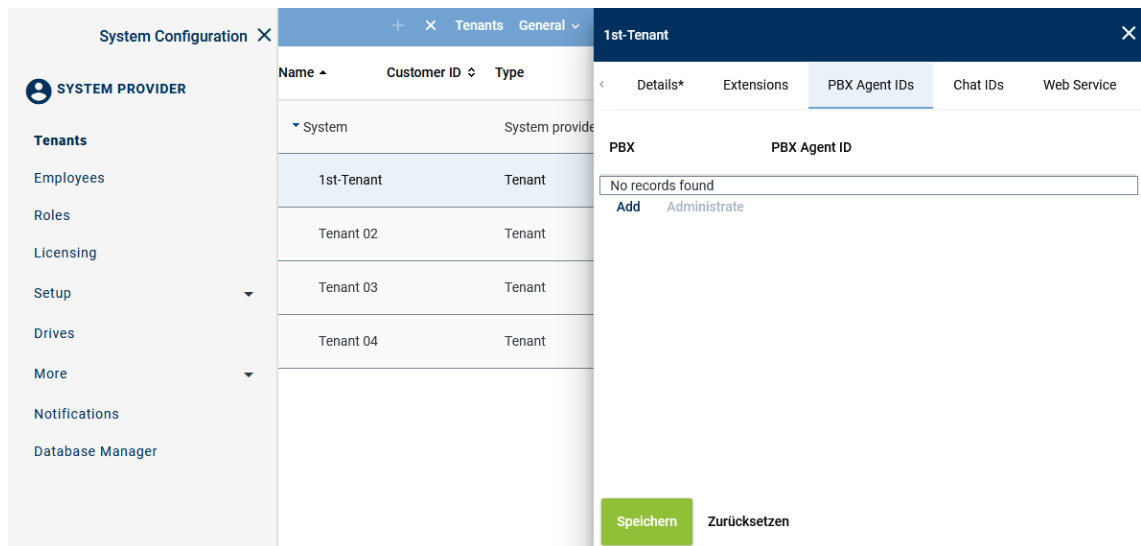


Fig. 302: Tenants - main view - tab PBX Agent ID

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:

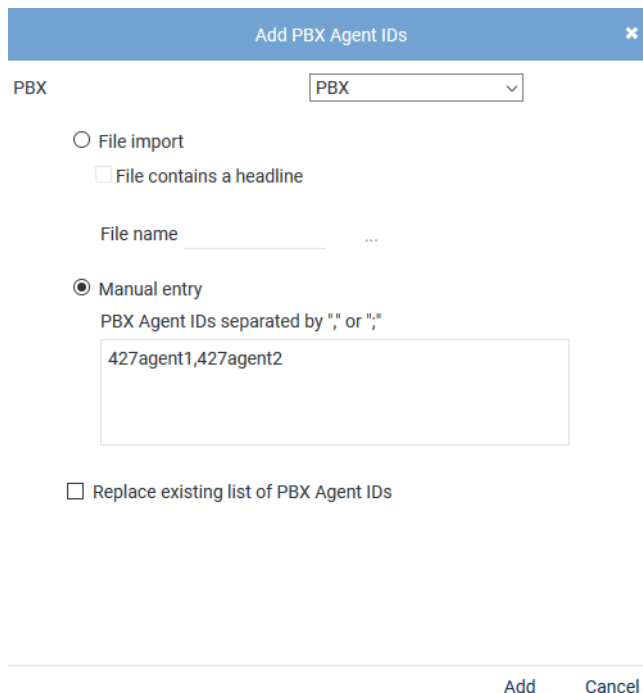




Fig. 303: Assign PBX Agent IDs to tenants

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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 304: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 305: Additional Data module main view

2. Select a data set

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

Change display name

Change Display Name v







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

Fig. 306: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 307: Additional data - configure availability

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



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

7.3.2.4.6 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:

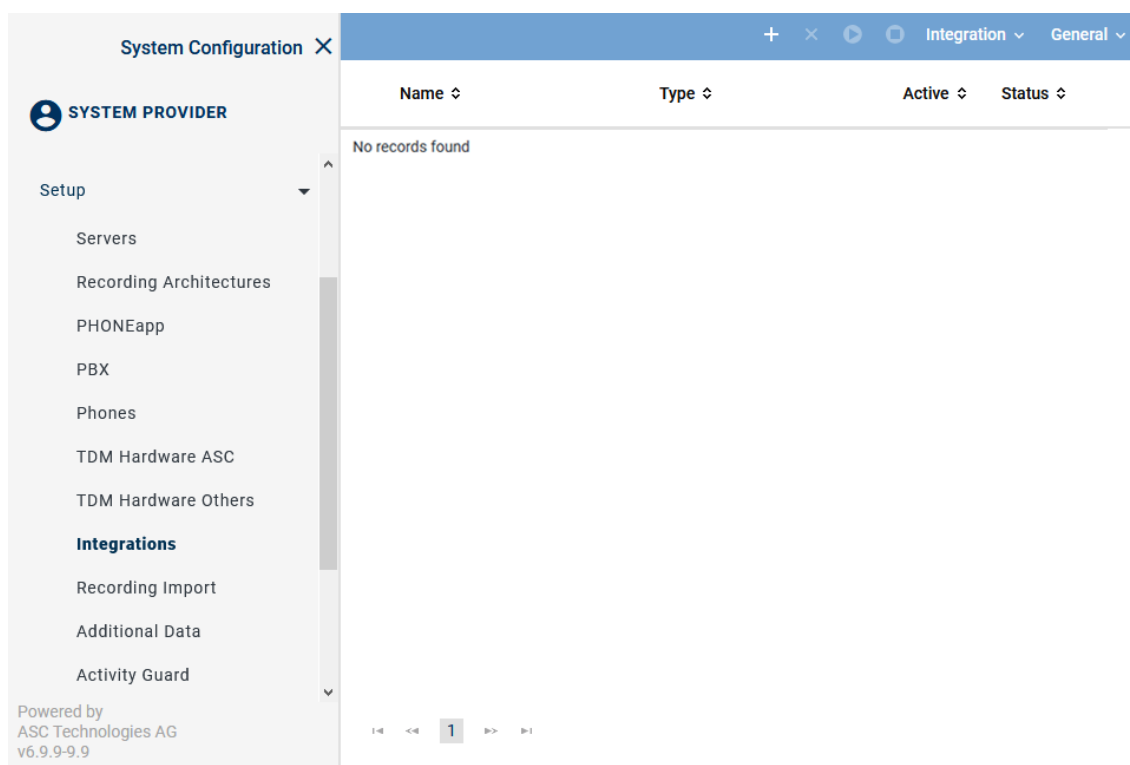




Fig. 308: Integrations - main view

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

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

Toolbar of the Integrations module

The toolbar offers the following functions.

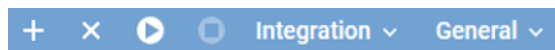






Fig. 309: Toolbar Integrations module

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

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

Import grammar

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

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

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

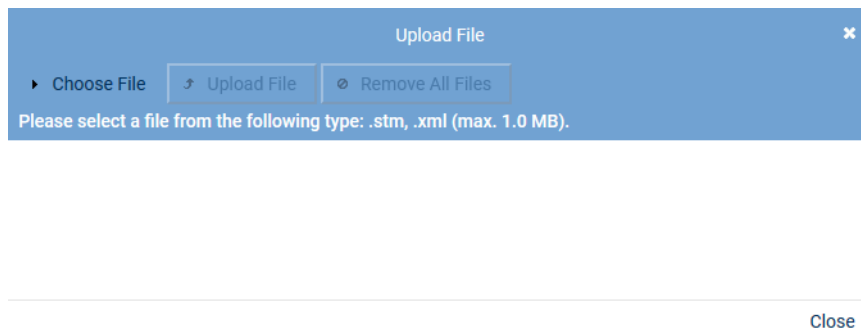


Fig. 310: Choose file

- 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*.

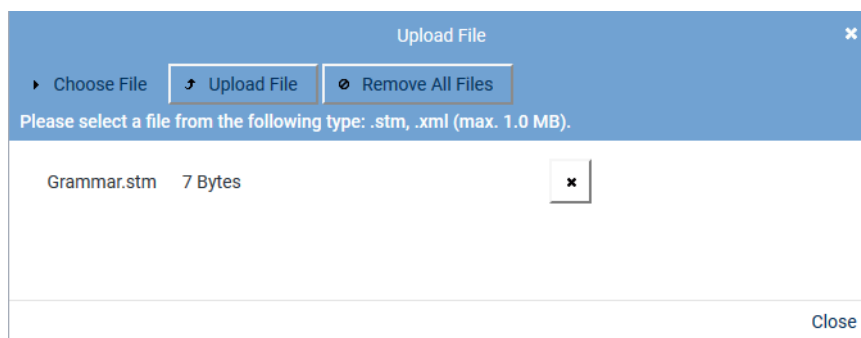



Fig. 311: Upload grammar

- 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. 312: Create integration type

2. Enter the following parameters:

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

Tab. 68: Create integration type

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

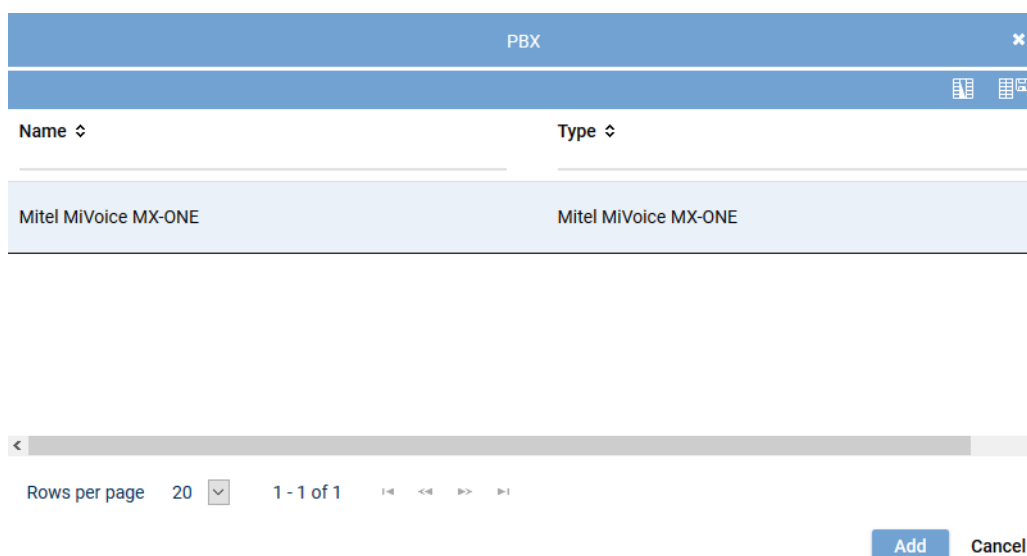
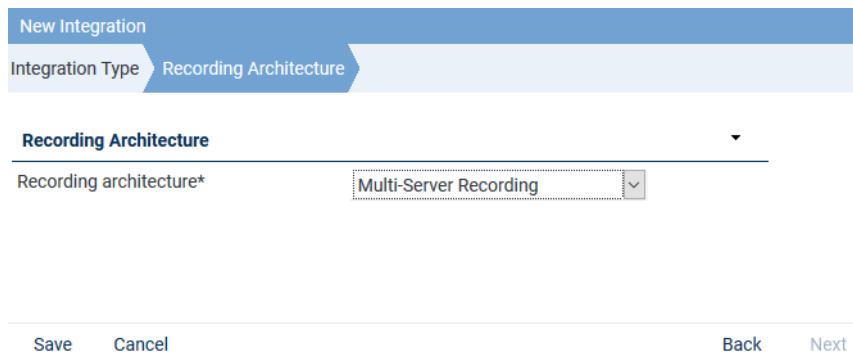


Fig. 313: Integrations - select PBX

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

Assign recording architecture for Multi-Server Recording

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Recording

Save Cancel Back Next

Fig. 314: 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. 315: 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.

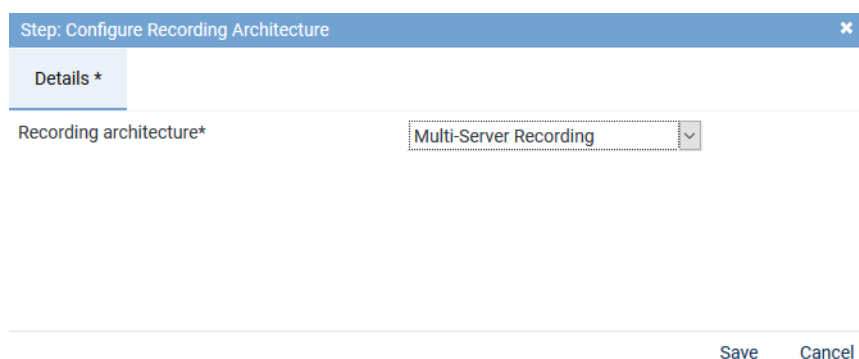



Fig. 316: Configuration step - Configure Recording Architecture

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)*

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

Save
Cancel

Fig. 317: 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. 318: 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. 319: Configure connection data

Configure Connection
✕

PBX IP address*	<input type="text" value="192.168.170.219"/>
PBX CSTA port*	<input type="text" value="8882"/>
Transport Layer Security (TLS)	<input type="checkbox"/>
<input checked="" type="checkbox"/> Activate authentication	
Application ID*	<input type="text" value="1234"/>
Password*	<input type="password" value="••••••••••••"/>

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

Fig. 320: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .
<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 chapter "Configure CSTA server", p. 14 .
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See chapter "Configure CSTA server", p. 14 .

Tab. 70: Configure connection data

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

Group field Additional Data

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

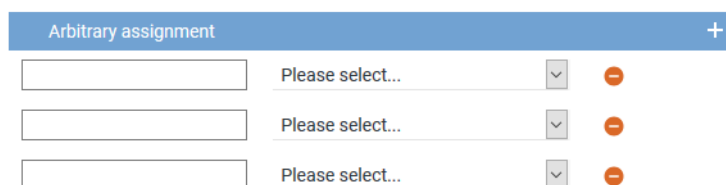



Fig. 321: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 322: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an MBG or if the regular expression does not apply for the respective phone type, recording runs via the MBG/SRC.

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 323: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

1. Select the tab **MBG** to configure the connection data for recording by means of MiVoice Border Gateway.

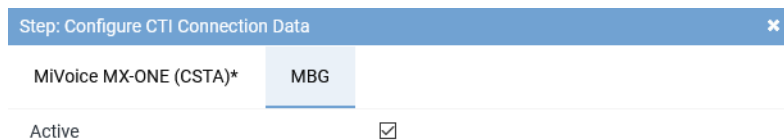


Fig. 324: Activate CTIconnect connection data for MBG

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.

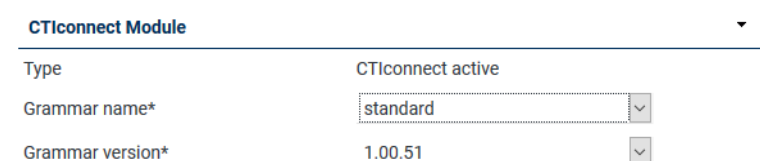


Fig. 325: Configure CTIconnect module

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.

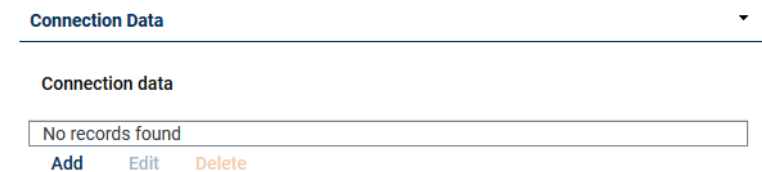


Fig. 326: Group field Connection Data

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

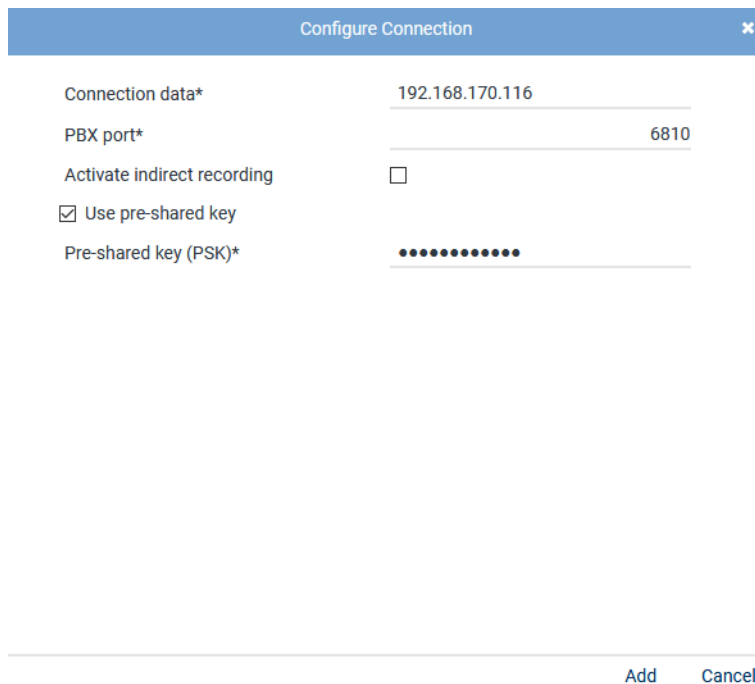


Fig. 327: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , 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 MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

Tab. 72: Configure connection data



A maximum of 20 MBG connections are possible.

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

Group field Additional Data MBG

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

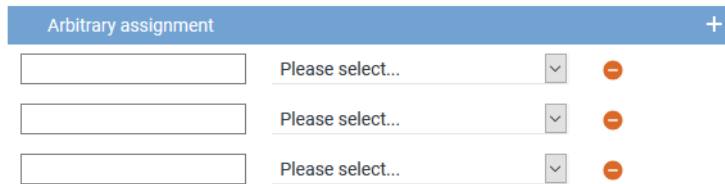



Fig. 328: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.




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



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

Configure monitor points 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.

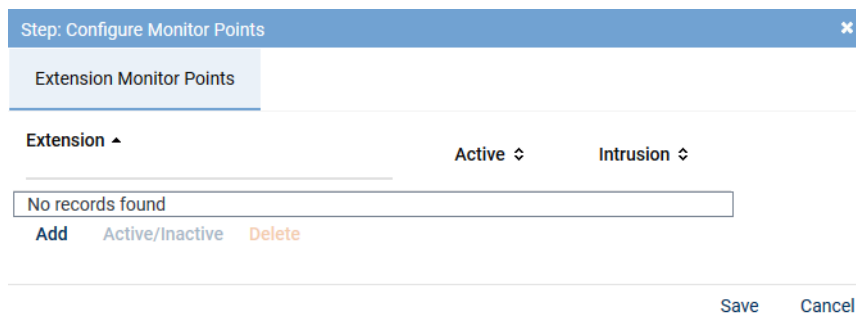


Fig. 329: Configuration step - configure monitor points

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.

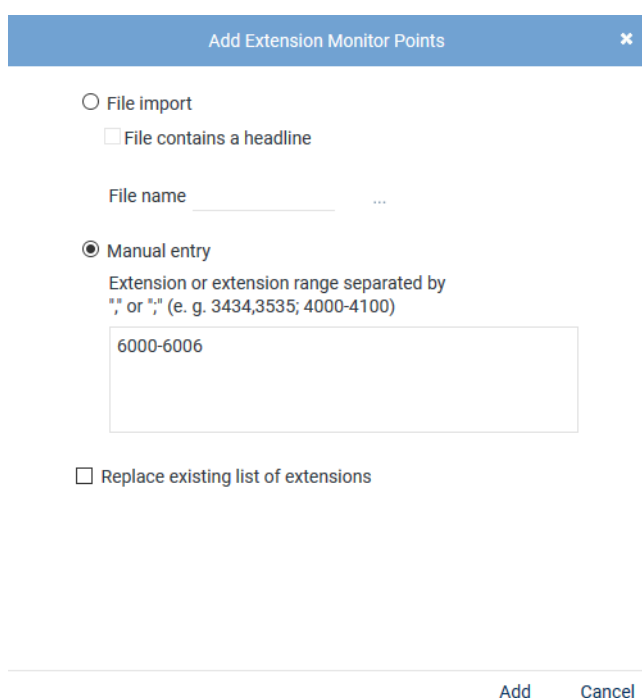






Fig. 330: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
File contains a headline	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.</p>
File name	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p>

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

Fig. 331: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at

	the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
<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. 332: 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. 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.

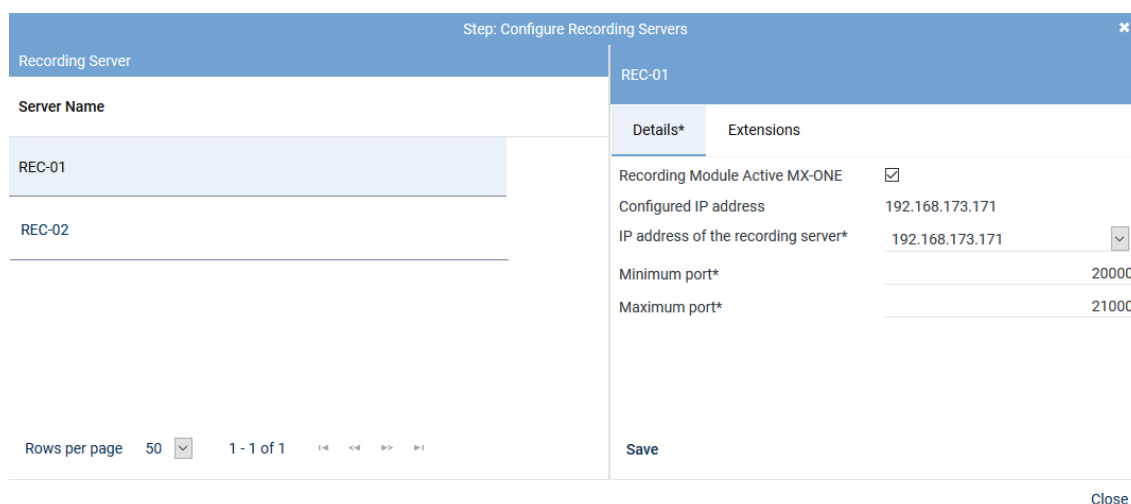


Fig. 333: Configuration step - Configure recording servers

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

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

Tab. 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*.

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*.

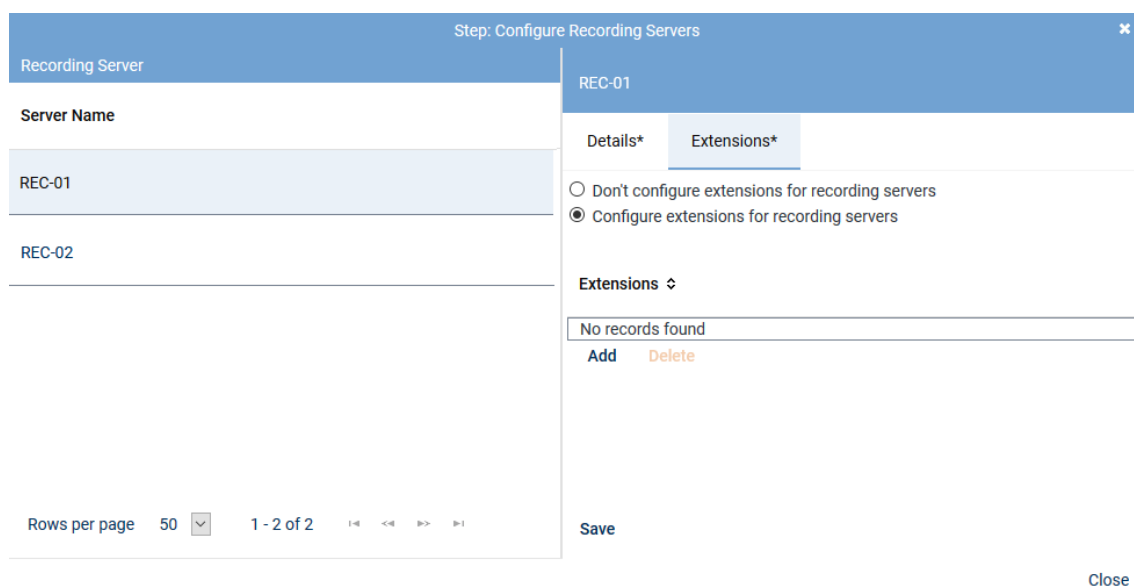


Fig. 334: Tab Extensions

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.

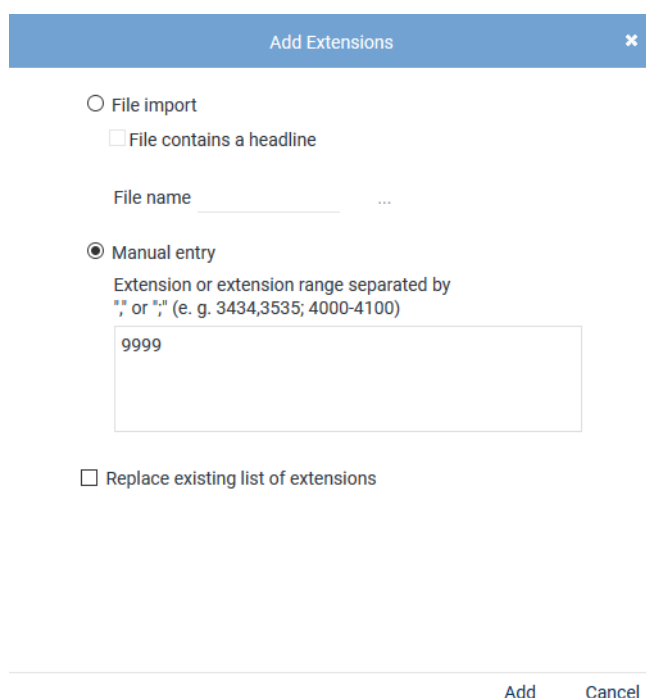


Fig. 335: Add extensions

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.

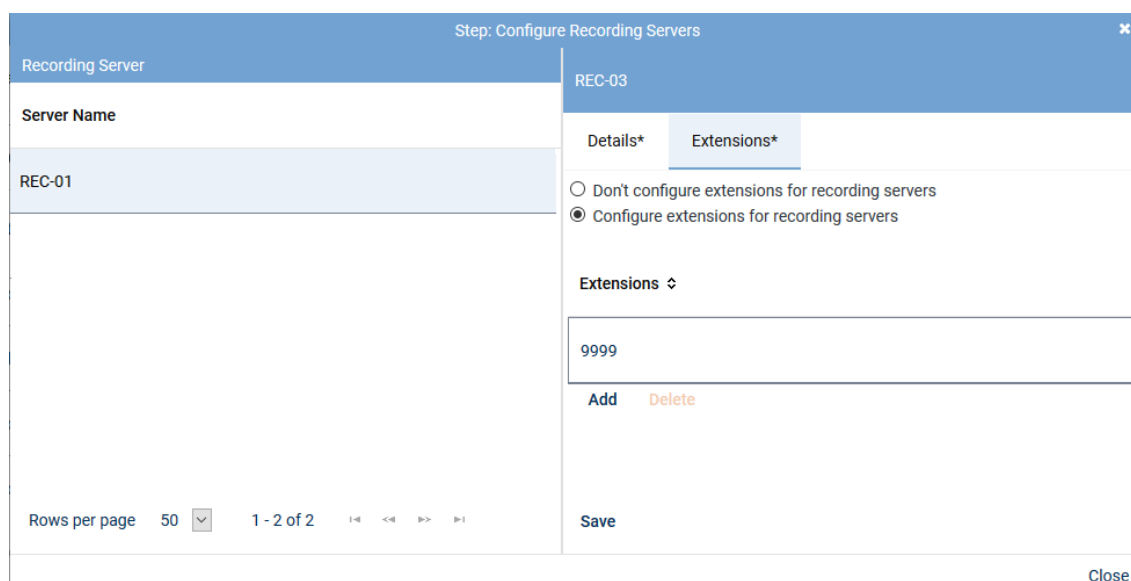


Fig. 336: Added extensions

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

Configure add-on



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

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



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



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. 337: 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. 75: 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. 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

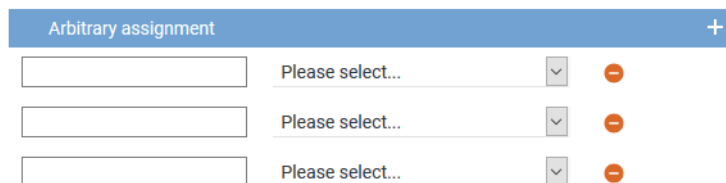



Fig. 338: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

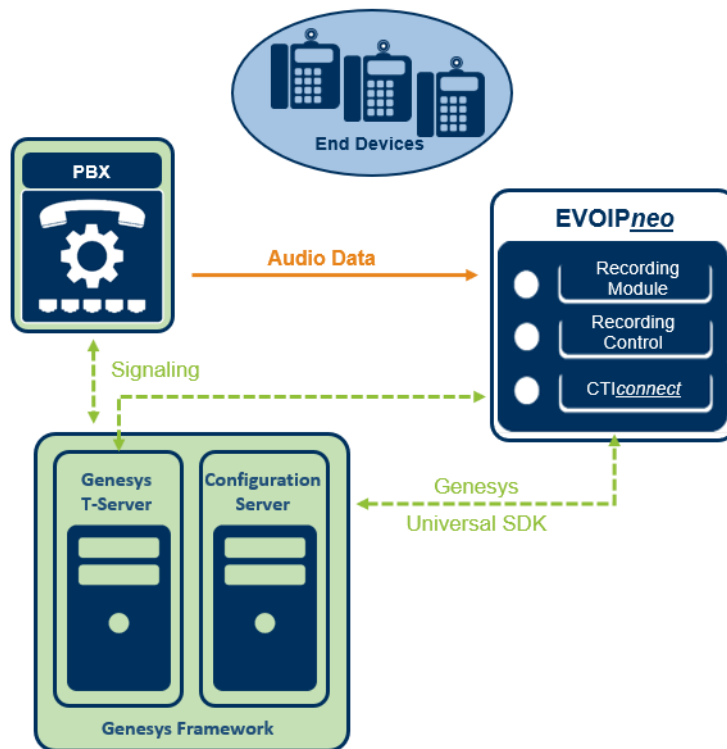


Fig. 339: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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*.

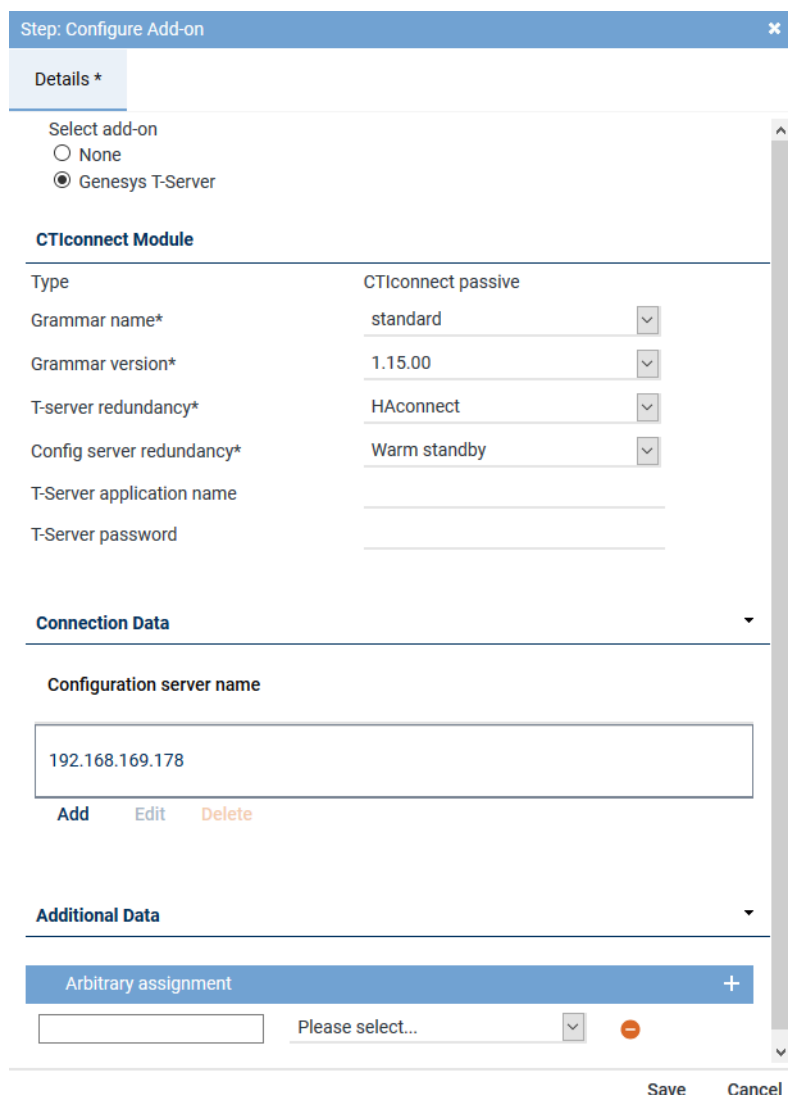


Fig. 340: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

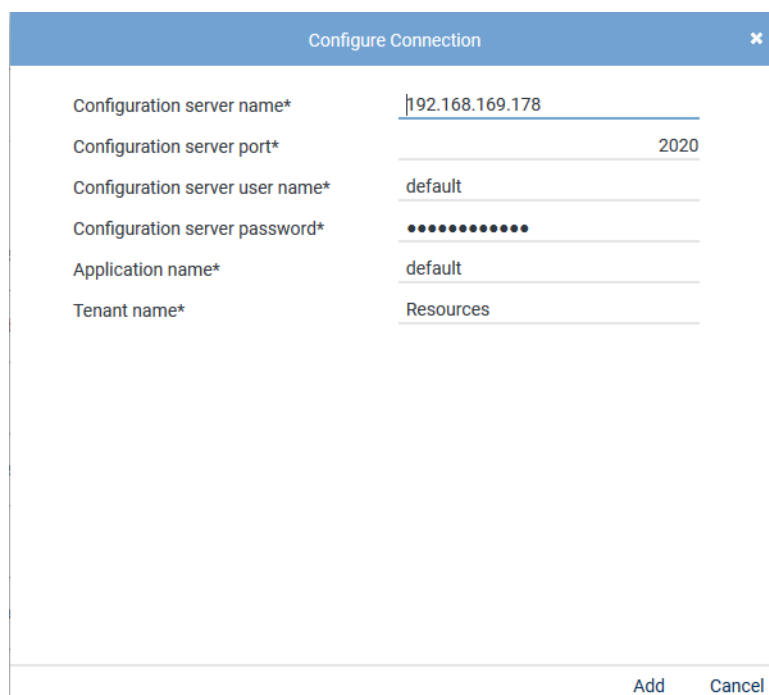
Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	<p>From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.</p> <ul style="list-style-type: none"> • <i>No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

Tab. 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:



Configure Connection

Configuration server name*

192.168.169.178

Configuration server port*

2020

Configuration server user name*

default

Configuration server password*

••••••••••

Application name*

default

Tenant name*

Resources

Add

Cancel

Fig. 341: 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.
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

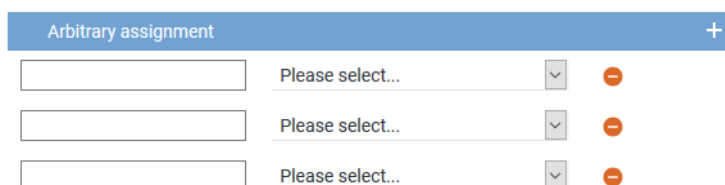




Fig. 342: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.

- Click on the button **Save** in the detail view to save the settings and complete this configuration step.

Configure miscellaneous settings

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

⇒ The window *Step: Miscellaneous Settings* appears.

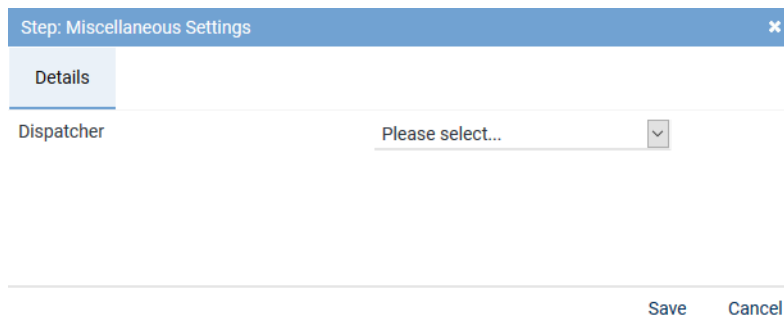


Fig. 343: Configure miscellaneous settings

- 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. 344: 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.

Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA	✔	✔
Name ↕	Type ↕	Active ↕	Status ↕	

Fig. 345: 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.

1. To deactivate the integration, click on the icon  (*Deactivate*) in the toolbar.

- ⇒ In the column *Active*, the icon  (*Inactive*) appears.
- ⇒ The icon  (*Delete*) becomes active in the toolbar.





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

Fig. 346: Deactivate integration

2. 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.

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

System Configuration X		⏮ 🔍 ⏭ + × ⏮ ⏭ Recording Architecture ▾ General ▾			
SYSTEM PROVIDER		Name ↕	Type ↕	Active	S
Setup		No records found			
Servers					
Recording Architectures					
PHONEapp					
PBX					
Phones					
TDM Hardware ASC					
TDM Hardware Others					
Integrations					
Recording Import					
Additional Data					
Activity Guard					
Powered by ASC Technologies AG v6.9.9-9.9		Rows per page 50 ▾ 1 - 1 of 1 < << >> >			

Fig. 347: Recording architectures - main view

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

	<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. 348: 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>NOTICE! 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>NOTICE! 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"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>


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



For detailed 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.

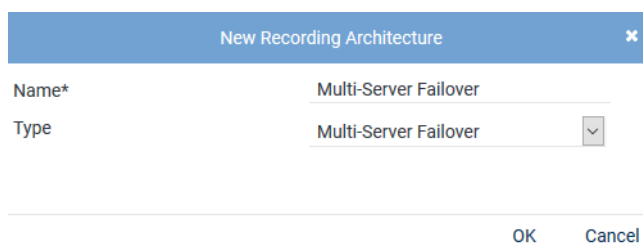


Fig. 349: Create recording architecture - Multi-Server Failover

- 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 Failover*.
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.

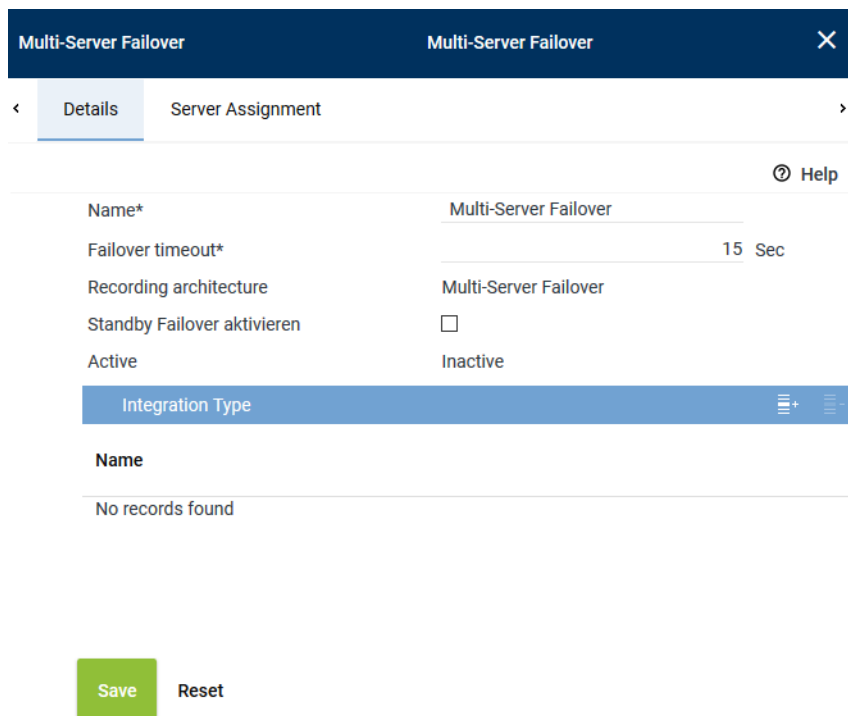



Fig. 350: Recording architecture - tab Details - Multi-Server Failover

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. 447](#).

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

Add integration type

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

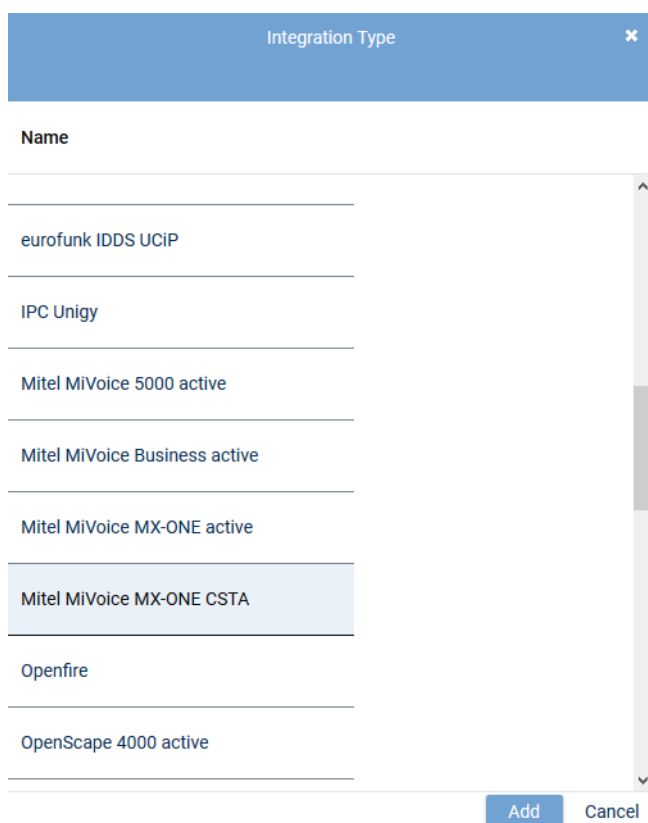


Fig. 351: Select integration type



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.

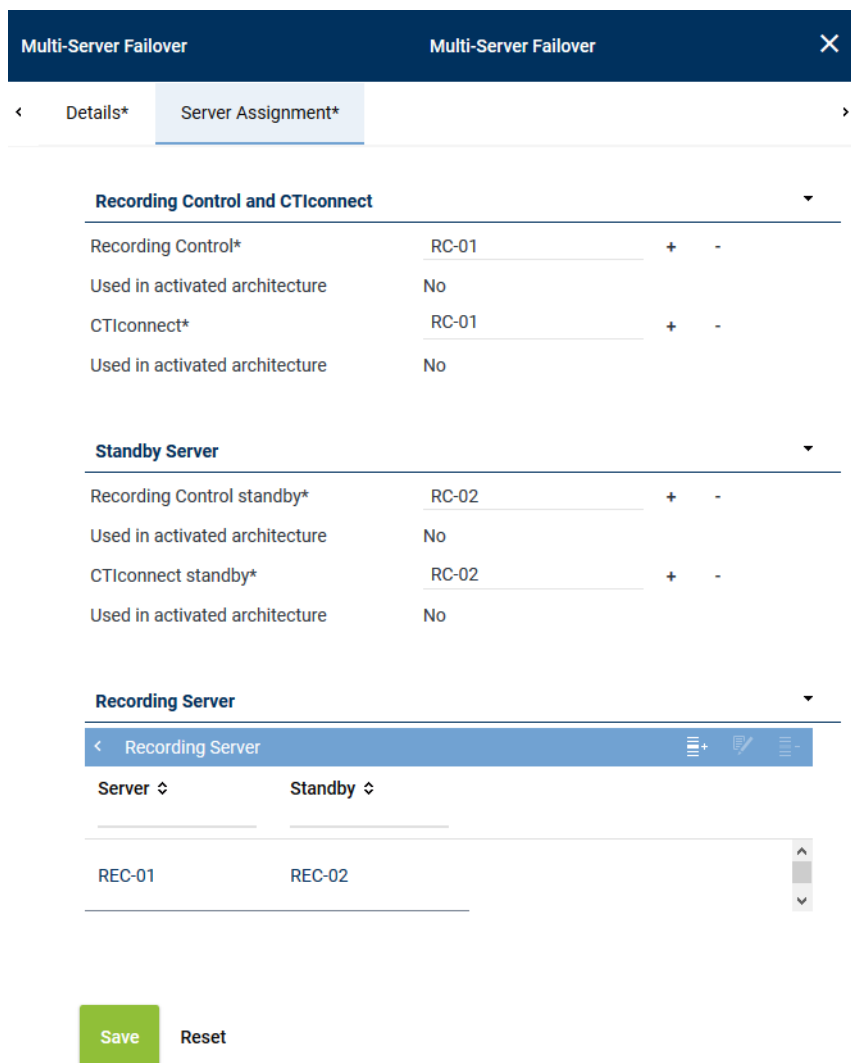
- Select *Mitel MiVoice MX-ONE CSTA* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign server for Multi-Server Failover

- Click on the tab *Server Assignment* to assign the recording components to the corresponding recording servers for the *Multi-Server Failover* recording architecture.

Group field Recording Control and CTIconnect

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



The screenshot shows the 'Multi-Server Failover' configuration window with the 'Server Assignment' tab selected. The window is divided into three main sections: 'Recording Control and CTIconnect', 'Standby Server', and 'Recording Server'.

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

Server	Standby
REC-01	REC-02

At the bottom of the window, there are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 352: 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. 353: 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	<div style="background-color: #ccc; width: 10px; height: 10px; margin: 0 auto;"></div>

Save



Reset

Fig. 354: Add Recording Server




2. As described in the previous steps, go to the entry field *Primary server* and click on the icon  to select the primary server on which the recording is supposed to run.
3. In the entry field *Standby server*, click on the icon  to select the standby server which is supposed to take over recording in case of an error.
4. Select the recording type you would like to use for these servers by activating the check box.



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



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

Activate recording architecture

1. Once all servers have been assigned, click on the button *Save*.
2. Select the recording architecture in the main view so that the icon  (*Activate*) in the 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 Failover	Multi-Server Failover	✓	✗

Fig. 355: 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. 447](#).



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. 356: 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. 357: 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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.
<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations", p. 295 .
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

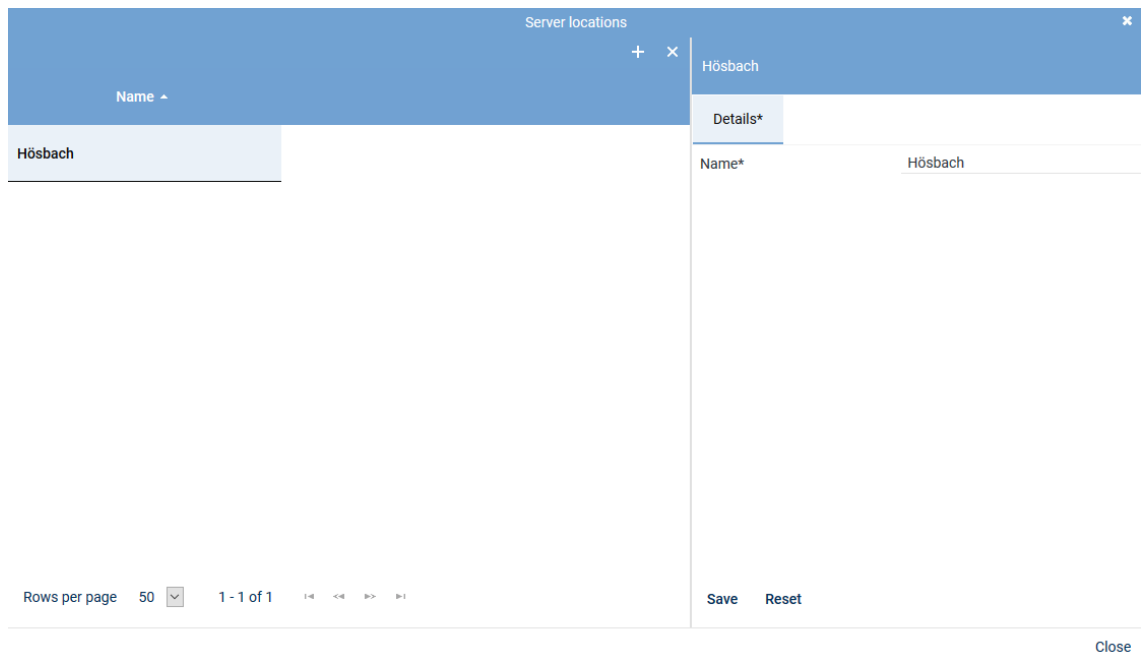



Fig. 358: Add server locations

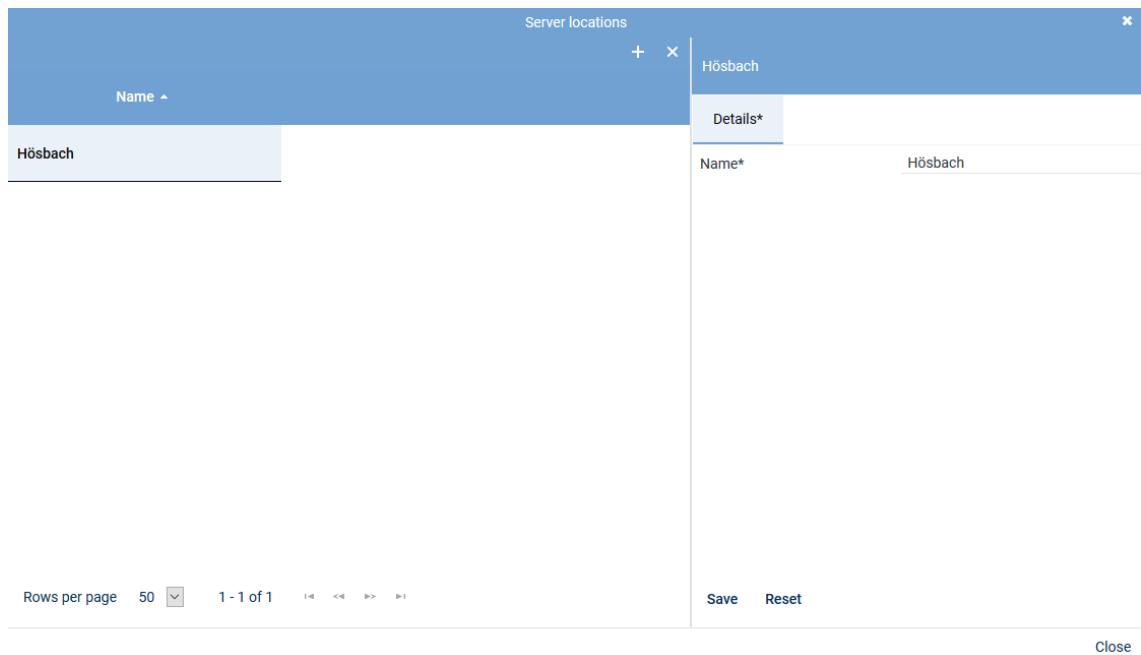
- Click on the icon  (*Create*) in the toolbar of the window *Server Locations*.
- Enter the name of the location on the right side in the tab *Details*.
- To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
- To add further locations, repeat the last 3 steps.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



Server locations

Name
Hösbach

Details*


Name* Hösbach

Rows per page 50 1 - 1 of 1

Save Reset

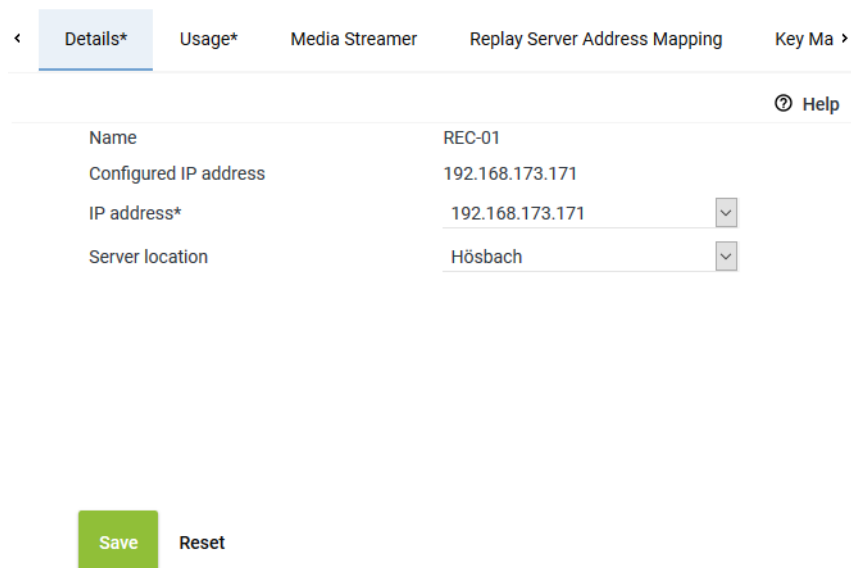
Close

Fig. 359: 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. 360: 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.

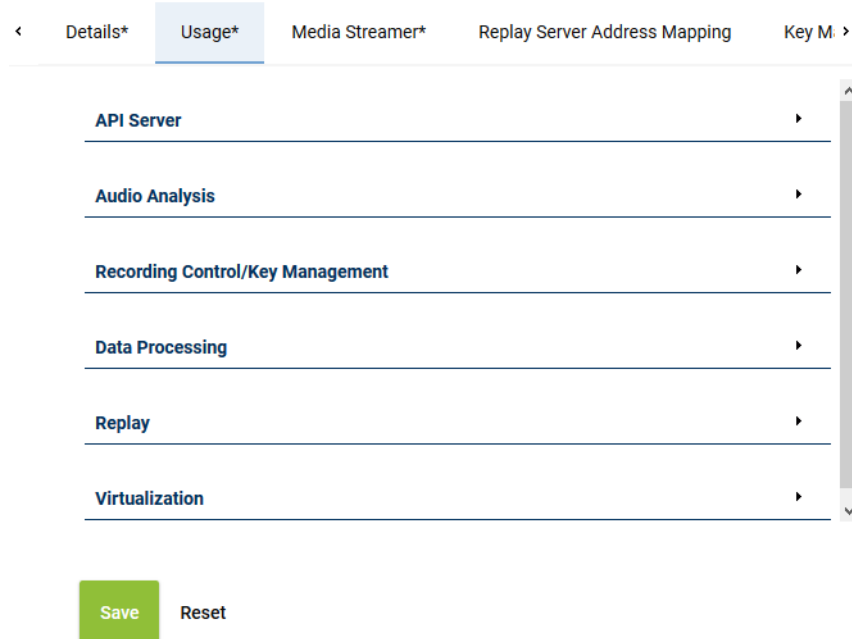


Fig. 361: Servers - tab usage

Group field API Server

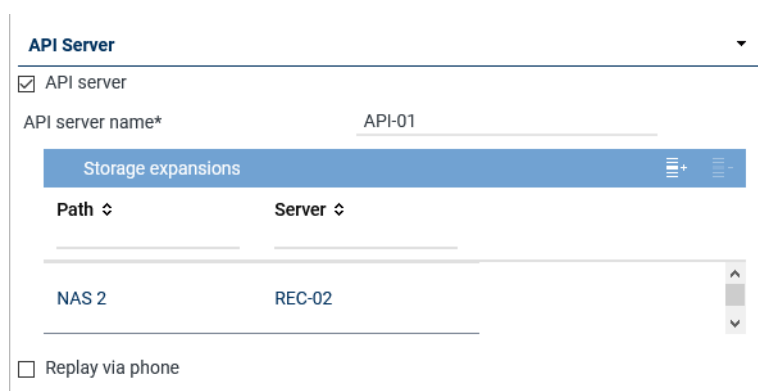




Fig. 362: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 308.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> • By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 300. • By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list. <p>If you use several recording servers in your system for which storage expansions have been configured, you can add any storage expansion of any recording server on every API server of the system.</p>
<i>Replay via phone</i>	<p>Activate this function if you would like to use the functions <i>Replay via phone</i> or <i>Last Call Repeat</i>.</p> <p><input checked="" type="checkbox"/> = Function has been activated.</p> <p><input type="checkbox"/> = Function has not been activated.</p> <p>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 307. 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. 363: 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

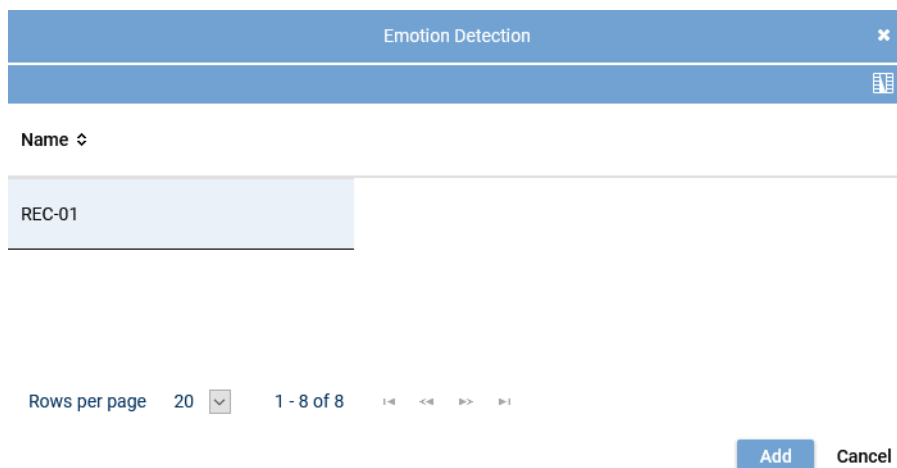
☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 364: Group field Audio Analysis

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

Tab. 79: Configure audio analysis



Emotion Detection

Name ↕

REC-01

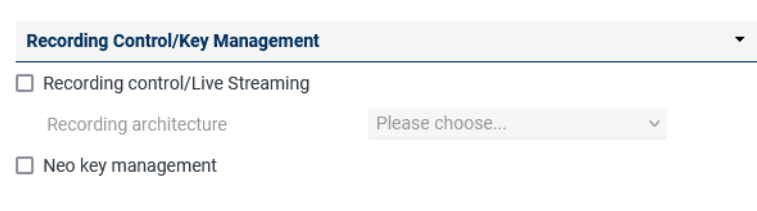
Rows per page 20 1 - 8 of 8

Add Cancel

Fig. 365: 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/Live Streaming

Recording architecture Please choose...

☐ Neo key management

Fig. 366: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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. 367: 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"> By clicking on the icon  (Add), you can add the target server, see chapter "Add target server to a list", p. 304. By clicking on the icon  (Remove), you can remove target servers from the list. <p>NOTICE! 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>

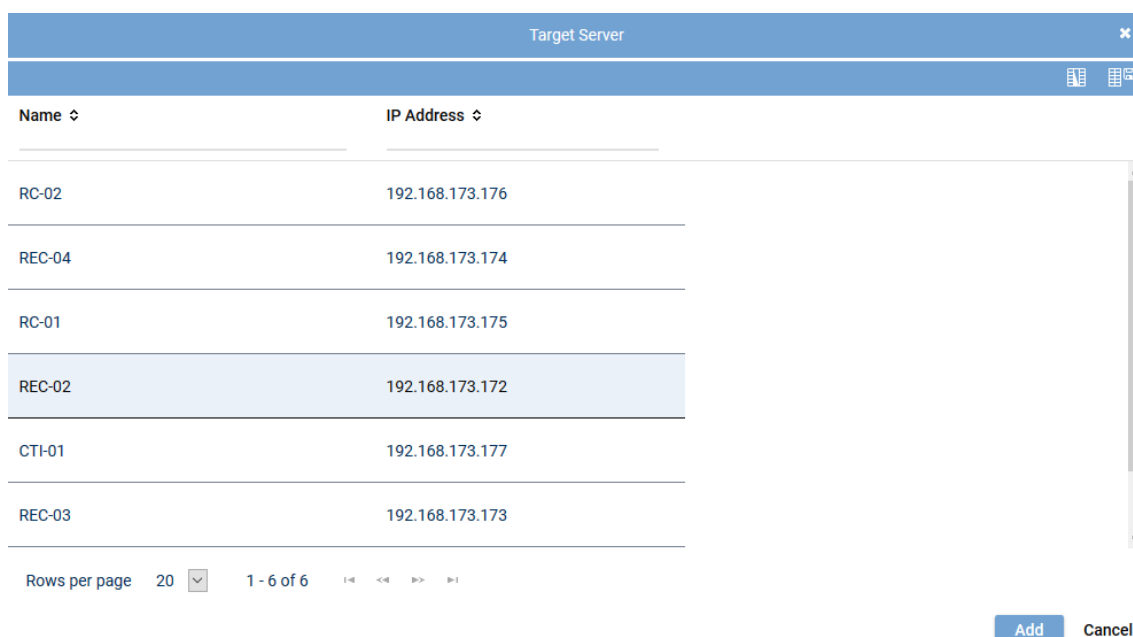
Parameter	Value/Description
	<p>ferred to be saved. The drop-down list displays all servers on which the function <i>data storage</i> has been activated. The data is copied to the target server and saved there.</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 304. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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"> <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. <p>NOTICE! For the export from Neo to Neo, 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"> <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.

Parameter	Value/Description
	NOTICE! 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

Rows per page: 20 | 1 - 6 of 6 | Add | Cancel

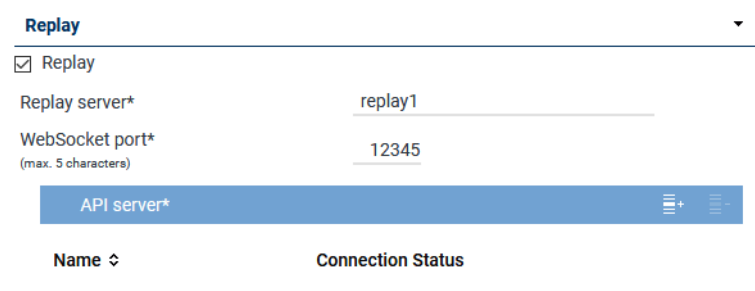
Fig. 368: Select server



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. 369: 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 API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add the API server, see chapter "Add API server to a list", p. 305. By clicking on the icon  (<i>Remove</i>), you can remove selected API servers from the list.

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. 370: Select server



Only those servers are available on which the **API** service has been installed and activated.
See [chapter "Group field API Server", p. 298](#).

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. 371: Group field Virtualization

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

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

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

Save

Reset

Fig. 372: Servers module - tab Media Streamer

- Enter the following parameters:

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

	If no PBX has been created in the system yet, you can create a PBX via the blue bar <i>PBX</i> .
<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 8000.</p>
<i>Media streamer IP address</i>	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</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>NOTICE! The port range must not have less than 64 ports.</p>
<i>Transport protocol</i>	<p>From the drop-down list, select the transport protocol type you would like to use for the SIP communication.</p> <p>TCP = unencrypted</p> <p>UDP = unencrypted</p> <p>TLS = encrypted</p> <p>If an external analog gateway has been integrated, select <i>UDP</i> in the drop-down list.</p>
<i>SIP signaling port</i>	<p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p>
<i>User name</i>	Enter the user name for the authentication on the SIP server.
<i>Password</i>	Enter the password for the authentication on the SIP server.
<i>PBX IP address</i>	Enter the IP address of the SIP registrar of the PBX .
<i>PBX port</i>	<p>Enter the port of the SIP registrar of the PBX.</p> <p>If an external analog gateway has been integrated, enter the value 5060.</p>
<i>Registration required</i>	<p>Select whether the SIP extension has to be registered with the SIP registrar of the PBX.</p> <p><input checked="" type="checkbox"/> = SIP extension has to be registered.</p> <p><input type="checkbox"/> = SIP extension does not have to be registered.</p> <p>If an external analog gateway has been integrated, deactivate the check box <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. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

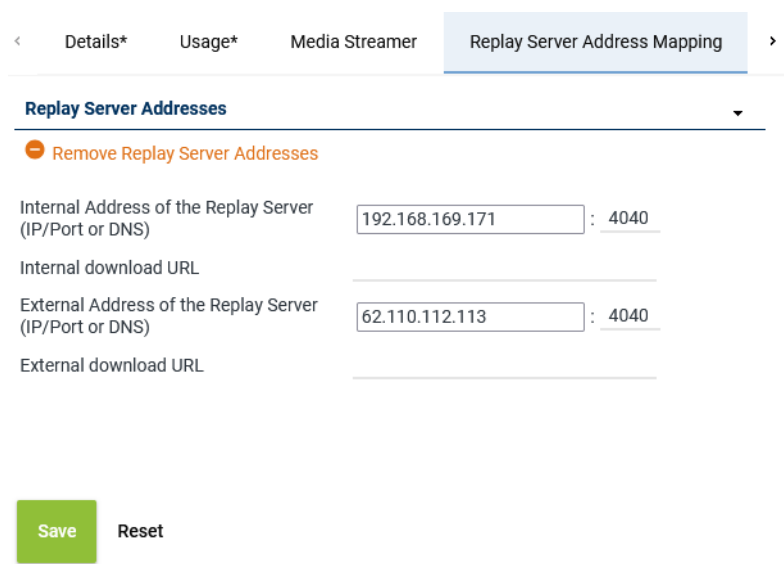



Fig. 373: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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*.

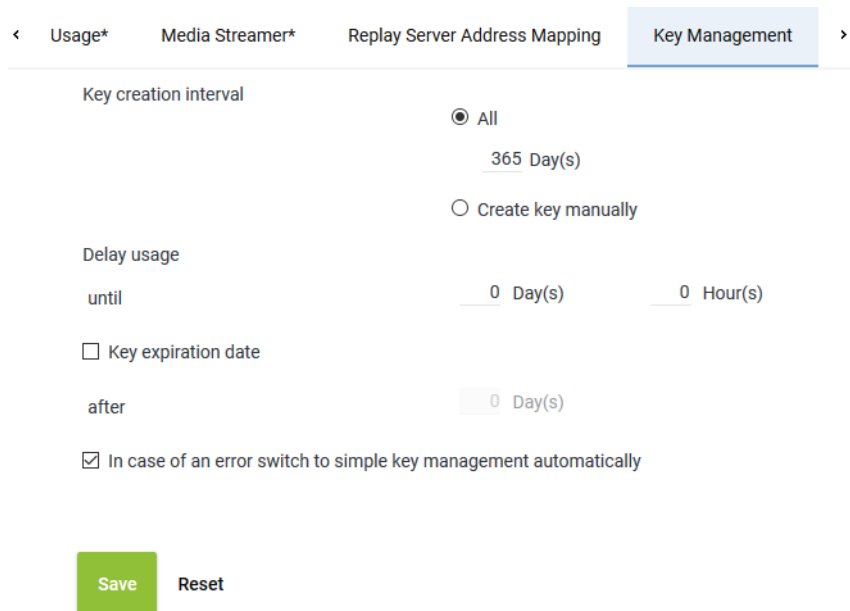


Fig. 374: Servers module - tab Key Management

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>CAUTION! All recordings which have been encrypted with a key which has meanwhile become invalid are useless and cannot be replayed anymore.</p>
<i>In case of an error ... automatically</i>	<p>Select whether simple key management is supposed to be used if the Neo 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 Neo 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 Neo 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*

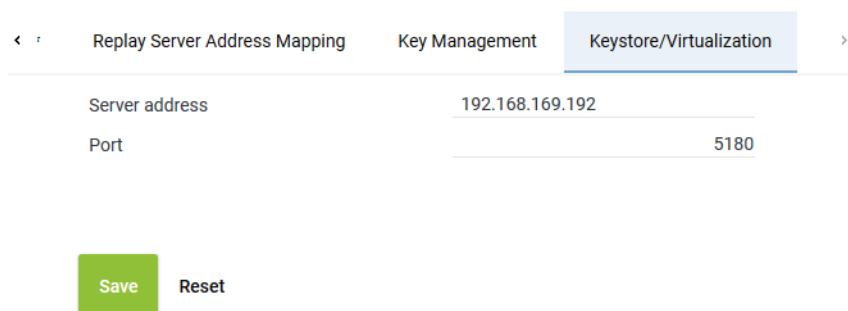
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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 Servers module, specifically the 'Keystore/Virtualization' tab. At the top, there are three tabs: 'Replay Server Address Mapping', 'Key Management', and 'Keystore/Virtualization', with the latter being the active tab. 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: a green 'Save' button and a grey 'Reset' button.

Fig. 375: Servers module - tab Keystore/Virtualization

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

	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:

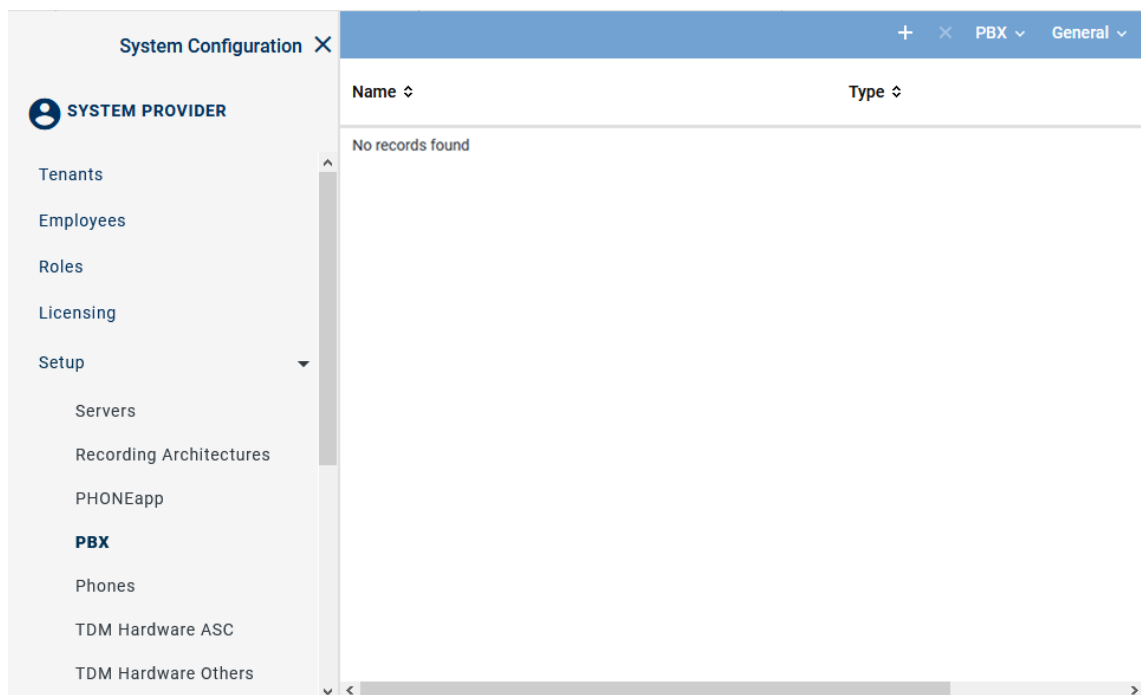


Fig. 376: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.

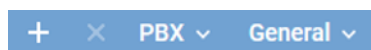




Fig. 377: Toolbar PBX module


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

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



For detailed 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. 378: Create new PBX - tab Details

2. Set the following parameters in the detail view:

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

Tab. 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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

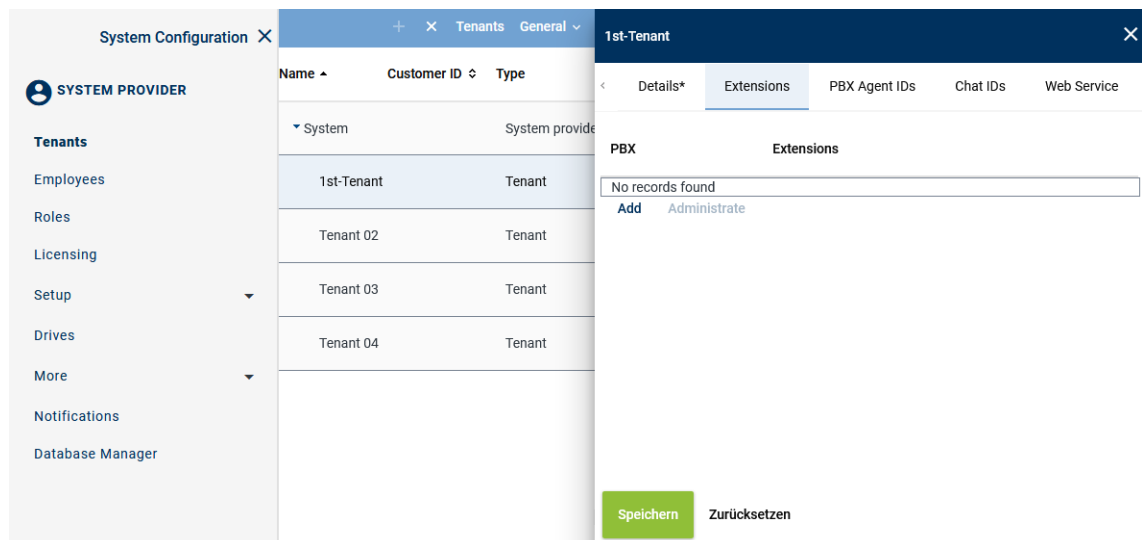


Fig. 379: Tenants - main view - tab Extensions

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. 380: 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"> • ZIP • TXT • CSV <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

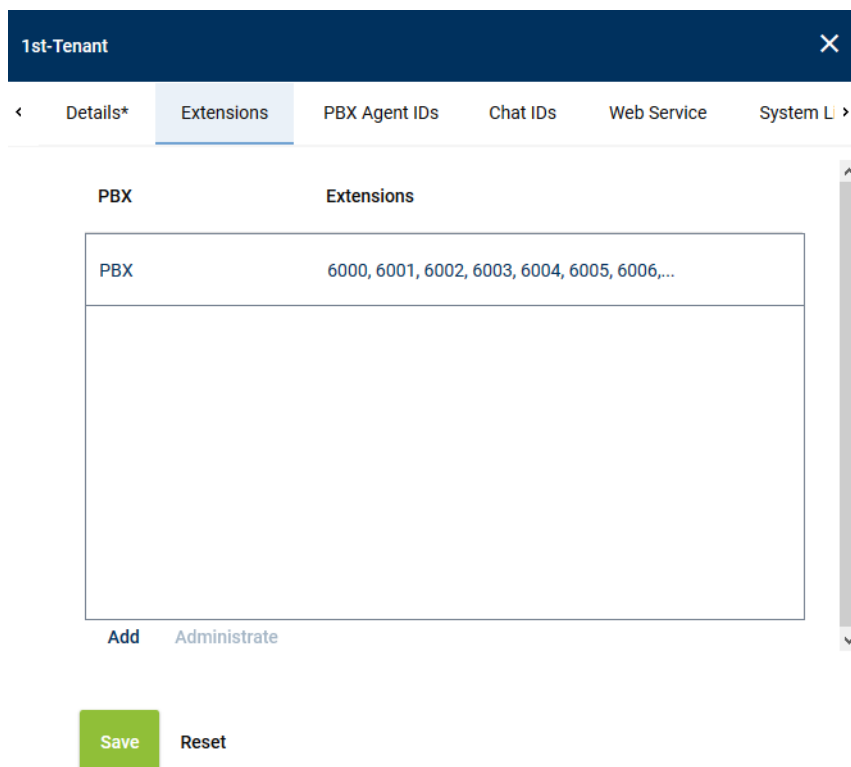


Fig. 381: Remove extensions

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. 382: 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.

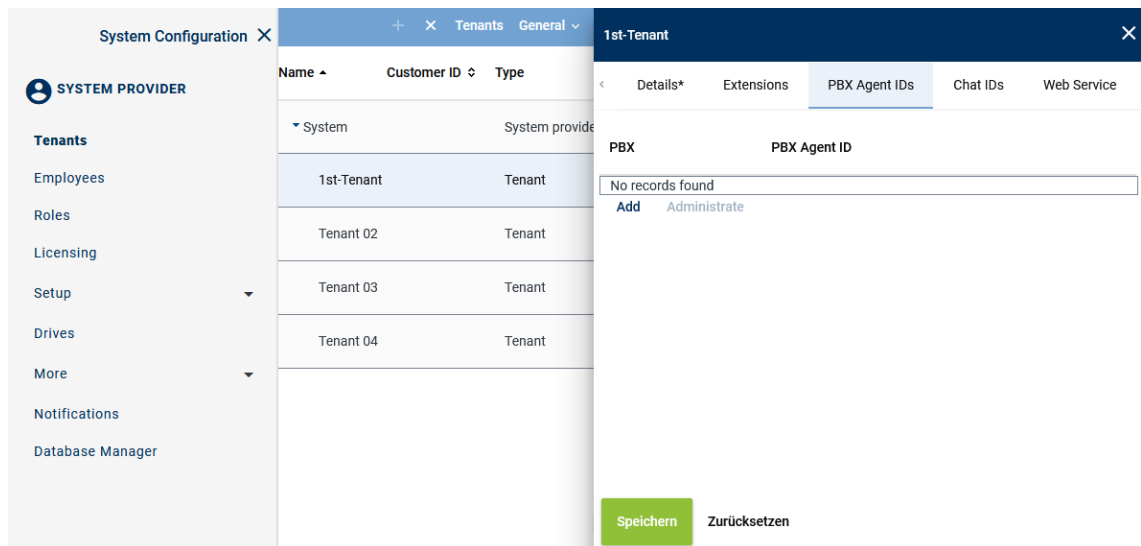
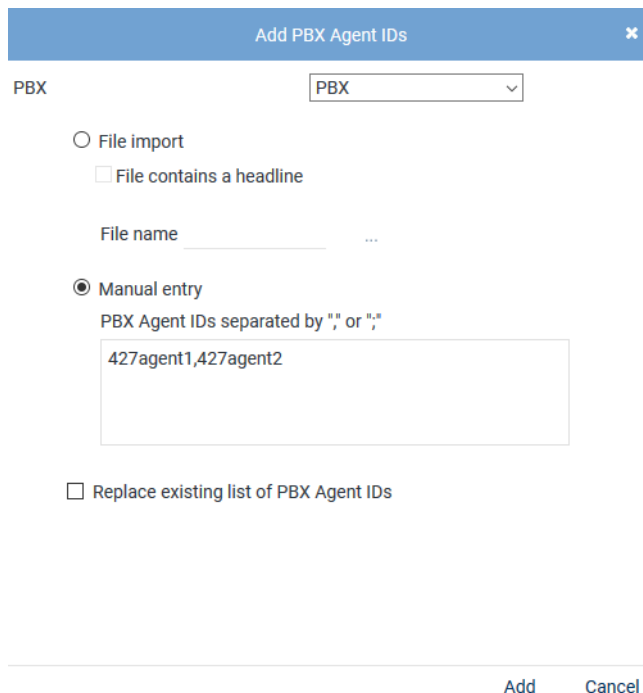


Fig. 383: Tenants - main view - tab PBX Agent ID

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 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'. Below the input field, there is a checkbox labeled 'Replace existing list of PBX Agent IDs'. At the bottom right, there are 'Add' and 'Cancel' buttons.

Fig. 384: 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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 385: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 386: Additional Data module main view

2. Select a data set

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

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. 387: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 388: Additional data - configure availability

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



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

7.3.2.5.6 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:

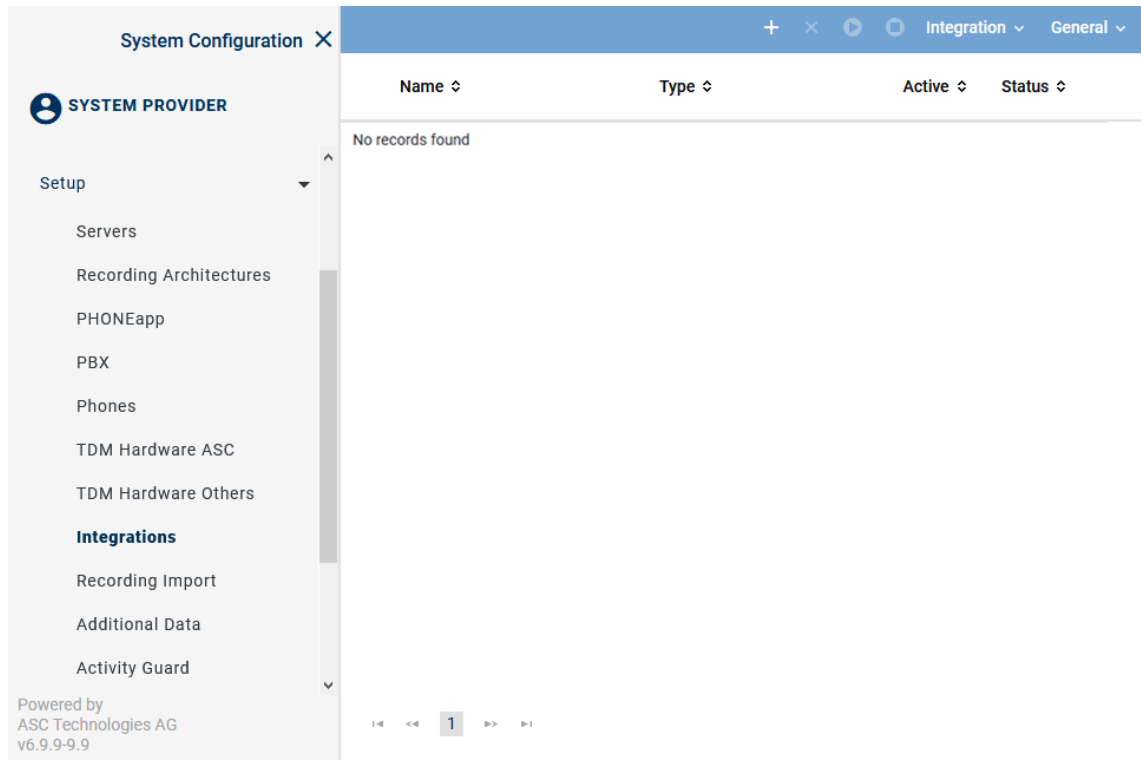




Fig. 389: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 390: Toolbar Integrations module

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

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

Import grammar

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

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

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

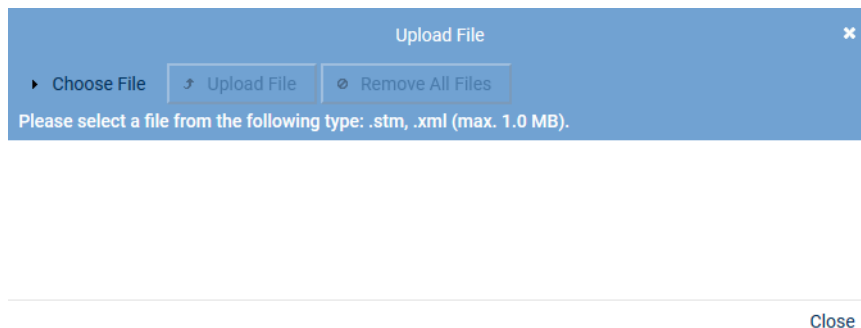


Fig. 391: Choose file

- 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*.

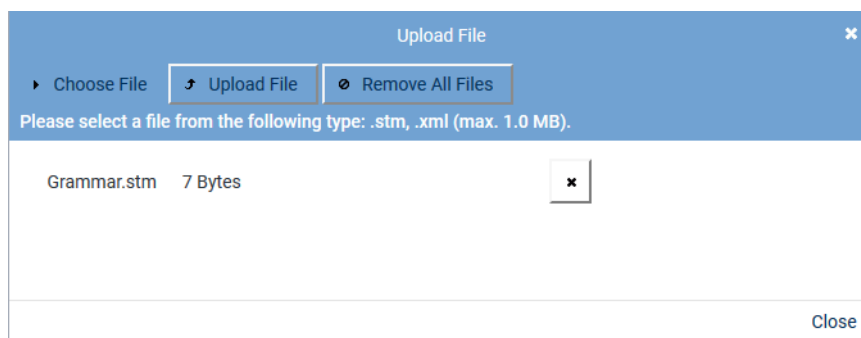



Fig. 392: Upload grammar

- 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. 393: Create integration type

2. Enter the following parameters:

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

Tab. 85: Create integration type

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

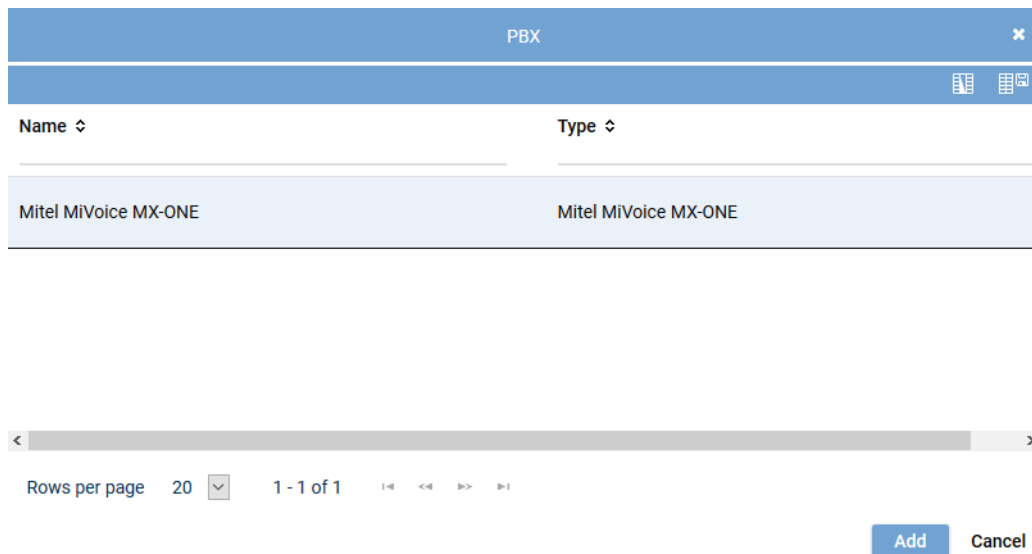
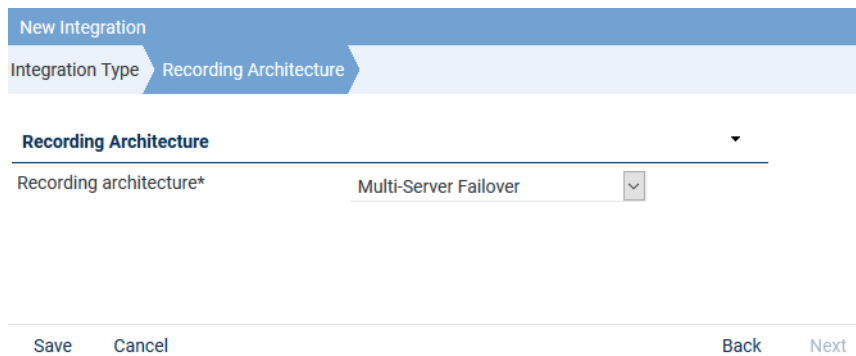


Fig. 394: Integrations - select PBX

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

Assign recording architecture for Multi-Server Failover

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* Multi-Server Failover

Save Cancel Back Next

Fig. 395: 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. 396: 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.

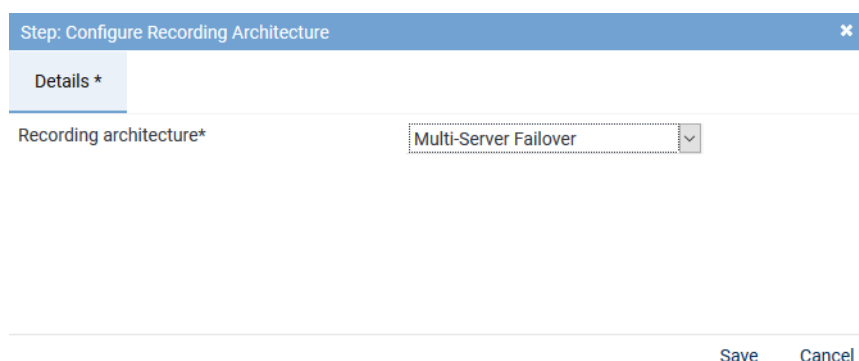



Fig. 397: Configuration step - Configure Recording Architecture

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. 398: 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. 399: 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~~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. 400: Configure connection data

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. 401: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .
<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 chapter "Configure CSTA server", p. 14 .
<i>Password</i>	Enter the password for the application ID. The password must be identical with the information in the Service Node Manager. See chapter "Configure CSTA server", p. 14 .

Tab. 87: Configure connection data

2. 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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.

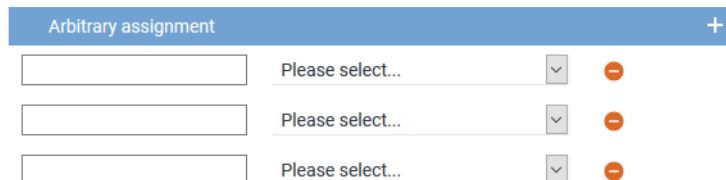


For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

Arbitrary assignment


In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.



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

Fig. 402: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information read out of the protocol is displayed in the columns in the players.
- 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.
- To add a new assignment, click on the icon  (*Create*) in the toolbar of the table.
⇒ An additional line to add another additional data type appears.
- Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 403: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an MBG or if the regular expression does not apply for the respective phone type, recording runs via the MBG/SRC.

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 404: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

1. Select the tab **MBG** to configure the connection data for recording by means of MiVoice Border Gateway.

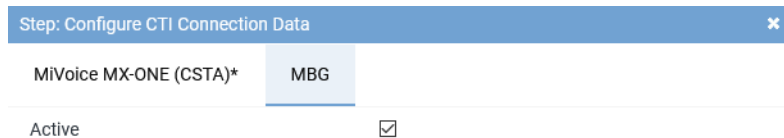


Fig. 405: Activate CTIconnect connection data for MBG

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.

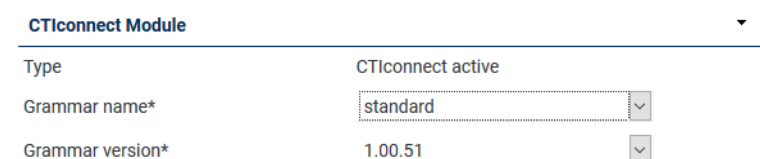


Fig. 406: Configure CTIconnect module

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.



Fig. 407: Group field Connection Data

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

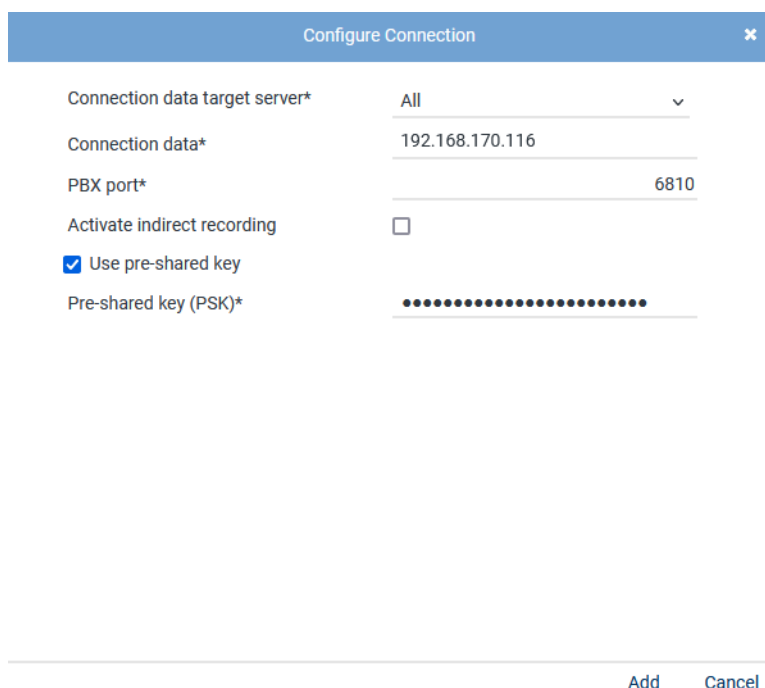


Fig. 408: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Configure target server</i>	From the drop-down list, select the option for which server the connection is intended. Select the option <i>All</i> if the connection is supposed to apply for all servers.
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , 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 MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

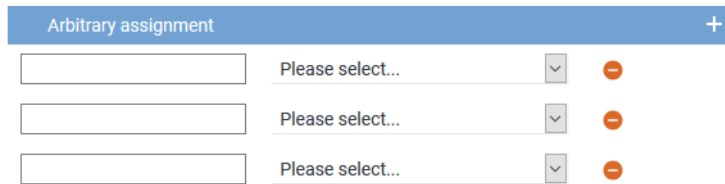



Fig. 409: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.




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



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

Configure monitor points 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.

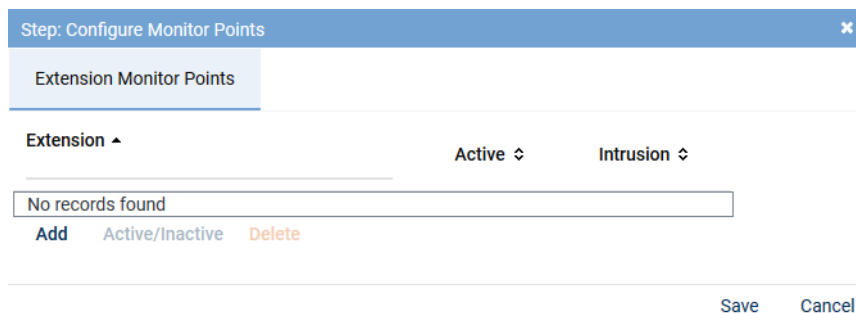


Fig. 410: Configuration step - configure monitor points

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.

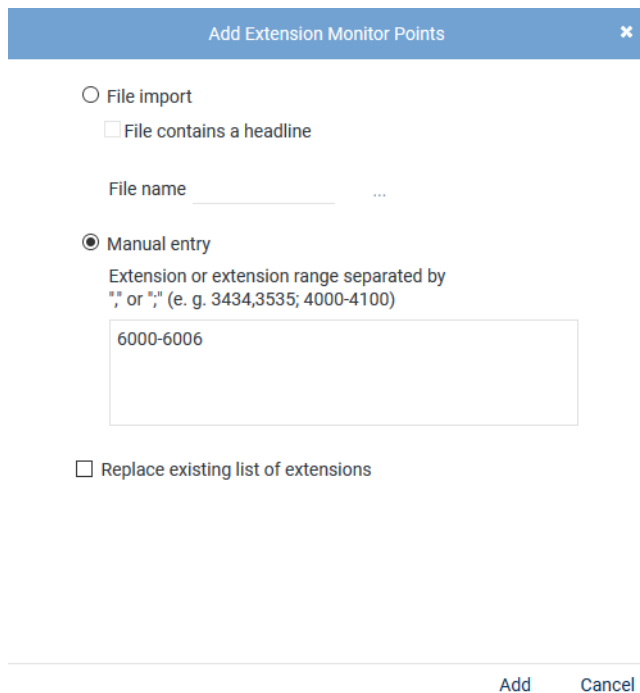






Fig. 411: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button  behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>).
File contains a headline	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.</p>
File name	<p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> Click on the button  behind the field <i>File name</i>. Click on the button <i>Choose File</i>. Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p>

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 ✕		
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. 412: Configured extension monitor points

Add	To add additional monitor points, click on the button <i>Add</i> and select the menu item <i>Enter Extensions</i> ; the window to enter the extension monitor points appears again. By clicking on the button <i>Add</i> , you close the window and the extension monitor points appear in the detail view.
Active/Inactive	The added extensions have been activated as monitor points by default. To change the status of an extension monitor point, select the respective extension and click on the button <i>Active/Inactive</i> . To select several entries at

	the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Delete	To delete extension monitor points, select the respective extension in the list and click on the button <i>Delete</i> . To select several entries at the once, click on the respective entries while holding the [Ctrl] key down. To select several contiguous entries, click on the first and the last entry while pressing the [Ctrl] + [Shift] key.
Intrusion	<p>To be able to use the intrusion feature, you have to activate the check box for the respective extension in the column <i>Intrusion</i>.</p> <p><input checked="" type="checkbox"/> = Intrusion feature has been activated.</p> <p><input type="checkbox"/> = Intrusion feature has not been activated.</p>


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



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

To do so, the parameter *Frei auf Zweitleitung* (free-line signal on second line) must have been set to *Nein, kann nicht im Endgerätemenü geändert werden* (No, cannot be changed in the menu of the end device). See [chapter "Configure extension monitor points", p. 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. 413: 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. 414: Configuration step - Configure recording servers

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

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

Tab. 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*.

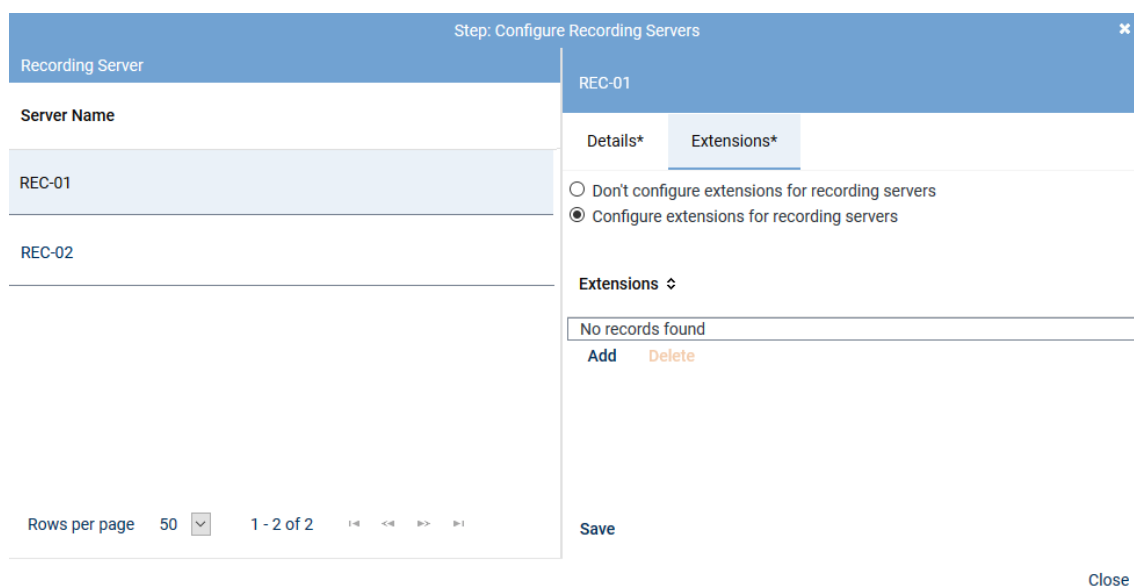


Fig. 415: Tab Extensions

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.

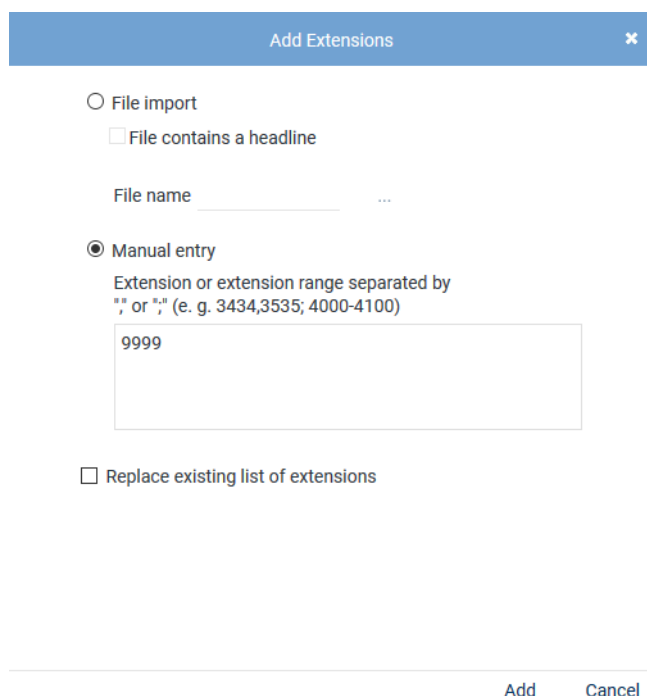


Fig. 416: Add extensions

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.

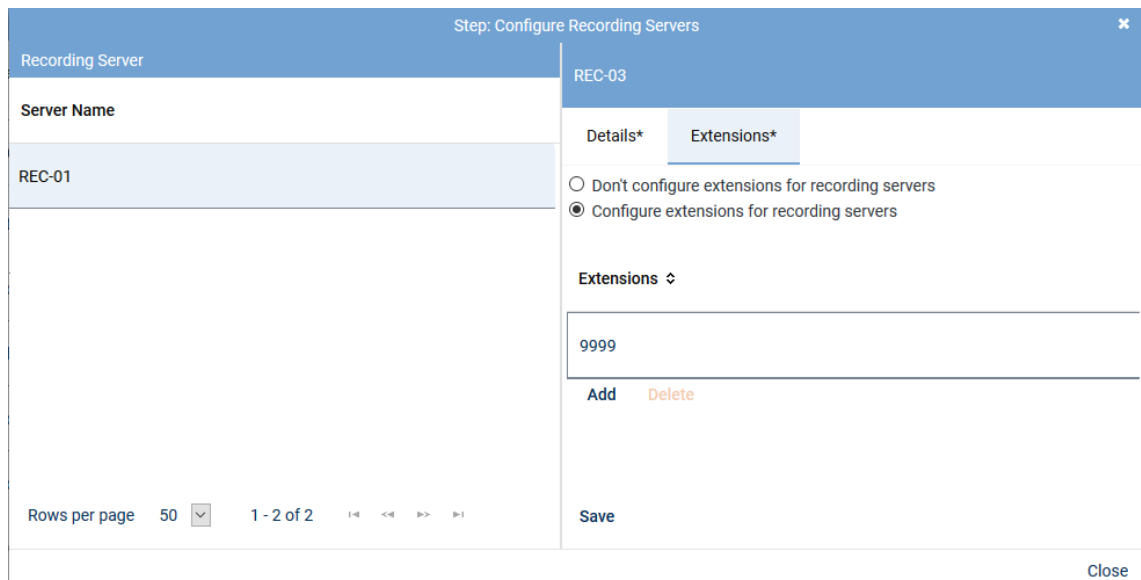


Fig. 417: Added extensions

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	▼
PRIVATEDATA	Please select...	▼
SERVICEGROUPID	Please select...	▼
SERVICEGROUPLIST	Please select...	▼
IVRDATA1	Please select...	▼
IVRLABEL1	Please select...	▼
IVRDATA2	Please select...	▼
IVRLABEL2	Please select...	▼
IVRDATA3	Please select...	▼
IVRLABEL3	Please select...	▼
OASID	Please select...	▼

Arbitrary assignment
+

<input type="text"/>	Please select...	▼	-
<input type="text"/>	Please select...	▼	-
<input type="text"/>	Please select...	▼	-

Save Cancel

Fig. 418: 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. 92: 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. 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

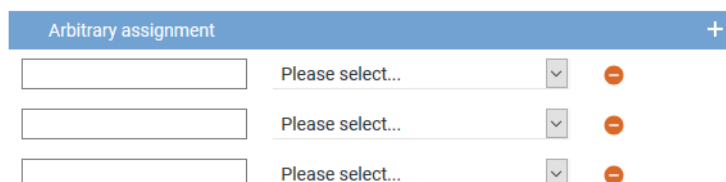



Fig. 419: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

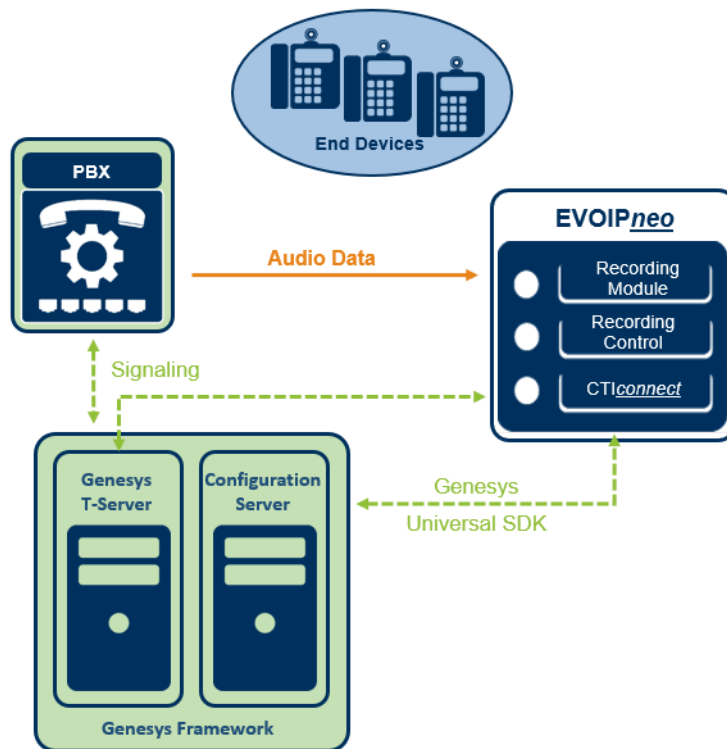


Fig. 420: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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*.

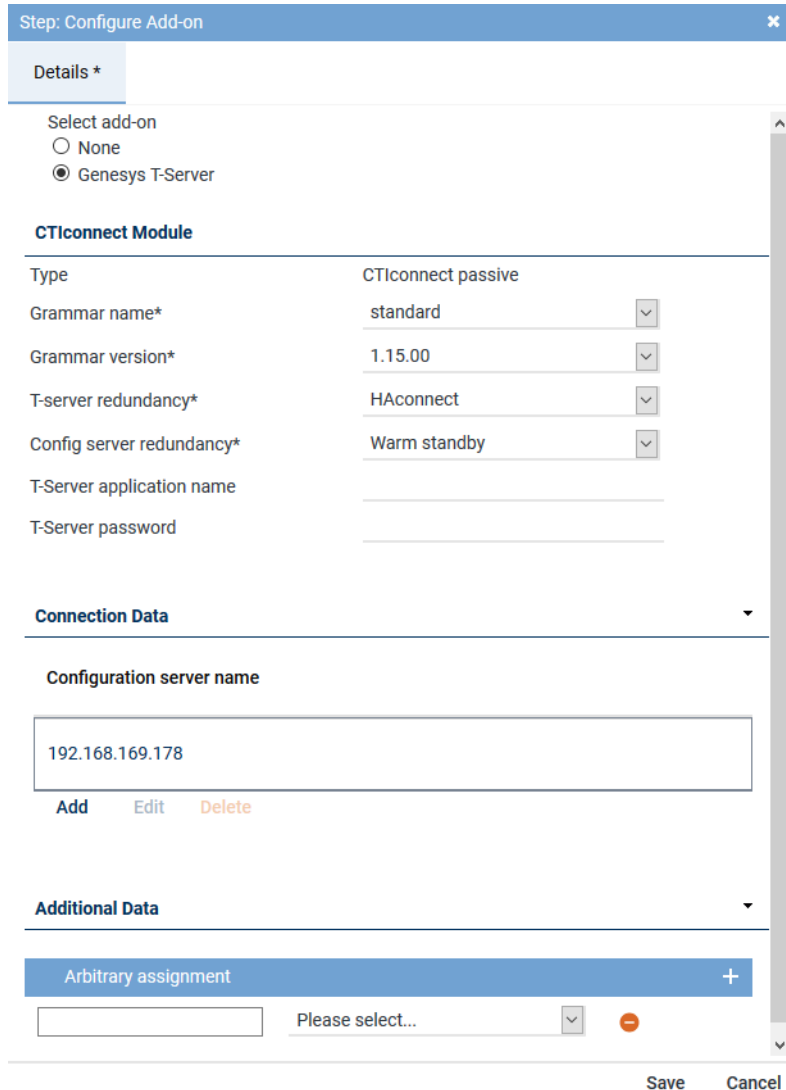


Fig. 421: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

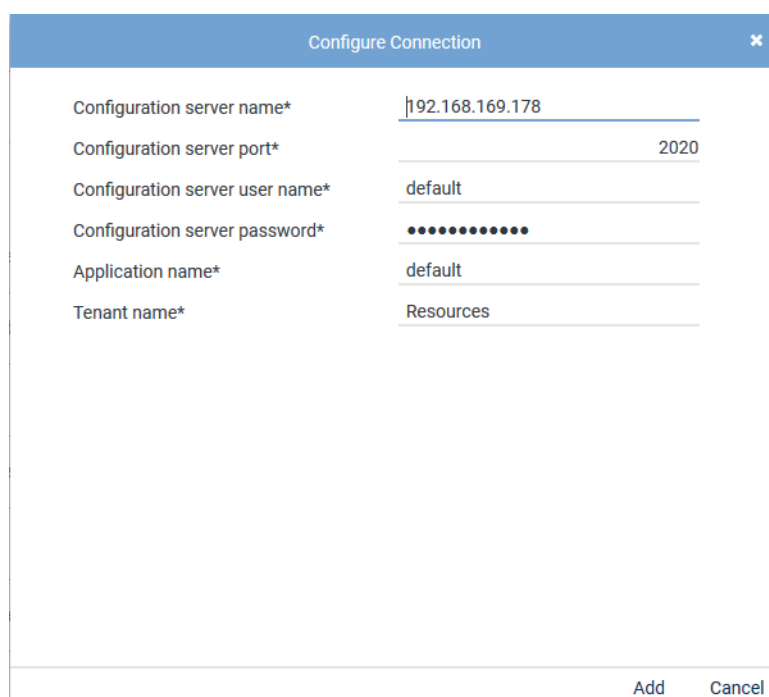
Parameter	Value/Description
	<ul style="list-style-type: none"> • <i>Warm Standby</i> - for a connectable redundancy
<i>Config server redundancy</i>	<p>From the drop-down list, select the redundancy which is used for the Configuration Server of Genesys.</p> <ul style="list-style-type: none"> • <i>No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

Tab. 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:



Configure Connection

Configuration server name*

192.168.169.178

Configuration server port*

2020

Configuration server user name*

default

Configuration server password*

••••••••••

Application name*

default

Tenant name*

Resources

Add

Cancel

Fig. 422: 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.
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

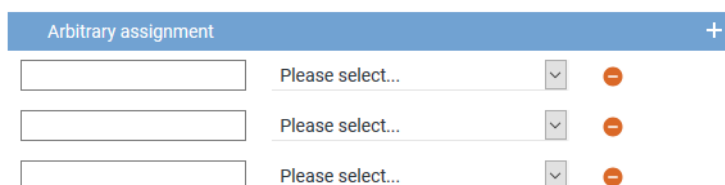




Fig. 423: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.

- Click on the button **Save** in the detail view to save the settings and complete this configuration step.

Configure miscellaneous settings

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

⇒ The window *Step: Miscellaneous Settings* appears.

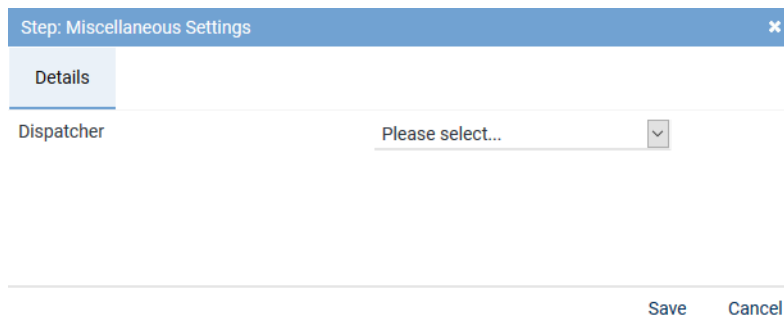


Fig. 424: Configure miscellaneous settings

- 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. 425: 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.

Mitel MiVoice MX-ONE CSTA		Mitel MiVoice MX-ONE CSTA	✓	✓
Name	Type	Active	Status	

Fig. 426: 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.

1. To deactivate the integration, click on the icon  (Deactivate) in the toolbar.

- ⇒ In the column *Active*, the icon  (*Inactive*) appears.
- ⇒ The icon  (*Delete*) becomes active in the toolbar.





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

Fig. 427: Deactivate integration

2. 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.

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

System Configuration X		⏮ 🔍 ⏭ + × ⏮ ⏭ Recording Architecture ▾ General ▾			
SYSTEM PROVIDER		Name ↕	Type ↕	Active	S
Setup		No records found			
Servers					
Recording Architectures					
PHONEapp					
PBX					
Phones					
TDM Hardware ASC					
TDM Hardware Others					
Integrations					
Recording Import					
Additional Data					
Activity Guard					
Powered by ASC Technologies AG v6.9.9-9.9		Rows per page 50 ▾ 1 - 1 of 1 < << >> >			

Fig. 428: Recording architectures - main view

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

	<p>✗ = Recording architecture is not active. It can be activated by clicking on the icon  (Activate) in the toolbar.</p>
<i>Standby Active</i>	<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>
<i>Creation Date</i>	Date on which the recording architecture was installed.
<i>Updated</i>	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. 429: 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>NOTICE! 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>NOTICE! 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"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>


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



For detailed 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.

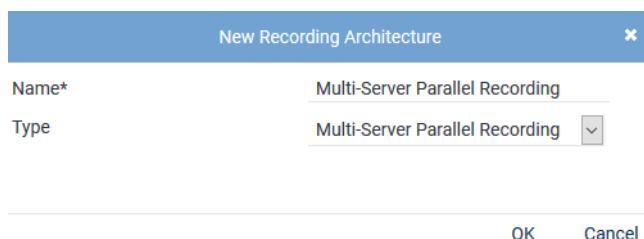


Fig. 430: Create recording architecture - Multi-Server Parallel Recording

- 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 Parallel 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 Parallel Recording
Multi-Server Parallel Recording ✕

<
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	<input type="checkbox"/>
Synchronize recording control	<input type="checkbox"/>
Active	Inactive

Integration Type
+

Name

No records found

Save
Reset

Fig. 431: 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. 447](#).



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. 439](#).

Add integration type

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

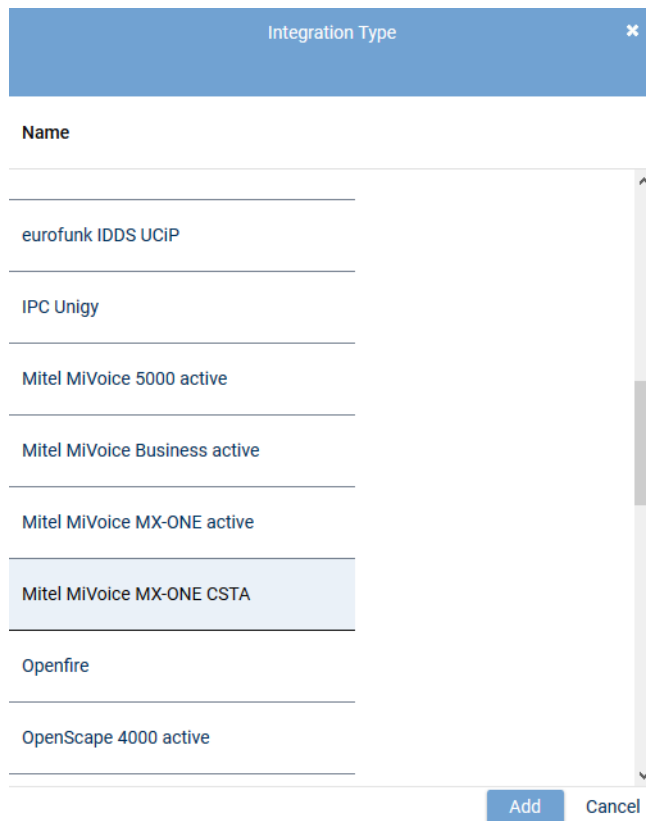


Fig. 432: Select integration type



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 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

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. 433: 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. 434: 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:

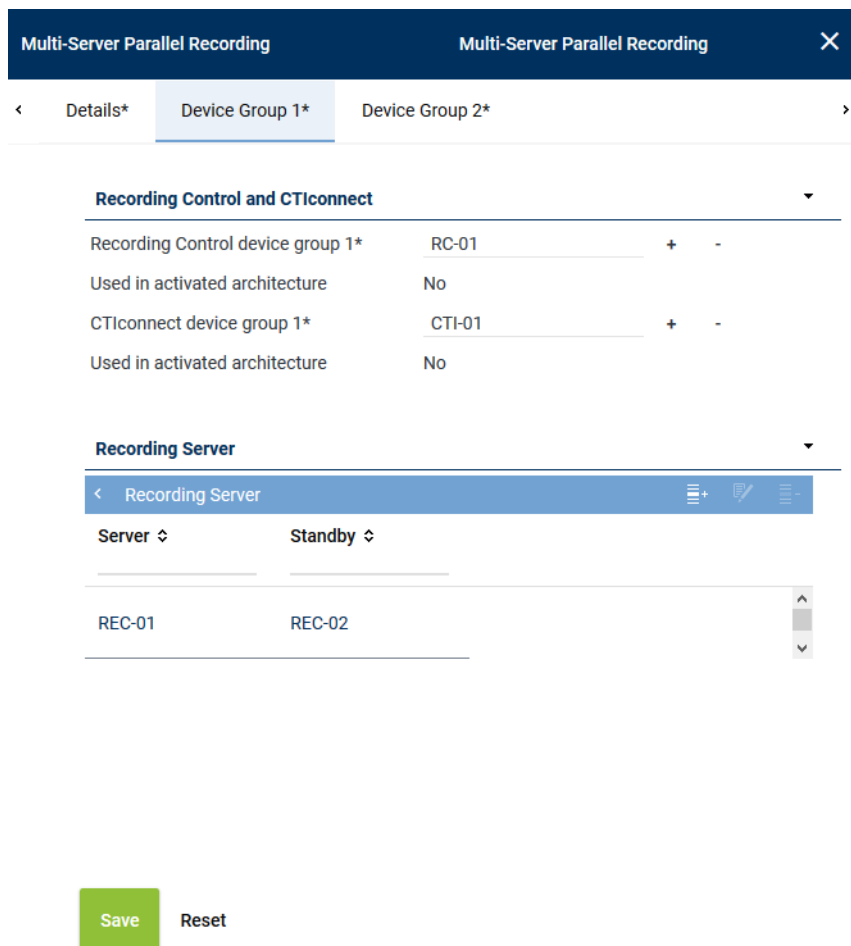






Fig. 435: Add recording server

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. 436: 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.



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:

System Configuration X		Servers v General v	
SYSTEM PROVIDER		Name ↕	IP Address ↕
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard	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. 437: Servers - main view

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

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






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

Toolbar of the Servers module

The toolbar offers the following functions.



Fig. 438: 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 the main view displays all data sets again.
	<i>Delete</i>	Deletes the selected server configuration. This functions serves the purpose of deleting the server configuration when the hardware of a server has been removed and there is no connection to the Neo system.

<i>Server</i>	<i>Administrate Server Locations</i>	Opens a window where you can set up and administrate the location of the servers, see chapter "Administrate server locations" , p. 362.
	<i>Administrate NTP Server</i>	Opens a window in which you can administrate the servers for time synchronization.
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

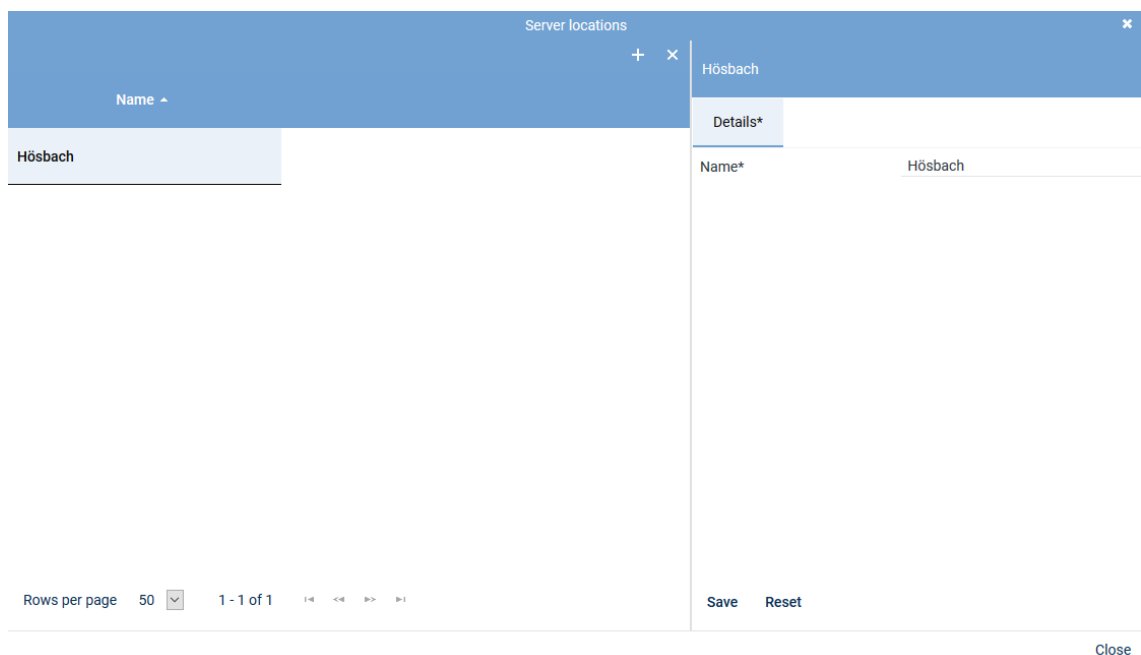



Fig. 439: Add server locations

- 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*.

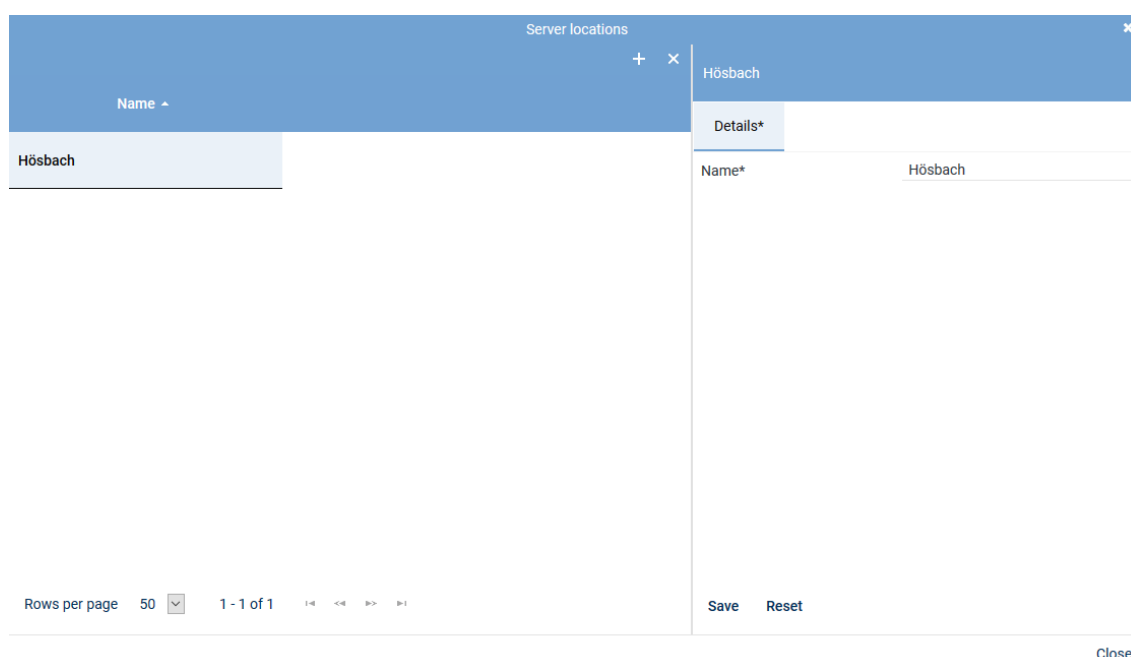
4. To save the entry, click on the button *Save*.
To discard the entry, click on the button *Reset*.
5. To add further locations, repeat the last 3 steps.
6. To close the window, click on the button *Close*.

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". In the bottom right corner of the window, there is a "Close" button.

Fig. 440: 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. 441: 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. 442: Servers - tab usage

Group field API Server

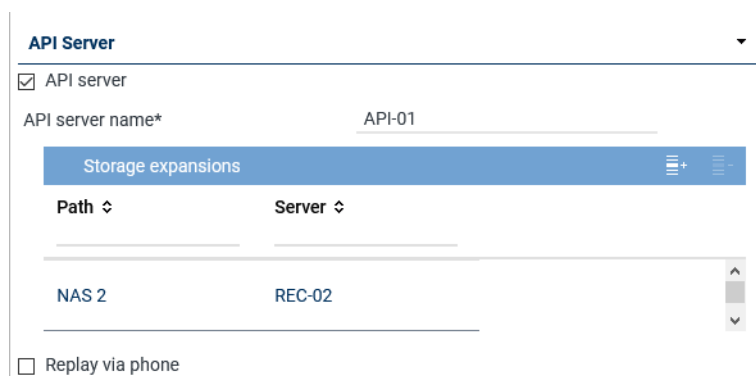




Fig. 443: Group field API Server

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 required 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 chapter "Tab Replay Server Address Mapping", p. 375.</p>
<i>API server name</i>	<p>Enter the name which is supposed to denote the server in the system. The displayed name can be selected arbitrarily and is a kind of pseudonym.</p> <p>The displayed name is meant to make it easier for users to select a server as different API servers may be used across the system by different tenants. When selecting the API server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p>
<i>List Storage expansions</i>	<p>Here, you can add storage expansions for replay. If a recording which is supposed to be replayed cannot be found on the server, the search is continued on the storage expansions which have been entered here. That way, even recordings can be replayed which have not been transferred to the server.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (<i>Add</i>), you can add storage expansions, see chapter "Add storage expansion for replay", p. 366. By clicking on the icon  (<i>Remove</i>), you can remove storage expansions from the list.

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>NOTICE! The function <i>Replay via phone</i> has been implemented in the following Neo components:</p> <ul style="list-style-type: none"> • Application POWERplay Pro • Application POWERplay Instant • Replay module <p>In order to enable a client to use the functionality <i>Replay via phone</i>, you have to assign this client an identifier either in the Employees module or in the Phones module which allows the system to clearly identify the phone.</p> <p>NOTICE! In the tab <i>Media Streamer</i>, you have to assign this function to a PBX, see chapter "Tab Media Streamer", p. 373. 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



 

Fig. 444: 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. 445: Group field Audio Analysis

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

Tab. 96: Configure audio analysis

Emotion Detection ✕

📄

Name ↕

REC-01

Rows per page 20 ▾ 1 - 8 of 8 |< << >> >|

Add **Cancel**

Fig. 446: 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/Live Streaming

Recording architecture Please choose... ▾

☐ Neo key management

Fig. 447: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/ Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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. 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

End

Receives data from

Name	Only Replay
No records found	

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 448: 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</p>

Parameter	Value/Description
	<p><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"> By clicking on the icon  (<i>Add</i>), you can add the target server, see chapter "Add target server to a list", p. 370. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> By clicking on the icon  (<i>Add</i>), you can add the target servers, see chapter "Add target server to a list", p. 370. By clicking on the icon  (<i>Remove</i>), you can remove target servers from the list. <p>NOTICE! 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"> <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. <i>Activate period of time</i> <input type="checkbox"/> = Function not activated. <p>NOTICE! 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>NOTICE! 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>

Group field Replay

Replay

☒ Replay

Replay server*

WebSocket port*

(max. 5 characters)


API server*


+

-

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

Fig. 450: Group field Replay

Parameter	Value/Description
<i>Replay</i>	<p>A replay server can replay recordings via the integrated <i>Replay Feature</i>. Only data which has either been recorded directly on this server or which has been transferred to this server for data storage or only for replay purposes can be replayed. The client computers of the system can connect to a replay server for replay purposes.</p> <p>Activate the check box <i>Replay</i> to be able to use the replay function of the players and the phones.</p> <p><input checked="" type="checkbox"/> = Function has been activated. You have to complete the entry field <i>Replay server</i>.</p> <p><input type="checkbox"/> = Function has not been activated.</p>
<i>Replay server</i>	<p>If the function has been activated, you can enter a displayed name which is supposed to denote the server as the replay server in the system in the entry field <i>Replay server</i>. The displayed name can be selected arbitrarily and is a kind of pseudonym. As the replay server and the API server must not be identical, you can select different pseudonyms.</p> <p>The displayed name is meant to make it easier for users to select a server as different replay servers may be used across the system by different tenants. When selecting the replay server, these pseudonyms are displayed on the client computers instead of the real server name or the IP address.</p> <p>In order to be able to reach the server activated for replay from a public network and with configured port forwarding, you have to set the configuration in the tab <i>Replay Server Address Mapping</i>. For further details about the configuration refer to the administration manual <i>Configuration of servers and recording architectures</i>.</p>
<i>WebSocket port</i> (maximum of 5 characters)	Enter the port via which the data to be replayed in POWERplay Web are supposed to be transmitted.
<i>List</i> <i>API server</i>	<p>Here, you can add API servers that the replay server may use. If a recording which is supposed to be replayed cannot be found on a server, the search is continued on the API servers which have been entered here.</p> <p>If the function <i>Replay</i> has been activated, you can adjust the following settings:</p> <ul style="list-style-type: none"> By clicking on the icon  (Add), you can add the API server, see chapter "Add API server to a list", p. 372.

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

Tab. 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. 451: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 365](#).

- 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. 452: Group field Virtualization

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

Tab. 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. 453: Servers module - tab Media Streamer

2. Enter the following parameters:

PBX	<p>PBX that the Media Streamer is supposed to be mapped to.</p> <p>Select a PBX from the drop-down list. The drop-down list displays all PBXs which have been created in the system.</p> <p>If no PBX has been created in the system yet, you can create a PBX via the blue bar PBX.</p>
Extension	<p>Extension which is supposed to be mapped to the Media Streamer. This is a mandatory field; the configuration cannot be saved if this information is missing.</p> <p>If an external analog gateway has been integrated, enter the value 8000.</p>
Media streamer IP address	<p>IP address which is supposed to be used for the exchange of the audio data and for the SIP communication.</p> <p>Select an IP address from the drop-down list. The drop-down list displays all IP addresses of the server.</p>
Minimum port	<p>Enter the minimum port which is supposed to be used for the audio data exchange.</p> <p>Enter an even number.</p>
Maximum port	<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>NOTICE! The port range must not have less than 64 ports.</p>

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

Tab Replay Server Address Mapping

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

In this tab, you can configure the replay server address mapping. This address mapping is required for servers which have been activated for replay to be able to reach them from a public network and with configured port forwarding.



The tab *Replay Server Address Mapping* is not active unless you have activated the function *Replay* in the tab *Usage*.

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

Replay Server Addresses

Remove Replay Server Addresses

Internal Address of the Replay Server (IP/Port or DNS) :

Internal download URL

External Address of the Replay Server (IP/Port or DNS) :

External download URL


Save
Reset

Fig. 454: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



If address mapping has been configured, the replay server receives the configured address and the configured port.

If address mapping has not been configured, the replay server 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. 455: Servers module - tab Key Management

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

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

In case of an error ... automatically

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

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

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



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



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

Tab Keystore/Virtualization

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

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

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

For key management there are the following options:

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

For licensing, there are the following options:

Without Internet access:

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

- *Trusted Virtualization License*

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

In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*

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

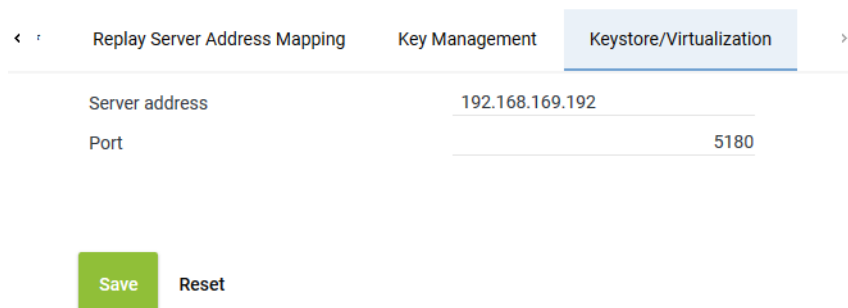


Fig. 456: Servers module - tab Keystore/Virtualization

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

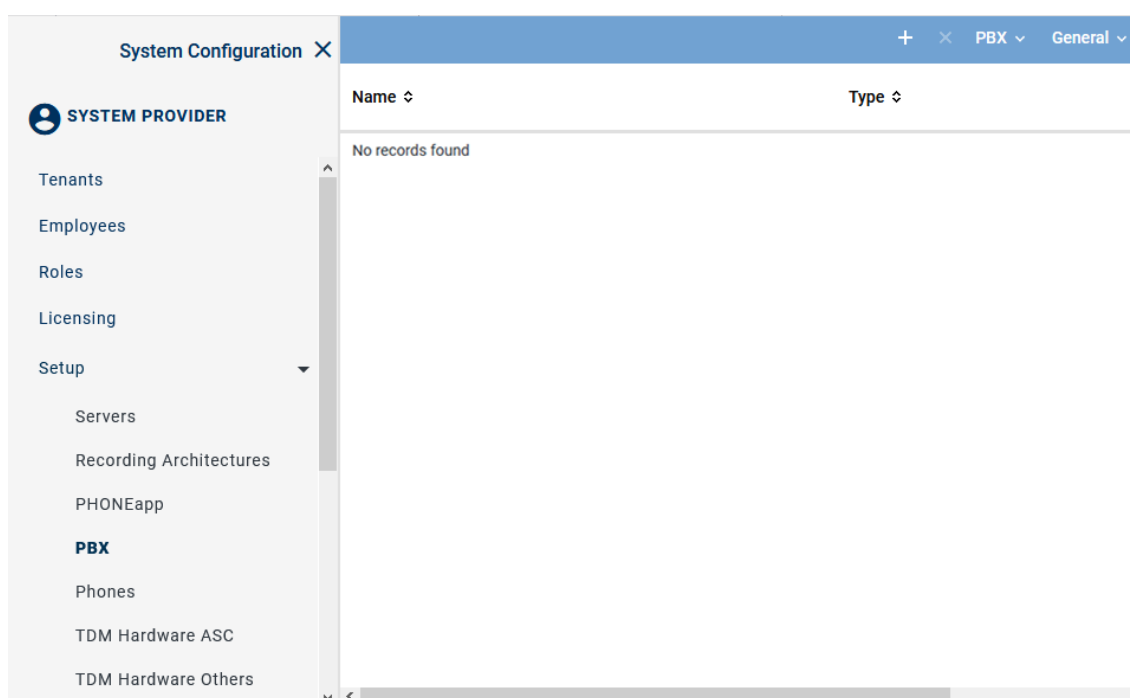




Fig. 457: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 458: 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>Administratre Unused Extensions</i>	Opens a window in which you can delete extensions that are not used in any configuration.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • <i>Displayed information</i> • <i>Order of the displayed columns</i> • <i>Number of rows per page</i>
	<i>General Help</i>	Opens the online help.
	<i>Module Help</i>	Opens the module-specific online help.



For detailed 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.

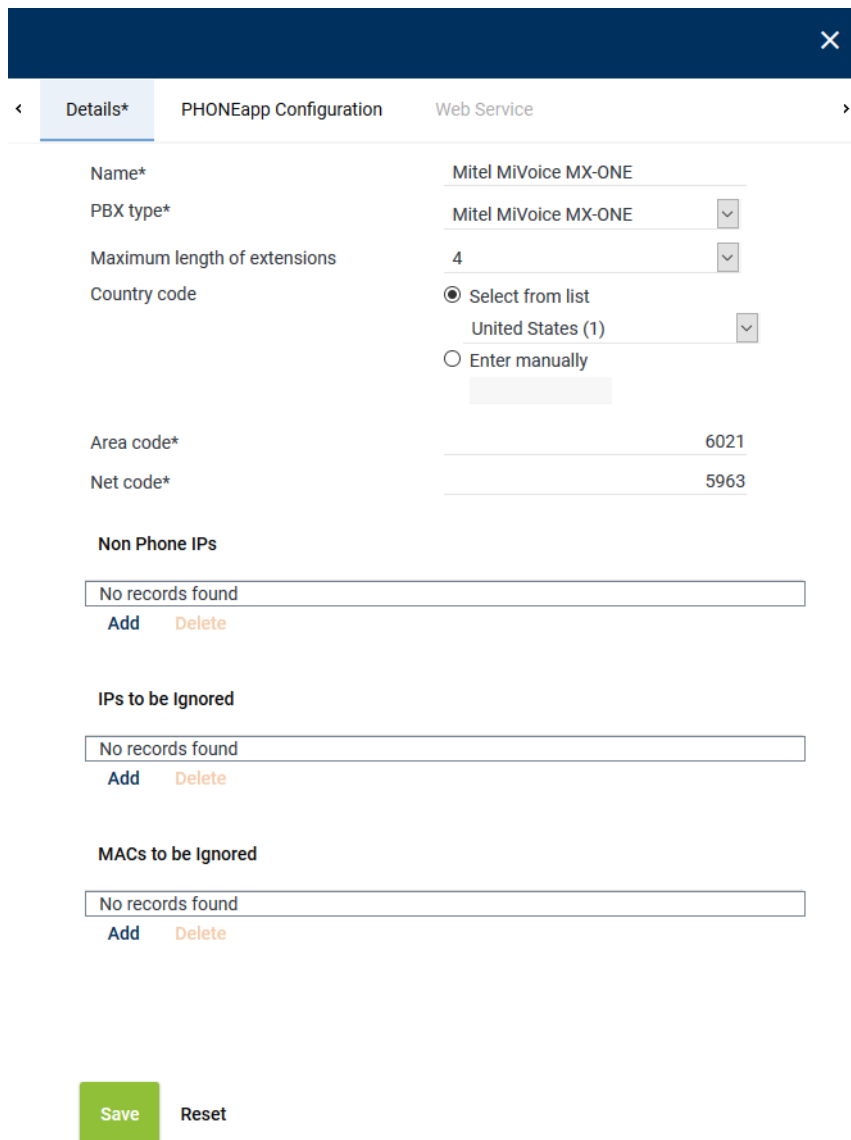


Fig. 459: Create new PBX - tab Details

- 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 PBX from the drop-down list.
<i>Maximum length of the extensions</i>	Enter the number of digits of the extensions, e. g. 4.
<i>Country code</i>	Select the option for the country code: <ul style="list-style-type: none"> <i>Select from list</i> Select the country code from the drop-down list. <i>Enter manually</i> If the corresponding country code is not available in the drop-down list, you can enter the 3-digit code manually. e. g. for Sri Lanka <i>094</i>.

Parameter	Value/Description
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.

Resources for employees

In systems deploying several PBXs, you can assign employees the recording resources of different PBXs.



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

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.

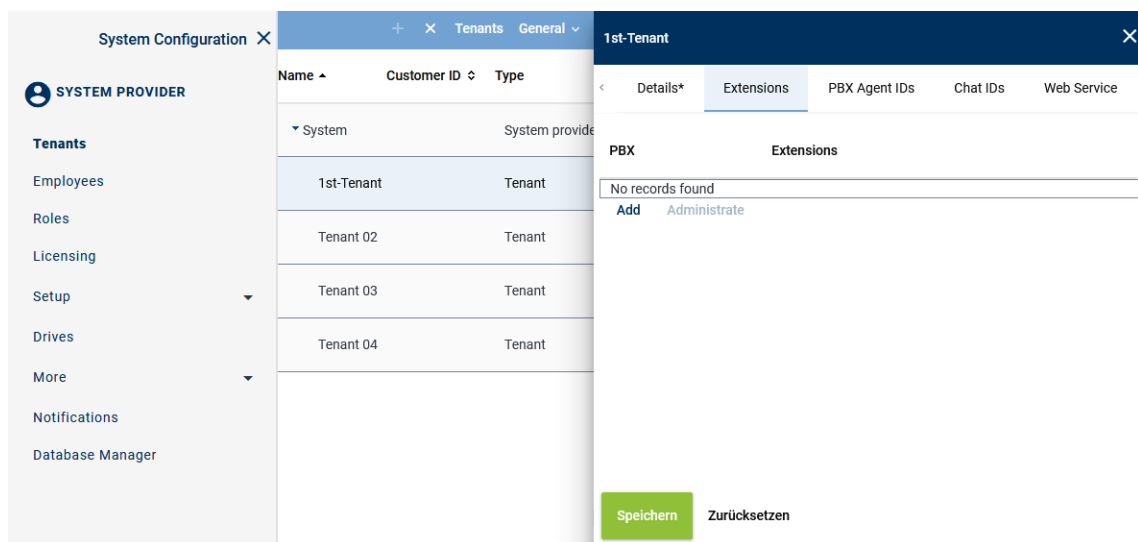


Fig. 460: Tenants - main view - tab Extensions

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. 461: 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"> • ZIP • TXT • CSV <p>NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.</p>
	<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"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

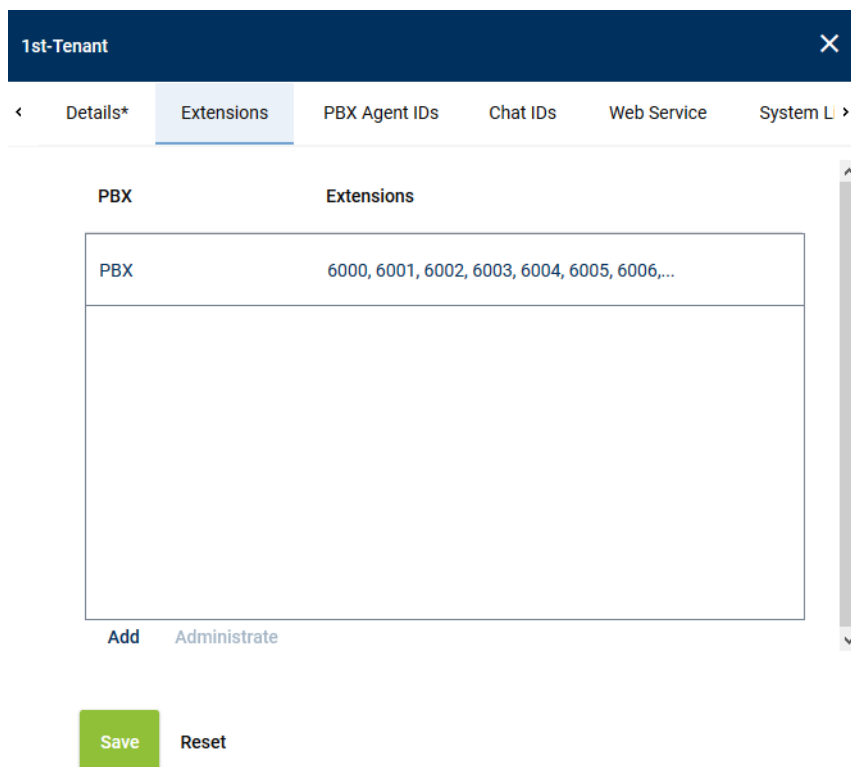


Fig. 462: Remove extensions

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.

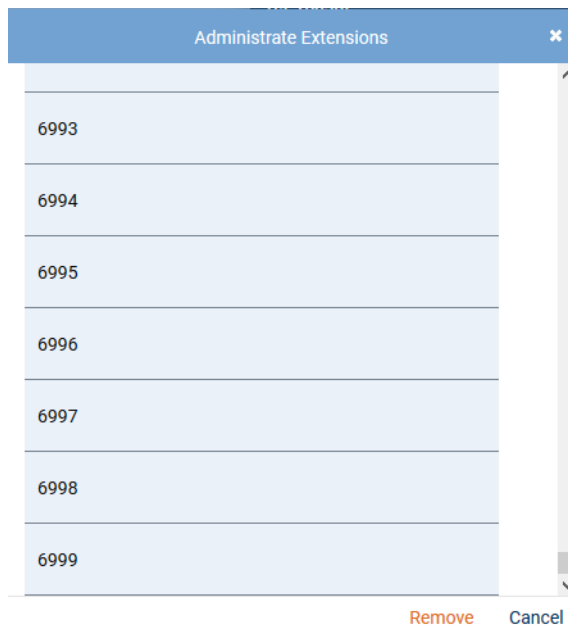


Fig. 463: Select extensions

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.

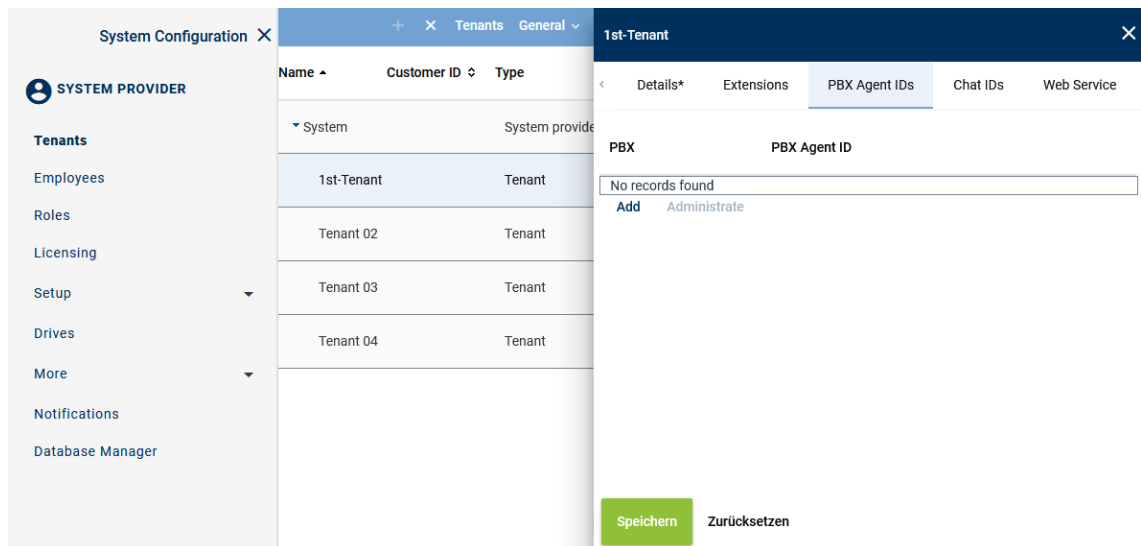
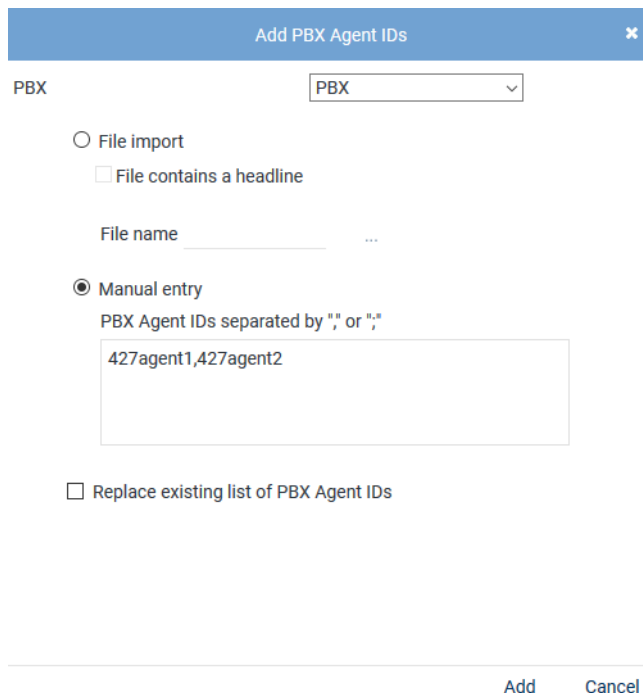


Fig. 464: Tenants - main view - tab PBX Agent ID

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 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'. Below the input field, there is a checkbox labeled 'Replace existing list of PBX Agent IDs'. At the bottom right, there are 'Add' and 'Cancel' buttons.

Fig. 465: 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 CSV file and add them to the table of PBX Agent IDs.
<i>File contains a headline</i>	

	<p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button Upload File.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

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

Remove PBX Agent ID

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

Administrate PBX Agent IDs
✕

ID

427agent1
427agent2

Remove Cancel

Fig. 466: 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

Additional data

Metadata for a conversation delivered by a communication platform are added to the respective conversation as additional data in the recording system.

The recording system differentiates between 2 types of additional data:

- *Default additional data fields*
This additional data cannot be changed such as the start time, the end time, and the phone number of the participants or the agent data.
- *CustomCP fields*
These fields can be adjusted by the user and can be configured as editable fields. Among those are e. g. comment fields or customer IDs. The configuration takes place in the Additional Data module of the application System Configuration.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.

In the Additional Data module, you can assign metadata to CustomCP fields in Neo so that the data is tagged and saved there.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.

In order to have the fields displayed in the drop-down list to be selected, they must be configured in the Additional Data module.

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

System Configuration X		Additional Data		Additional Data	General v
SYSTEM PROVIDER		ID ↕	Displayed Name ↕	Available ↕	
Setup Servers Recording Architectures PHONEapp PBX Phones TDM Hardware ASC TDM Hardware Others Integrations Recording Import Additional Data Activity Guard		customCP01	customCP01	✗	
		customCP02	customCP02	✗	
		customCP03	customCP03	✗	
		customCP04	customCP04	✗	
		customCP05	customCP05	✗	
		customCP06	customCP06	✗	
		customCP07	customCP07	✗	
		customCP08	customCP08	✗	

Fig. 467: Additional Data module main view

2. Select a data set

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

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. 468: Configure additional data

- To change the display name, click on the pen icon in the line of the language that you would like to change.
- 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. 469: Additional data - configure availability

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



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

7.3.2.6.6 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:

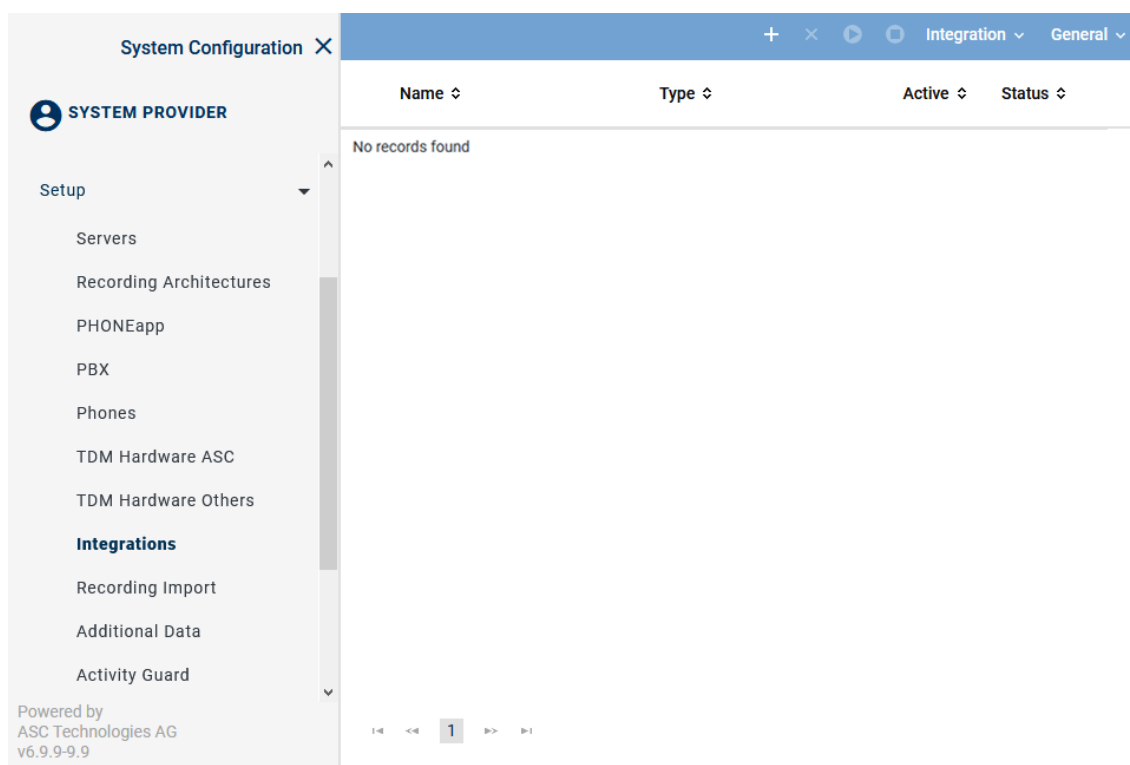








Fig. 470: Integrations - main view

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





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

Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 471: Toolbar Integrations module

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

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

Import grammar

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

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

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

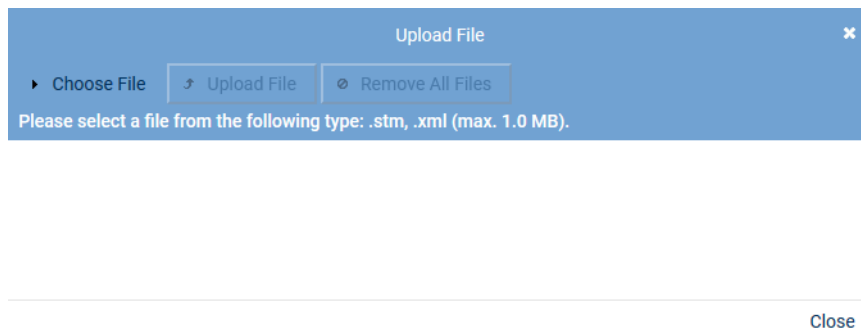


Fig. 472: Choose file

- 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*.

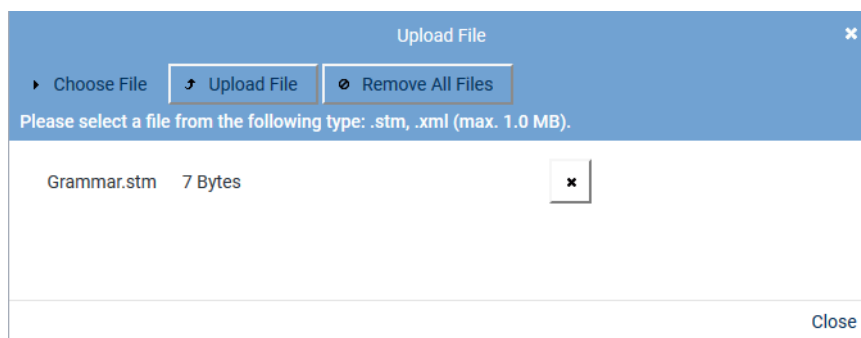




Fig. 473: Upload grammar

- 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. 474: Create integration type

2. Enter the following parameters:

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

Tab. 102: Create integration type

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

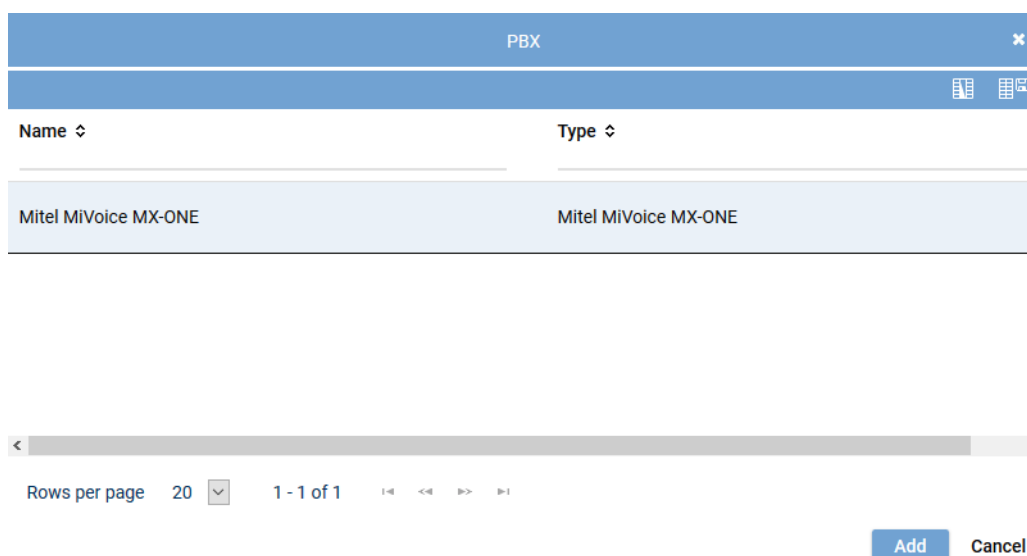


Fig. 475: Integrations - select PBX

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

Assign recording architecture for Multi-Server Parallel Recording

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

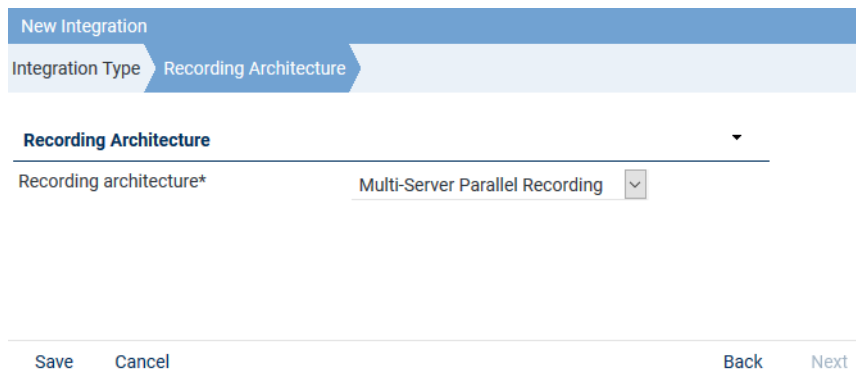


Fig. 476: Assign recording architecture - Multi-Server Parallel


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.

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. 477: 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.

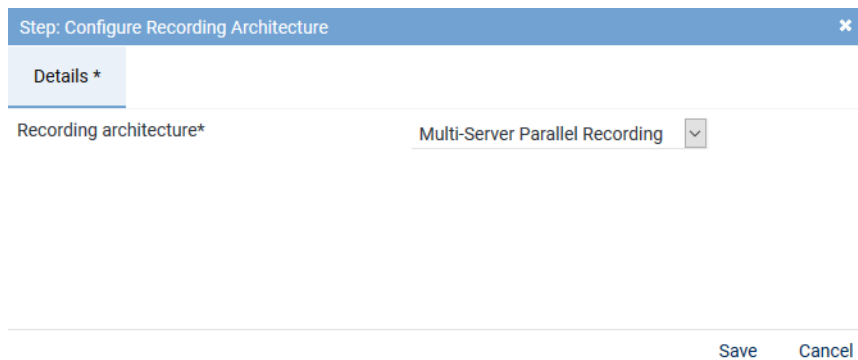



Fig. 478: Configuration step - Configure Recording Architecture

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)*

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 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

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. 479: 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. 480: 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. 481: Configure connection data

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. 482: Configure connection data

1. 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 TLS .
<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 chapter "Configure CSTA server", p. 14 .

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

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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

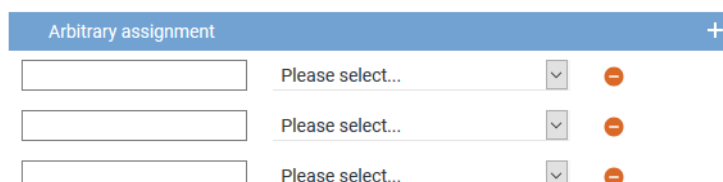



Fig. 483: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

Configure CTI parameters

The following parameters are only valid for the CTI connections.

Switching conditions for the CTI failover connection

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



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

Failover waiting time*	10
Failover repetitions*	3

Fig. 484: Configure switching conditions

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



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



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 can be recorded with the recording type *Active-Stream-Recording/Copy-Stream-Recording* (INVITATION) or via the MBG.

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.
- *Active Stream Recording*
If the feature Intrusion has not been activated, the regular expression is used to identify the recording type. Thereby, the *deviceModelName* is checked. If the check confirms a supported hardware phone type registered directly with MX-ONE, the recording type *Active Stream Recording* is used.
- *MBG*
If the end device (softphones, teleworkers, etc.) has been registered on an [MBG](#) or if the regular expression does not apply for the respective phone type, recording runs via the [MBG/SRC](#).

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

NOTICE! Do not change this expression without having consulted ASC previously.

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. 485: Configure regular expression for phone type identification

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 e. g. 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>.

Tab MBG

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

Step: Configure CTI Connection Data

MiVoice 5000 (CSTA)* MBG

Active ☒

CTIconnect Module

Type CTIconnect active

Grammar name* standard

Grammar version* 1.00.04

Connection Data Device Group 1

Connection Data Device Group 2

Additional Data

Save Cancel

Fig. 486: 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.

CTIconnect Module

Type CTIconnect active

Grammar name* standard

Grammar version* 1.00.51

Fig. 487: 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.

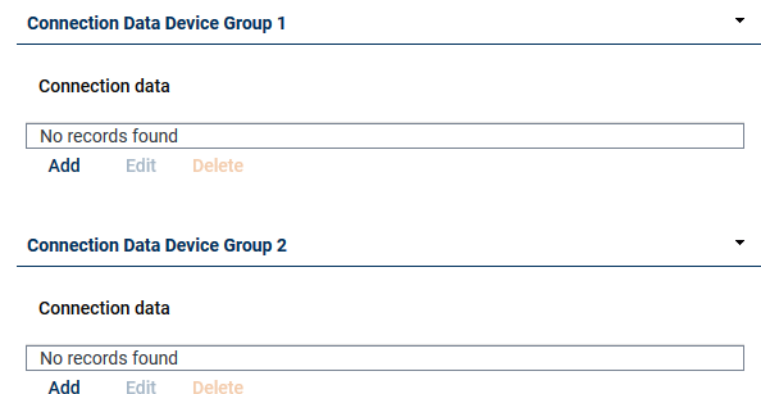


Fig. 488: Group field Connection Data

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

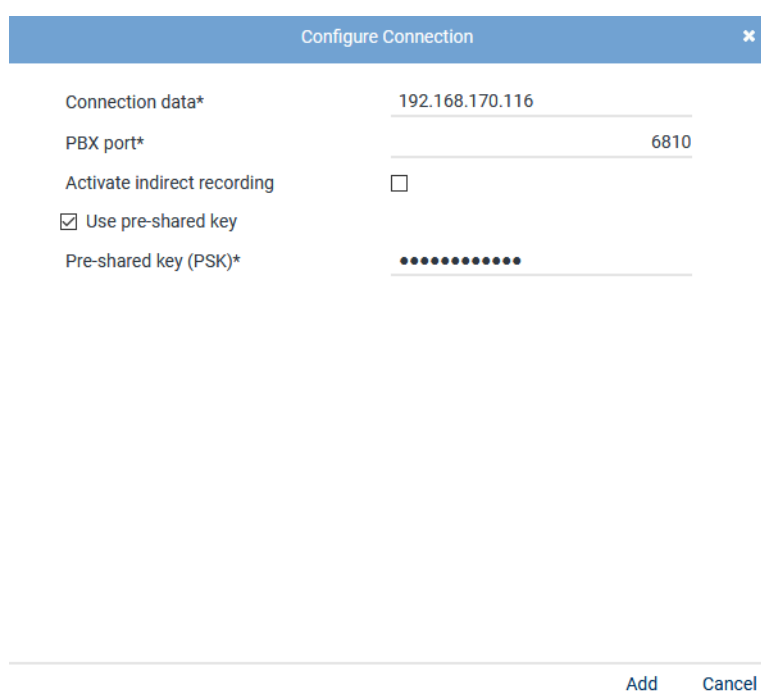


Fig. 489: Configure connection

2. Enter the following parameters:

Parameter	Value/Description
<i>Connection data</i>	Enter the link to the MBG . Enter all MBGs that are used including MiCollab. In the connection data, enter either the IP address or the FQDN of the MBG .
<i>PBX port</i>	Enter the port for the MBG or the SRC , default 6810.
<i>Activate indirect recording</i>	Activate the check box if you would like to use indirect recording.

Parameter	Value/Description
<i>Use Pre-shared key</i>	Activate the check box if the MBG is used in PSK mode and authentication is supposed to be done by means of the pre-shared key.
<i>Pre-shared key (PSK)</i>	Enter the password for the pre-shared key. The password must be identical with the configuration in the MBG , see chapter "Configure MiVoice Border Gateway for NEO access via Web Proxy" , p. 23

Tab. 106: 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

The metadata delivered for a conversation with the protocol of the communication platform can be tagged and saved in Neo in user-defined additional data fields, the so-called CustomCP fields.

In this group field, you can assign the metadata delivered for a conversation with the protocol of the communication platform to the CustomCP fields in Neo so that they are available to be used elsewhere.



Start time, end time, phone number or call direction are available as default additional data and cannot be edited. The data is tagged in default additional data fields and do not have to be assigned separately.



Only those CustomCP fields are available in the drop-down list that have been configured previously in the Additional Data module. In the Additional Data module, you can define a display name, select whether the fields can be edited and are supposed to be available across the system.



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

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

Arbitrary assignment

In the section *Arbitrary assignment*, you can configure additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

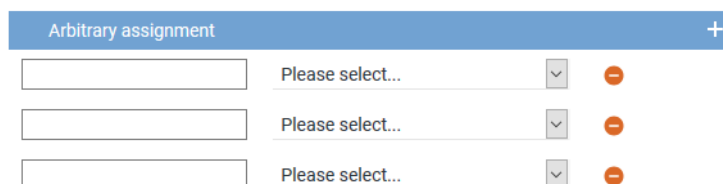



Fig. 490: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

The information tagged in CustomCP fields can also be used in the Recording Planner for instance to control recording behavior and displayed in the search and replay applications.




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



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

Configure monitor points 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.

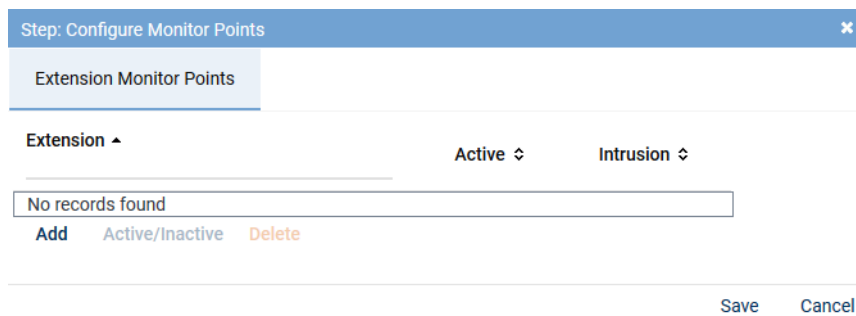


Fig. 491: Configuration step - configure monitor points

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. 492: Add extension monitor points

File import	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
	<p>File contains a headline</p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p>
	<p>File name</p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  (<i>Upload file</i>).
Manual entry	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p>

NOTICE! Wildcards cannot be used!

Replace existing list of extensions

Activate the check box to replace the list of extensions.

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

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

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

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

Fig. 493: Configured extension monitor points

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

<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. 494: 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.

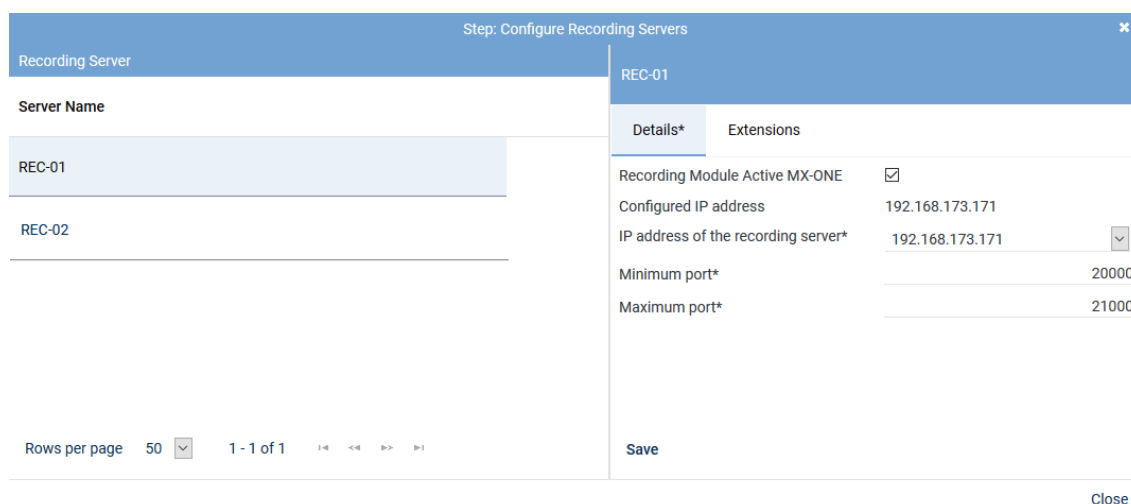


Fig. 495: Configuration step - Configure recording servers

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

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

Tab. 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. 496: 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

- 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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

- In the group field headline *Additional Data*, click on the arrow ► to open the group field and assign the additional data to the data fields.

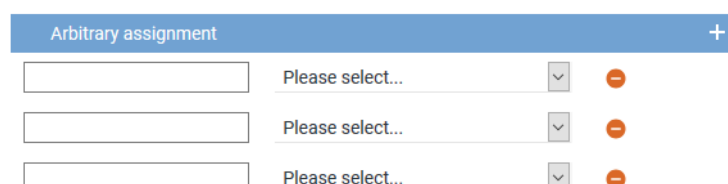



Fig. 497: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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 CTIconnect 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

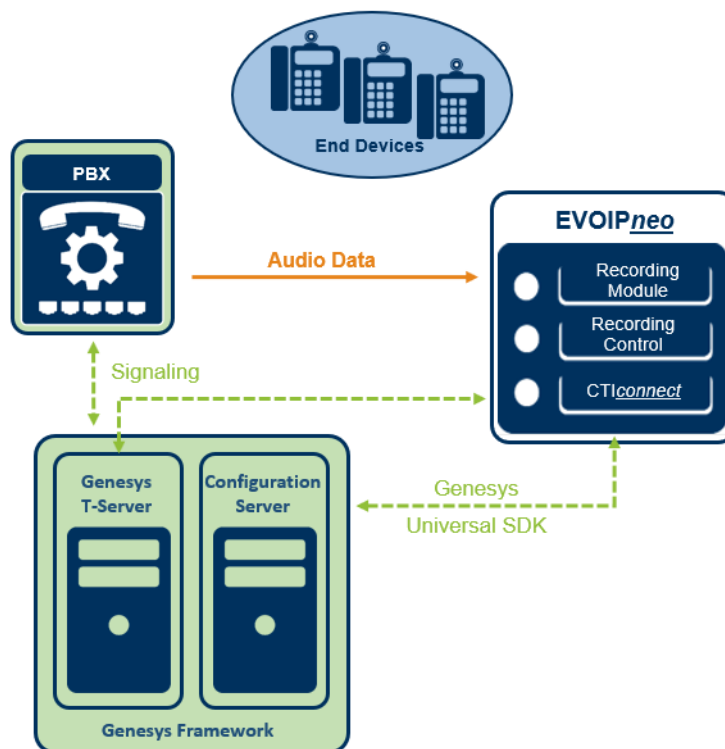


Fig. 498: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 451](#).

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 CTI~~connect~~ 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. 499: Configure add-on for Genesys T-Server

Group field CTIconnect Module

1. Enter the following parameters:

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

Parameter	Value/Description
<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 CTIconnect 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 CTIconnect 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.

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

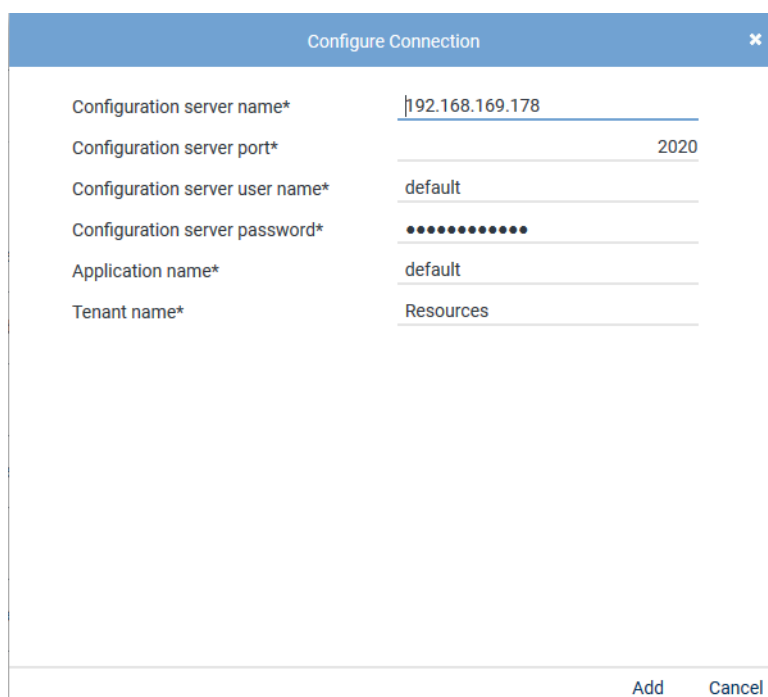


Fig. 500: Configure connection data

- 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.
<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.

Parameter	Value/Description
<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 additional data which is delivered additionally by the PBX or an add-on and which has not been preconfigured.

1. In the group field headline *Additional Data*, click on the arrow ▶ to open the group field and assign the additional data to the data fields.

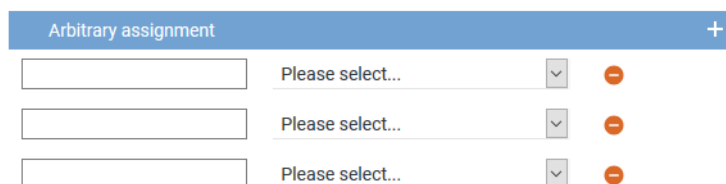



Fig. 501: Group field Additional Data - free assignment of additional data

2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information 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 line to add another additional data type appears.
5. Click on the button *Save* in the detail view to save the settings and complete this configuration step.

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.

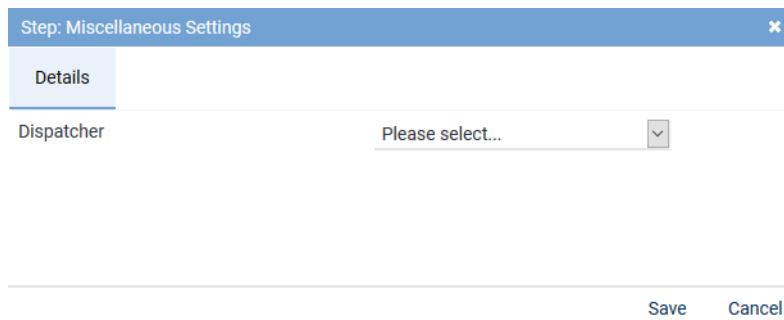


Fig. 502: Configure miscellaneous settings

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. 503: 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. 504: 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.

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







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

Fig. 505: Deactivate integration

2. 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

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

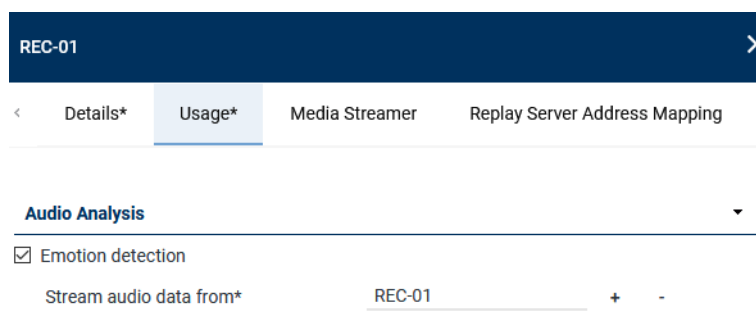


Fig. 506: Servers module - Activate emotion detection

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	<input checked="" type="checkbox"/>	
Activate decryption error detection	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> Activate silence detection		
Minimum duration*	30000	ms
Threshold value*	-60	dB
Silence percentage*	90	%
Weighting*	10	
Emotion detection*	+ -	


Save

Reset

Fig. 507: Create integration - tab Recording Content Validation

Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost. NOTICE! Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	<input checked="" type="checkbox"/> Activate the check box to check whether errors occurred during decryption. NOTICE! 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. NOTICE! 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 (<i>30 seconds</i>).
<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.

Emotion detection server

By clicking on the icon , select the server that emotion detection runs on.
The speech analysis software recognizes whether there are silence sections in the recording.

NOTICE! The list only displays servers which have been configured for audio analysis and have been assigned in the Servers module.

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

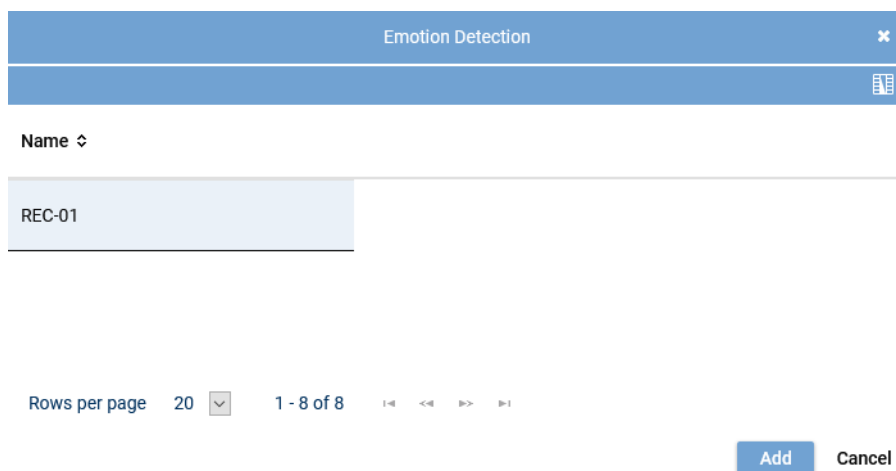


Fig. 508: Select server for emotion detection

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

Configuration in the Notifications module

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



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

Configuration in the application INSIGHT_{neo}

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



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

7.3.4 Configure PHONEapp for Mitel

If you would like to use the XML PHONE_{app}, you have to execute the following configuration:

1. Configure key assignment for the phones.
2. Modules in the application Configure *System Configuration*:
 - Servers module
 - Activate recording control
 - Select recording architecture
 - PHONEapp module
 - Configure phone types

- Configure basic settings
- PBX module
 - Activate PHONEapp configuration
 - Configure PBX-specific parameters
- Phones module
 - Configure the parameters for the assignment of the phone, e. g. extension, PBX phone ID, computer name, address for replay via phone, phone type, and time slot.
- Recording Planner module
 - Configure operation modes

7.3.4.1 Configure Servers module

To be able to control the recording by means of PHONEapp, you have to activate recording control in the Servers module.

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

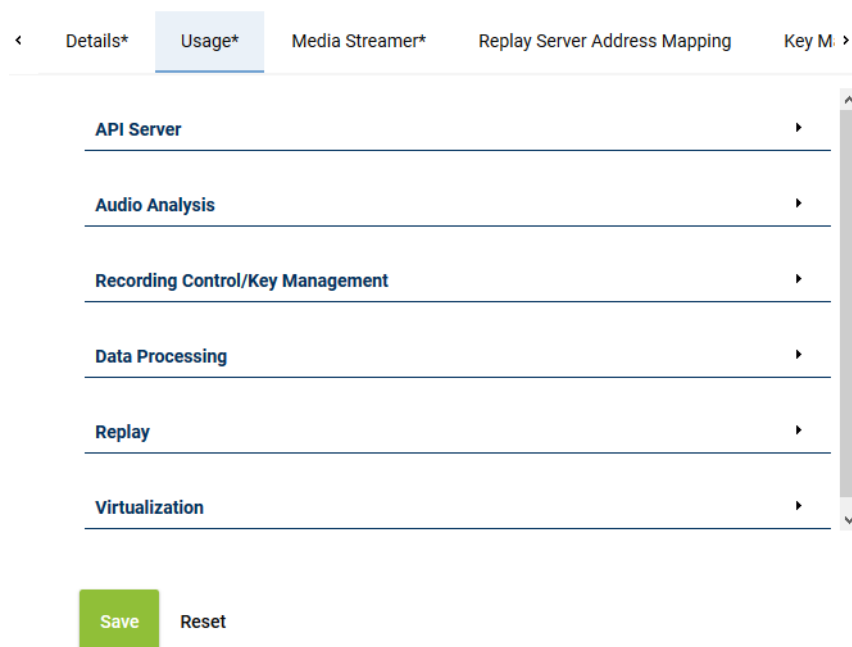


Fig. 509: Servers - tab Usage

3. Open the group field *Recording Control/Key Management*.

7.3.4.1.1 Group field Recording Control/Key Management

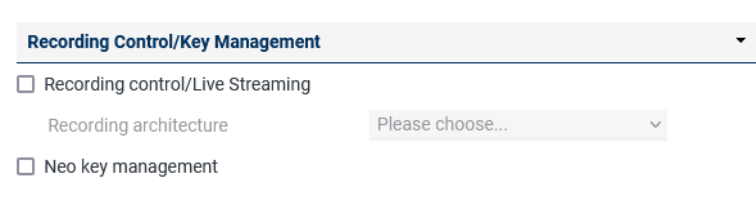


Fig. 510: Group field Recording Control/Key Management

Parameter	Value/Description
<i>Recording control/ Live Streaming</i>	This recording solution does not support external recording control.
<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>Neo 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. 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:

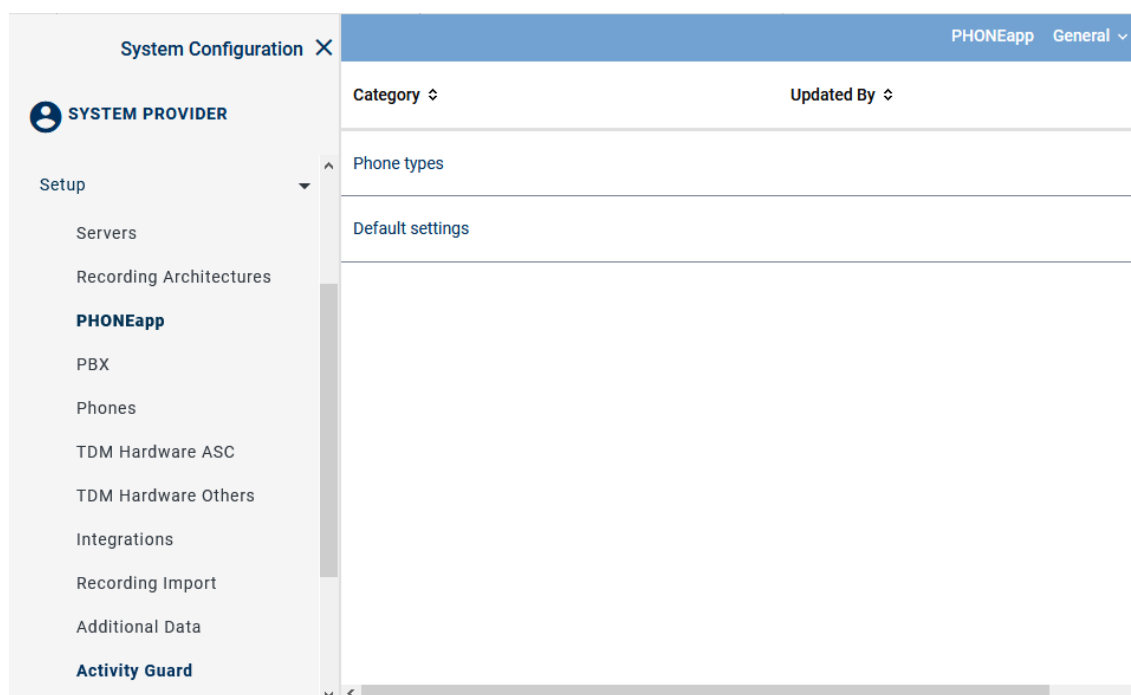


Fig. 511: PHONEapp - main view:

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. 512: 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. 513: 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*
Only certified requests ☐

Language

Time Parameter



Response waiting time* Milliseconds
Error waiting time* Milliseconds
Phone refresh interval* Milliseconds

Tagging Attributes

Request Parameter	Field
tag_field	ASC_COMMENT 

Add Delete


Register Fields

Field	Recording Control Field	Active
Comment	ASC_COMMENT	 

Add Delete

Predefined Tagging Fields

☐ Activated



Tagging Field

Save Reset

Fig. 514: 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"> • <i>Activated</i> 	Activates the recording control by means of the <u>PHONEapp</u> .
<ul style="list-style-type: none"> • <i>PHONEapp URL</i> 	<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://<core_ip>: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"> • <i>Only certified requests</i> 	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 > 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"> • <i>Response waiting time</i> 	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"> • <i>Error waiting time</i> 	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"> • <i>Phone refresh interval</i> (this setting is only relevant for Alcatel and Cisco) 	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 > 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"> • <i>Activated</i> 	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"> • <i>Tagging Field</i> 	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.

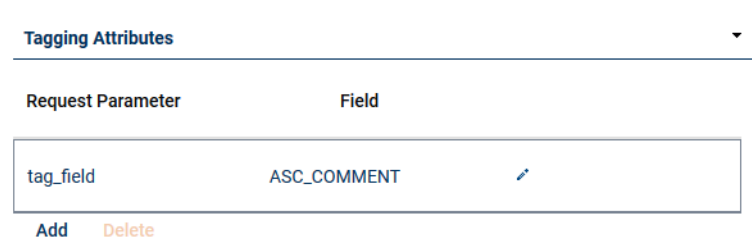


Tagging attributes should only be changed in exceptional justified cases. Incorrect changes can cause a malfunction of the PHONEapp.

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. 515: 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. 516: 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. 517: 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 type="checkbox"/>  

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

Fig. 518: 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 recorded conversations. This allows associating conversations with certain topics and later on filtering or searching for these conversations. By default, the *PHONEapp* offers either comment fields to enter free text or predefined tagging fields. Users can see these attributes when pressing a certain key on the end device. Users can tag conversations during or after 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 conversations.

- In the detail view of *Setup > PHONEapp > Default Settings*, open the group field *Predefined Tagging Fields*



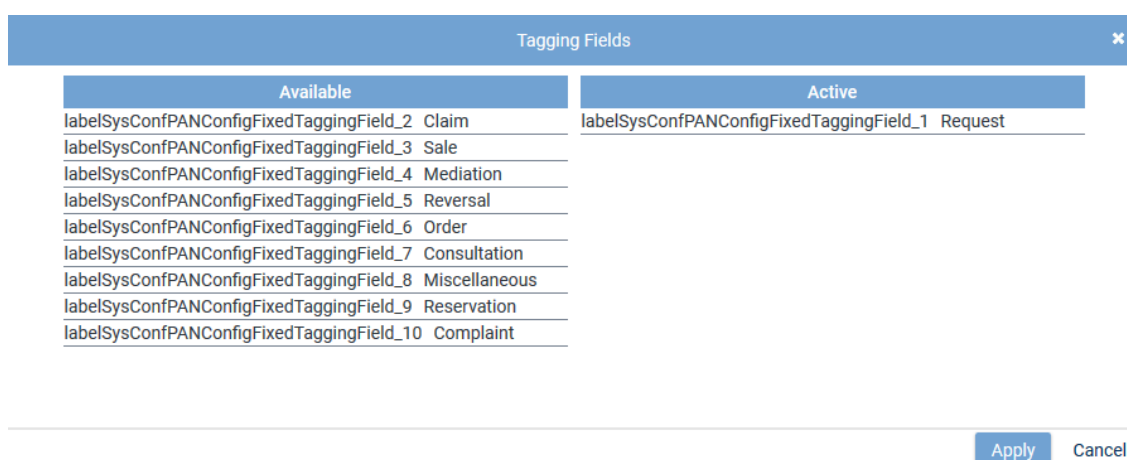



Fig. 519: Configure tagging fields

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. 520: Edit tagging fields

4. To add a field, drag the selected field from the list of available fields on the left to the list *Active* in the window on the right and drop it there.
 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 added fields, 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 revolving around a request.
<i>Claim</i>	Use this attribute to tag conversations revolving around a claim.
<i>Mediation</i>	Use this attribute to tag conversations revolving around a mediation.
<i>Order</i>	Use this attribute to tag conversations revolving around an order.
<i>Consultation</i>	Use this attribute to tag conversations revolving around a consultation.
<i>Reservation</i>	Use this attribute to tag conversations revolving around a reservation.
<i>Complaint</i>	Use this attribute to tag conversations revolving around a complaint.
<i>Sale</i>	Use this attribute to tag conversations revolving around a sale.
<i>Reversal</i>	Use this attribute to tag conversations revolving around a reversal.



The tagging fields are displayed along with the corresponding resource string. You can adjust 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 affect 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.
Apply		Saves all changes and closes the window <i>Tagging Fields</i> .
Cancel		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 moving the selected field to the required position while holding the left mouse key down, too.

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.

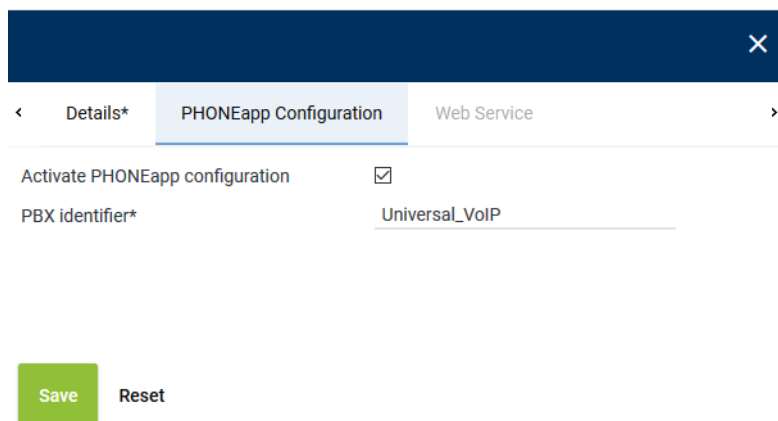


Fig. 521: Activate PHONEapp configuration

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 PHONE <u>apps</u> .. 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:

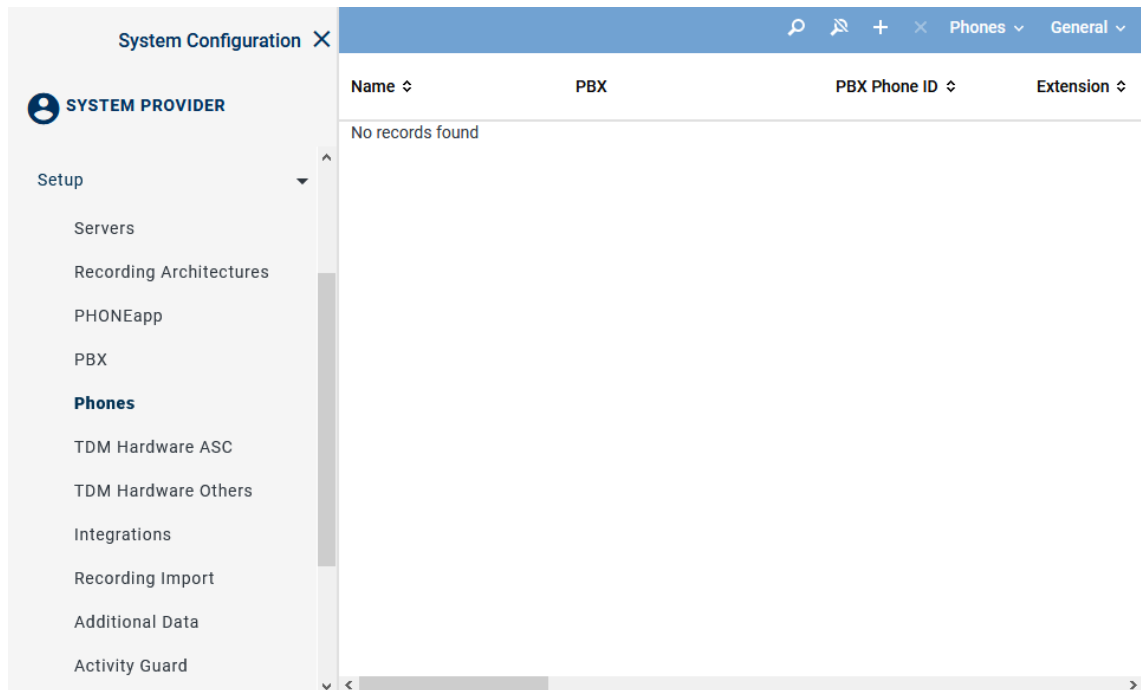


Fig. 522: Phones - main view

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

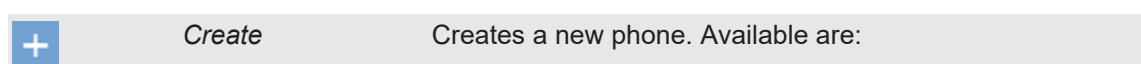
<i>Name</i>	Shows the name of the phone.
<i>PBX</i>	Shows the name of the PBX.
<i>PBX Phone ID</i>	Shows the identifier which has been configured for the phone in the PBX.
<i>Extension</i>	Shows the assigned extension of the phone.
<i>Computer Name</i>	Shows the computer name if it has been defined in the details.
<i>Phone Type</i>	Shows the selected phone type if the PHONEapp configuration has been activated.
<i>Display Language</i>	Shows the selected display language.





7.3.4.4.1 Toolbar of the Phones module

The toolbar offers the following functions:



Fig. 523: Toolbar




		<ul style="list-style-type: none"> • IP phone • TDM phone
	<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 where you can adjust the following settings for the main view: <ul style="list-style-type: none"> • Displayed information • Order of the displayed columns • Number of rows per page
	<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.



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*.

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.

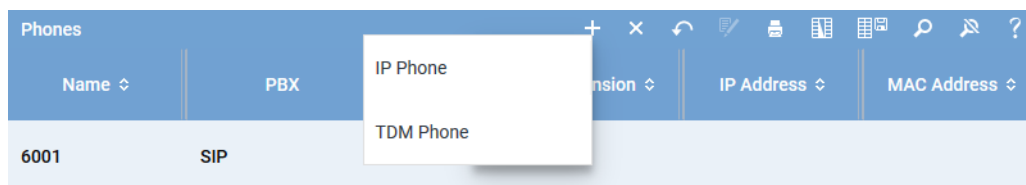


Fig. 524: Create phone

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. 525: 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"> • in the PBX module in the tab PHONEapp • and in the PHONEapp module
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"> • For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey3</i>. • For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey3</i>.
Mute LED identifier	<p>Enter the softkey for the mute function.</p> <ul style="list-style-type: none"> • For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey4</i>. • For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey4</i>.
Keep LED identifier	<p>Enter the softkey for the keep function.</p> <ul style="list-style-type: none"> • For SIP phones, softkeys are called <i>topsoftkey</i>, in the example <i>topsoftkey5</i>. • For Mitel MiNet phones in combination with a Mitel MiVoice Business PBX, softkeys are called <i>prgkey</i>; enter <i>prgkey5</i>.

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.

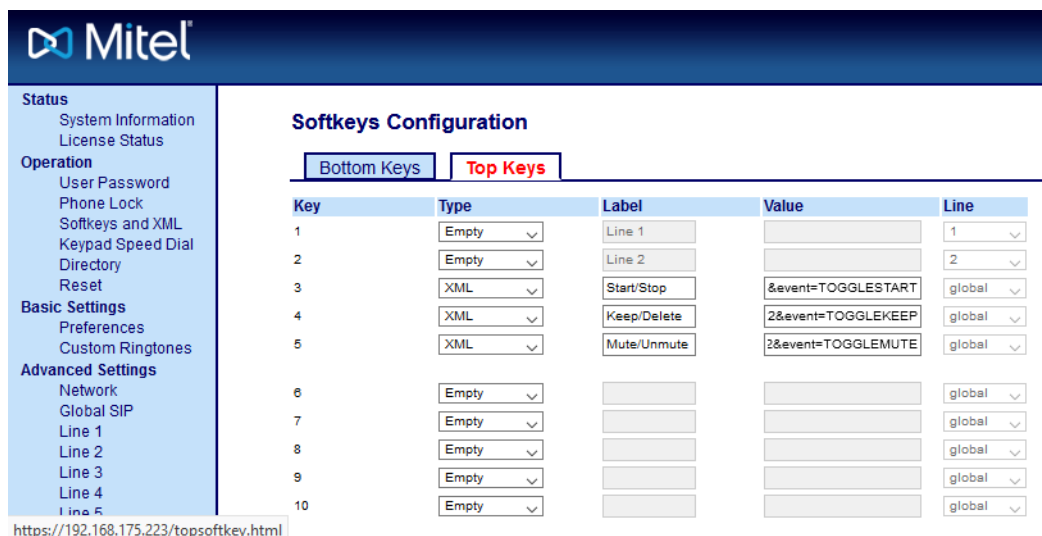


For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

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.



Mitel

Status
System Information
License Status

Operation
User Password
Phone Lock
Softkeys and XML
Keypad Speed Dial
Directory
Reset

Basic Settings
Preferences
Custom Ringtones

Advanced Settings
Network
Global SIP
Line 1
Line 2
Line 3
Line 4
Line 5

Softkeys Configuration

Bottom Keys **Top Keys**

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

<https://192.168.175.223/topsoftkey.html>

Fig. 526: 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	<code>http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGLESTART</code>
Keep/Delete	<code>http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGLEKEEP</code>
Mute/Unmute	<code>http://192.168.173.171/PHONEapp/MitelPHONEApp?&deviceExtension=\$\$\$SIPUSERNAME\$\$&event=TOGGMUTE</code>

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*.

Status System Information License Status Operation User Password Phone Lock Softkeys and XML Keypad Speed Dial Directory Reset Basic Settings Preferences Custom Ringtones Advanced Settings 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> IPv6 Settings IPv6 <input type="checkbox"/> Enabled </div> <div> Basic Network Settings 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> Advanced Network Settings 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> HTTPS Settings 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. 527: 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.

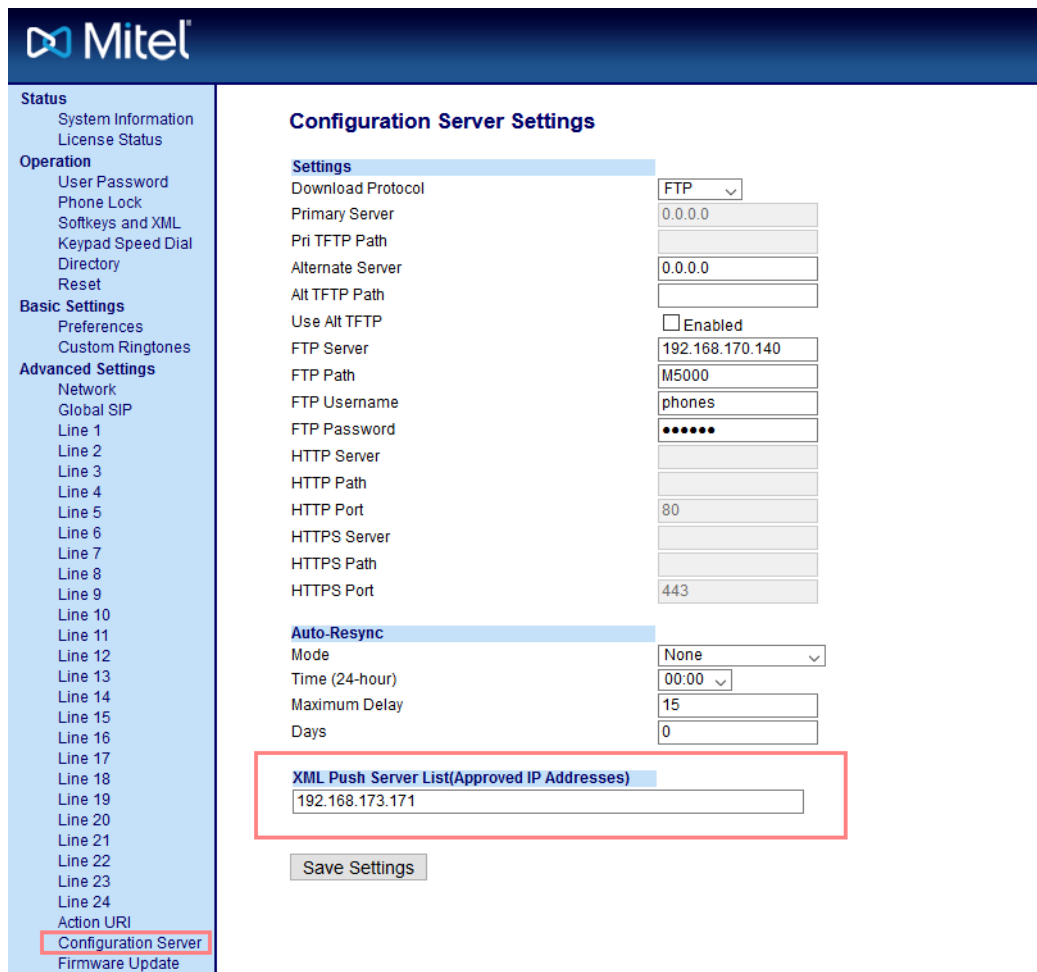


Fig. 528: Configure XML Push Server

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. 529: 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.

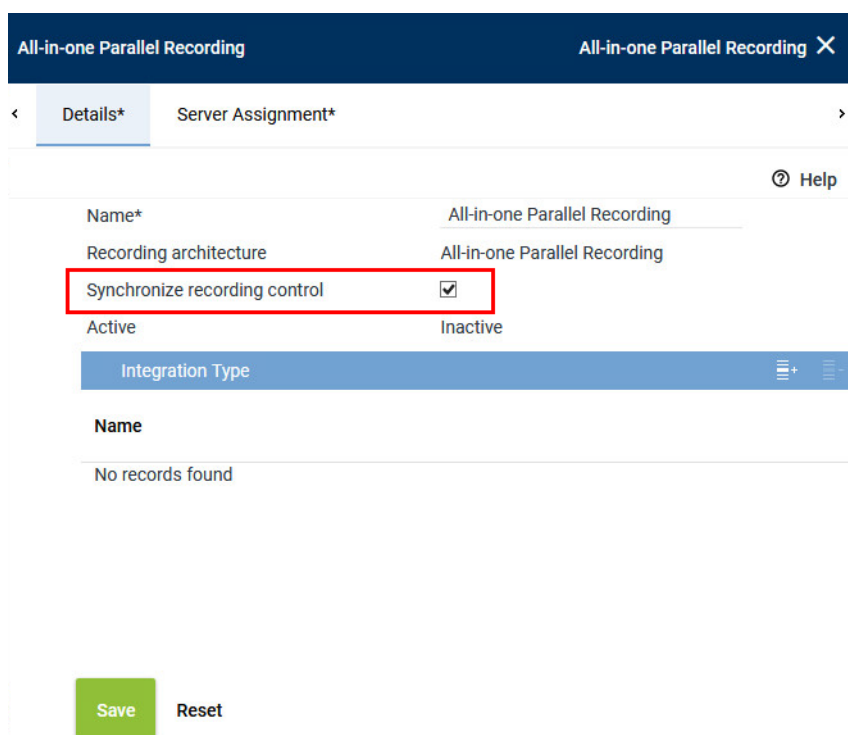
If recording is supposed to be controlled manually by means of applications such as *CLIENT-command*, *PHONEapp*, *SCREENrec* scan Editor, or by external control, synchronization of the Recording Control Services of the parallel recording servers must be created.

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 interface 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 single row with the value 'Name'. At the bottom of the interface are two buttons: 'Save' (green) and 'Reset' (grey).

Fig. 530: 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. 531: Menu item Manage Synchronization Configurations

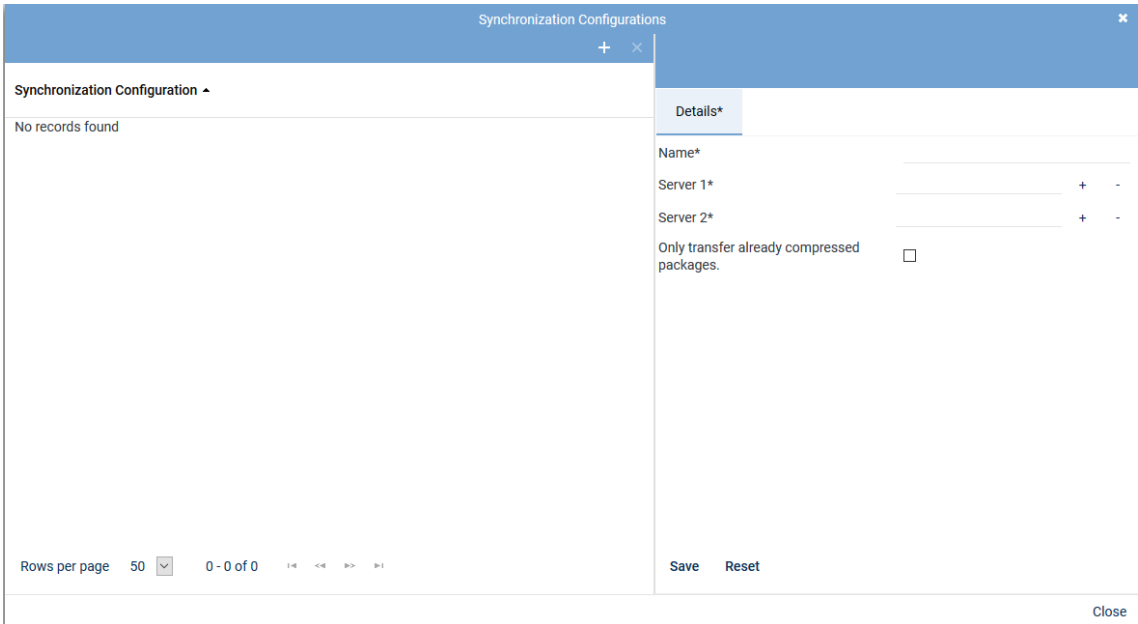




Fig. 532: Configure synchronization configurations

The following options are available:


	Create	Creates a new synchronization configuration, see chapter "Create synchronization configuration", p. 441 .
	Delete	Deletes the selected synchronization configuration, see chapter "Delete synchronization configuration", p. 442 .

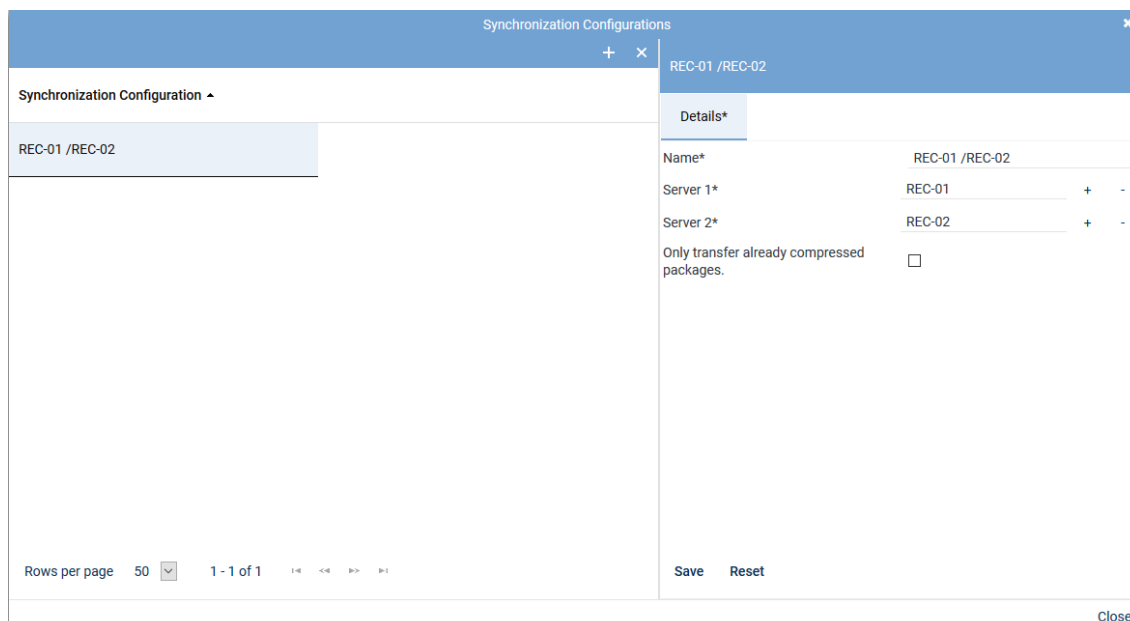
A synchronization configuration becomes active upon saving it and remains active until deleted. During this time, both system storages are regularly checked for new content and synchronized.



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

1. In the window *Administrate Synchronization Configuration*, click on the icon  (*Create*).
⇒ The tab *Details* becomes active.



The screenshot shows a window titled "Synchronization Configurations" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "Synchronization Configuration" (selected) and "Details*". The "Synchronization Configuration" tab shows a table with one row labeled "REC-01 / REC-02". At the bottom of this tab, there is a "Rows per page" dropdown set to "50", a "1 - 1 of 1" indicator, and navigation buttons. The "Details*" tab is active, showing fields for "Name*" (REC-01 / REC-02), "Server 1*" (REC-01 with + and - buttons), "Server 2*" (REC-02 with + and - buttons), and a checkbox for "Only transfer already compressed packages." (which is unchecked). At the bottom of the details tab are "Save" and "Reset" buttons. A "Close" button is located at the bottom right of the window.


Fig. 533: Create synchronization configuration

2. Complete all fields for the new synchronization configuration:

Name	Enter a name for the synchronization configuration.
Server 1 / Server 2	<p>Click on the button + next to the entry field to select the respective server for the synchronization of the system storage from the list of available servers.</p> <p>If you would like to delete an entry in one of the entry fields, click on the button - next to the respective entry field.</p>
Only transfer already compressed packages	<p>Select whether data which has not yet been compressed is supposed to be transferred, too.</p> <p><input checked="" type="checkbox"/> = Uncompressed data is transferred, too. <input type="checkbox"/> = Only compressed data is transferred.</p> <p>NOTICE! This option is not available until you have entered and saved the two servers.</p>

3. Click on the button **Save** to apply the configuration.
4. Click on the button **Close** to finish this configuration step and close the window.

7.3.5.2.2 Delete synchronization configuration

1. In the window *Administrate synchronization configurations*, select the synchronization configuration you would like to delete.
 2. Click on the icon  (**Delete**) in the toolbar of the window.
- ⇒ The synchronization of the two entered system storages is finished.
- ⇒ The selected synchronization configuration is deleted.

7.3.6 Configure duplicate detection

The following duplicates may occur in the recording system:

Conversation

Umbrella term for the different types of communication that can be recorded. A conversation may consist of several recordings. Several scenarios may cause duplicate conversations and duplicate recordings.

Recording

A recording is a part of a conversation. Due to different participants and events during a conversation such as consultations, interruptions, or transfers one conversation may consist of several recordings.

The following scenarios may cause duplicate conversations or duplicate recordings:

1. In internal conversations, duplicate recordings may occur when both participants have been configured for recording.
2. In parallel recording architectures, the conversations are saved twice. Duplicate recordings within those two conversations may occur when both participants have been configured for recording.
3. In parallel synchronized recording architectures, only one conversation is created. This conversation may still contain duplicate recording sections.

Conversations or recordings are considered identical if they have the following characteristics:

- Identical start and end times

You can define a difference for start and end times so that conversations are still considered as duplicates despite of a certain difference, see [chapter "Tab Detect Duplicates", p. 443](#).

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

- Identical conversation participants
- Identical additional data

To calculate the recording duration, the sum of all recording durations of all sections of a conversation are taken into account. The additional data as well as the audio data of the duplicate are deleted. If the recording duration is identical, the recording which has been checked last is considered the duplicate. You can check the execution status in the Jobs module.



For information about the status of a job refer to the Jobs module in the application System Monitoring, see user manual *Usage System Monitoring*.

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

Duplicate detection is configured in the Integrations module. There, you can select for each integration separately, when conversations are supposed to be considered as identical.

7.3.6.1

Tab Detect Duplicates

1. In the main view of the Integrations module, select the integration for which you would like to configure duplicate detection.
2. In the detail view, select the tab *Detect Duplicates* and adjust the respective settings.

Details*
Recording Content Validation
Detect Duplicates

☒ Delete nothing
☐ Delete redundant recordings
☐ Delete redundant recordings and conversations
☐ Delete redundant conversations

The start times differ by a maximum of * Milliseconds

The end times differ by a maximum of * Milliseconds

Additional settings

Time after which conversations are to be checked at the earliest * 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. 534: Tab Detect Duplicates (integration)

A conversation may consist of several recordings. Duplicate recordings may occur here. This may be the case for internal conversations for instance when all participants are recorded. External conversations may be divided into several recordings and recorded as duplicates, too, e. g. when a new participant is added to the conversation, when a conversation is transferred, put on hold or a consultation takes place.

- Select the deletion criteria for duplicates from the following options.

<i>Delete nothing</i>	Duplicates are not deleted. Be aware of the required storage consumption.
<i>Delete redundant recordings</i>	This option only deletes duplicate recordings within one conversation.
<i>Delete redundant recordings and conversations</i>	This option deletes duplicate conversations. If there are duplicate recording sections within the remaining conversation, they are deleted from the remaining conversation, too.
<i>Delete redundant conversations</i>	This option only deletes duplicate conversations which occur e. g. in parallel recording which has not been synchronized. Duplicate recording sections within the remaining conversations are maintained.

Tab. 115: Deletion criteria for duplicates

<i>The start times differ in a maximum of</i>	<p>Select the maximum difference for the start time. The start times of complete conversations as well as of individual recordings belonging to a conversation are checked.</p> <p>Example: <i>1.000 milliseconds</i></p> <p>If one conversation started at 2:20:15 pm and a second conversation started at 2:20:16 pm and if the start times of the individual recordings of the two conversations do not differ for more than 1.000 milliseconds, then the conversations are considered as possible duplicates with regard to their start time.</p>
<i>The end times differ in a maximum of</i>	<p>Select the maximum difference for the end time. The end times of complete conversations as well as of individual recording sections of a conversation are checked.</p> <p>Example: <i>1.000 milliseconds</i></p> <p>If one conversation ended at 2:20:15 pm and a second conversation ended at 2:20:16 pm and if the end times of the individual recordings of the two conversations do not differ for more than 1.000 milliseconds, then the conversations are considered as possible duplicates with regard to their end time.</p>
Additional Settings	NOTICE! This setting is only active if you include conversations to be deleted.
<i>Time after which conversations are to be checked at the earliest</i>	<p>Select the time period which is supposed to pass before the recordings of conversations are supposed to be checked for duplicates.</p> <p>Example: <i>3 minutes</i></p> <p>If a conversation ended at 2:20 pm, i. e. the recording has been saved at 2:20 pm, then the recording is not checked for duplicates before 2:23 pm.</p>

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.

1. In the list *Additional data*, click on the icon  (*Add*) to configure more additional data.

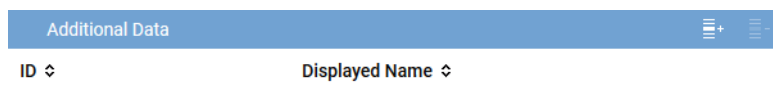


Fig. 535: Map additional data

2. 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. 536: 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. 537: 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 or recordings to be detected as duplicates.

If conversations or recordings differ in just one attribute, they are not considered as duplicates. This holds true for conversations or recordings 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.

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

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.



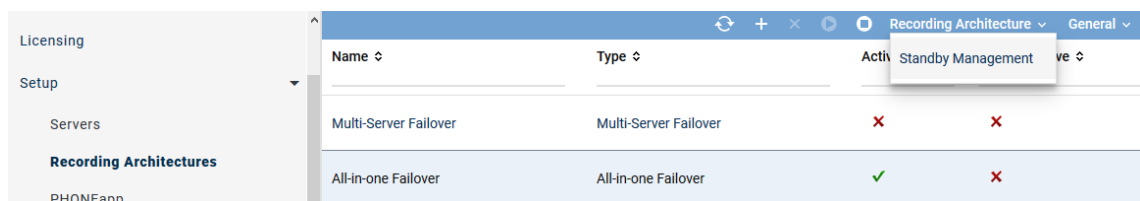
You can only make changes in standby management when the corresponding recording architecture has been activated.

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.



Name	Type	Active	Standby Management
Multi-Server Failover	Multi-Server Failover	✗	✗
All-in-one Failover	All-in-one Failover	✓	✗

Fig. 538: 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. 539: 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/Deactivate 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.

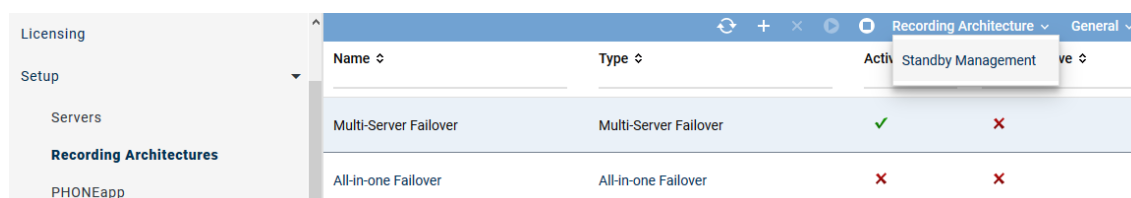


Fig. 540: Menu of the standby management

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. 541: 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/Deactivate 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.

7.4 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.

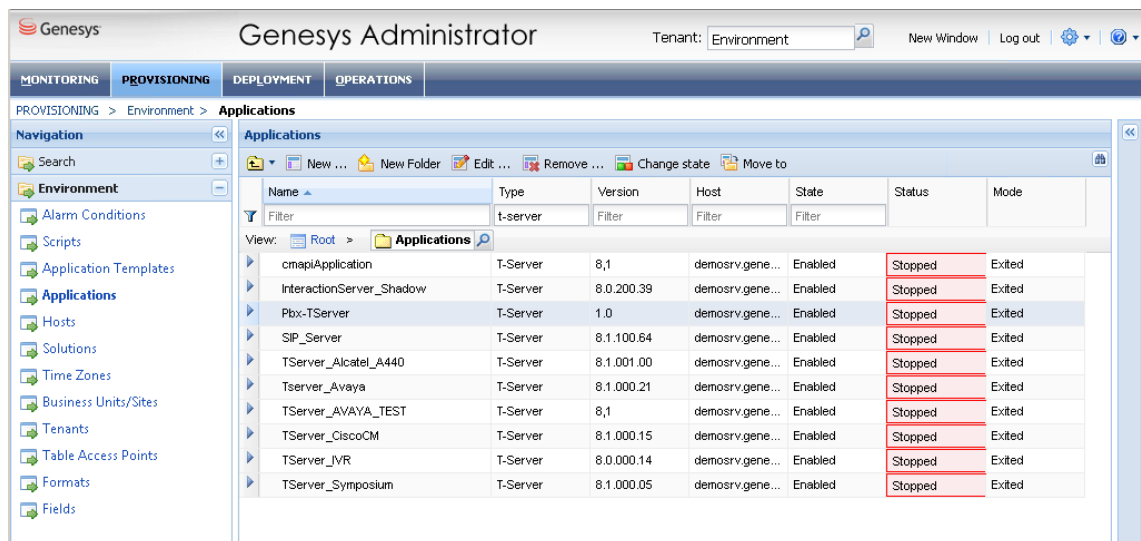


Fig. 542: Genesys Administrator - select T-Server

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*.

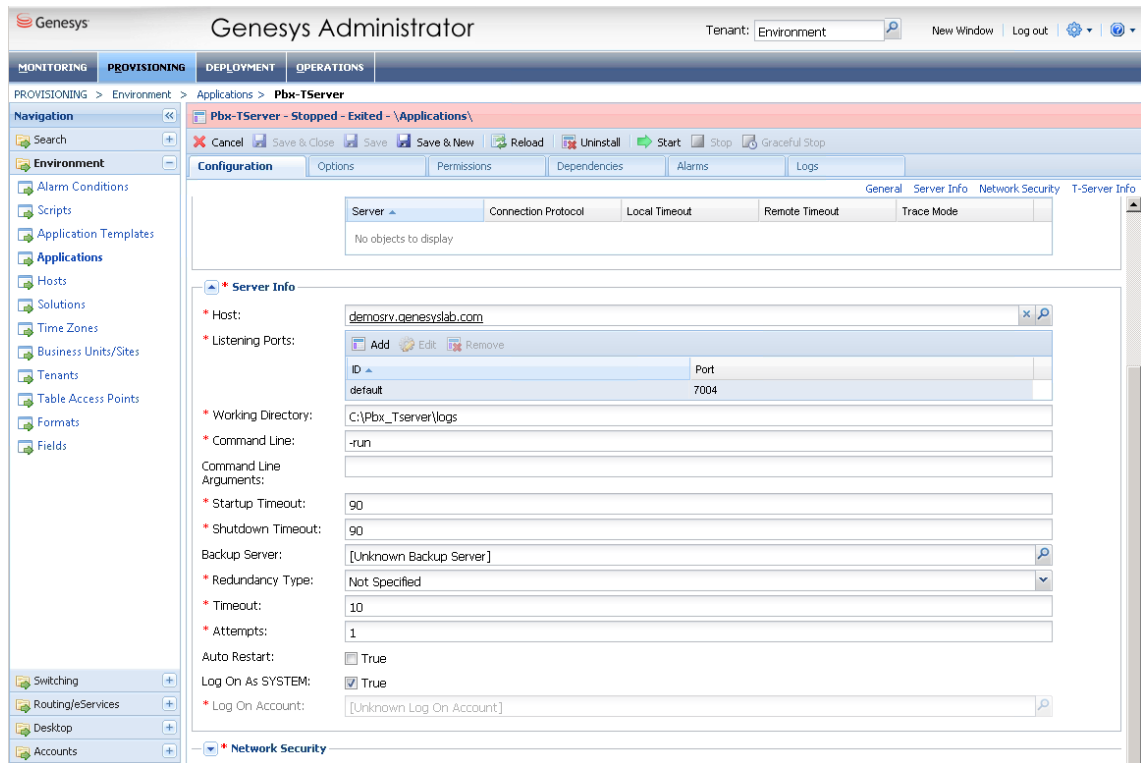


Fig. 543: Genesys Administrator - configure T-Server

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.

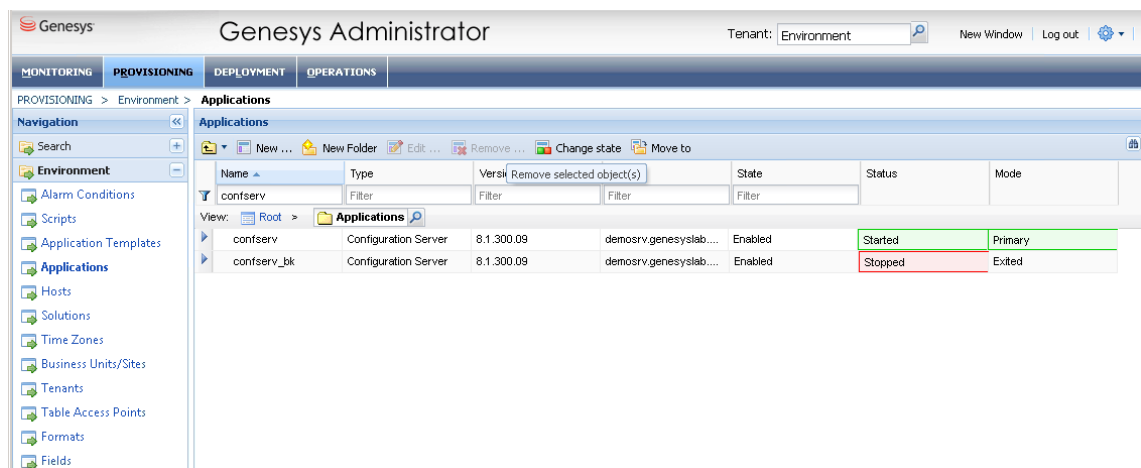


Fig. 544: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.
⇒ The window *Configuration* appears.
3. Expand the area *Server Info*.

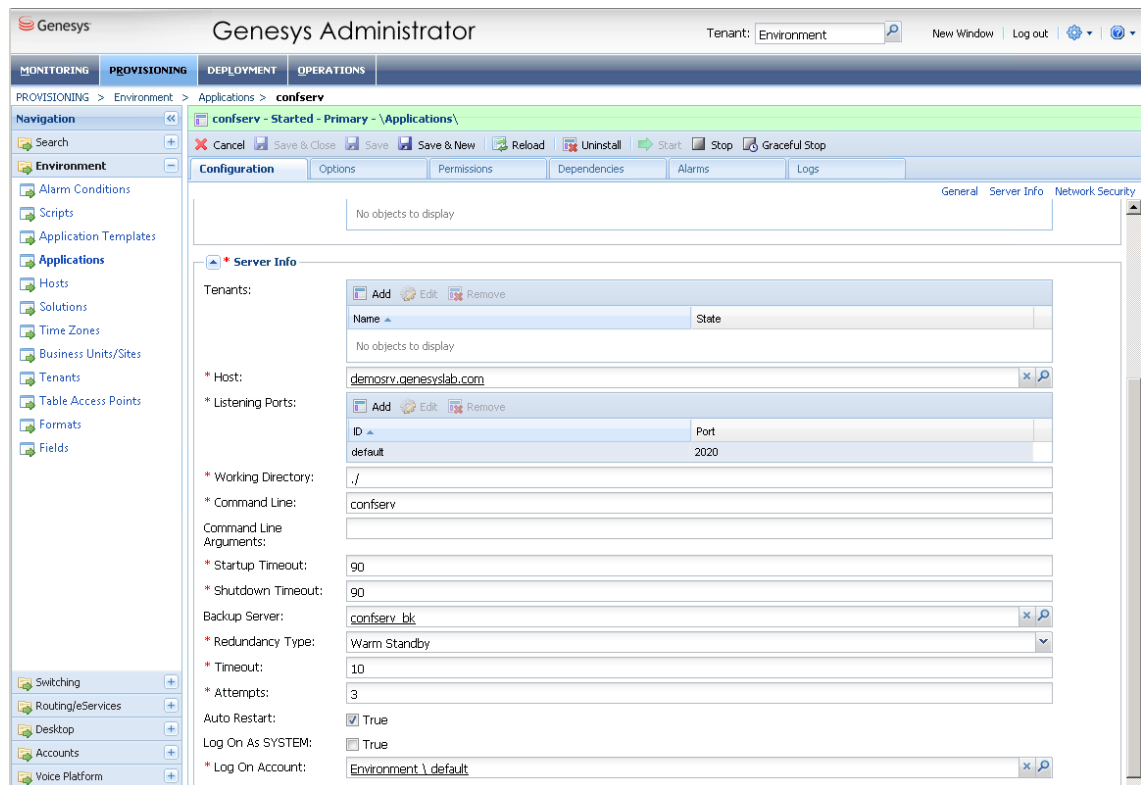


Fig. 545: Genesys Administrator - configure configuration server

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.

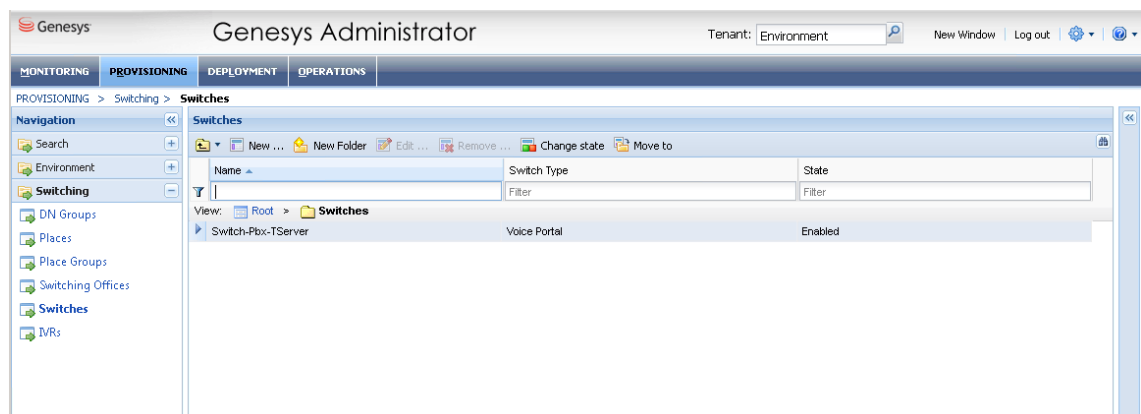
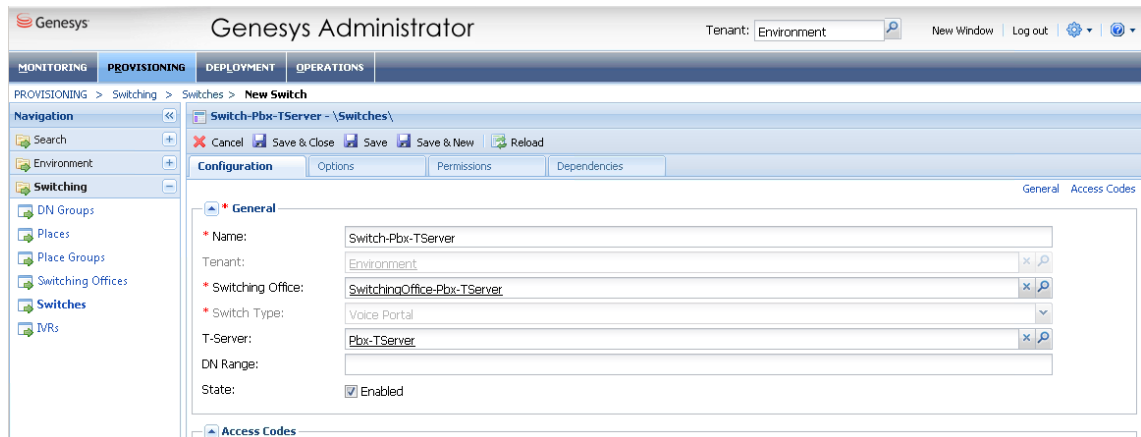


Fig. 546: Genesys Administrator - switch instances

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.

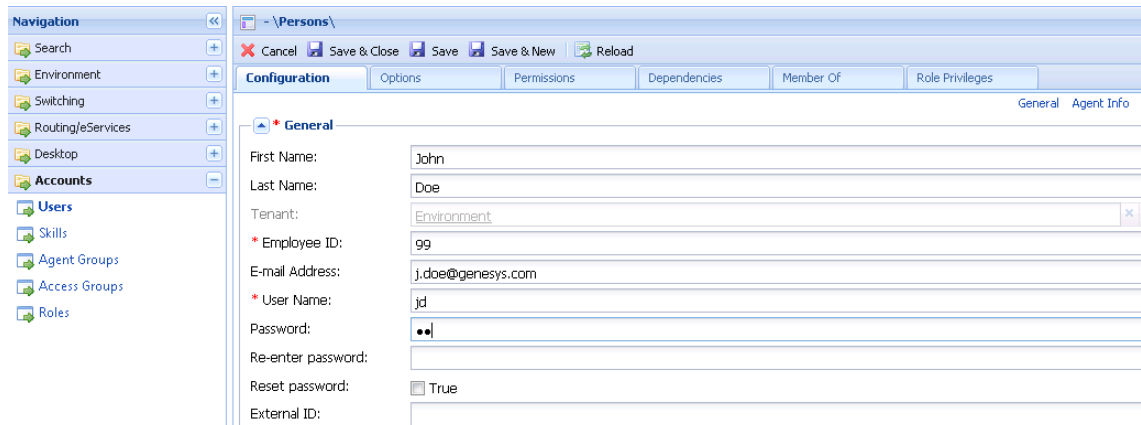
Fig. 547: Genesys Administrator - configure switch instance

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. 548: 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 (Active Stream Recording).....	6
Fig. 2	Recording solution with MBG	7
Fig. 3	Recording solution with intrusion	7
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	Proxy configuration	23
Fig. 18	Create forwarding rule for the port of the replay server	24
Fig. 19	Select PSK method.....	24
Fig. 20	Login screen MBG	24
Fig. 21	Certificate Management.....	25
Fig. 22	Confirm selected certificate	26
Fig. 23	Success notification for shared certificate	26
Fig. 24	System Configuration - Web interface	27
Fig. 25	System Configuration - main view	28
Fig. 26	Recording architectures - main view.....	29
Fig. 27	Toolbar Recording Architectures module	29
Fig. 28	Create recording architecture - All-in-one Basic Recording.....	30
Fig. 29	Recording architecture - tab Details	31
Fig. 30	Select integration type	31
Fig. 31	Recording architecture - tab Server Assignment.....	32
Fig. 32	Recording architecture - assign server	32
Fig. 33	Recording architecture - activate recording variant	33
Fig. 34	Recording architecture - activate recording architecture	33
Fig. 35	Servers - main view	34
Fig. 36	Toolbar Servers module	34
Fig. 37	Add server locations	35
Fig. 38	Delete server location	36
Fig. 39	Servers - tab Details	37
Fig. 40	Servers - tab usage	37

Fig. 41	Group field API Server	38
Fig. 42	Select storage expansion	39
Fig. 43	Group field Audio Analysis.....	40
Fig. 44	Select server for emotion detection	40
Fig. 45	Group field Recording Control/Key Management	40
Fig. 46	Group field Data Processing	41
Fig. 47	Select server	43
Fig. 48	Group field Replay	44
Fig. 49	Select server	45
Fig. 50	Group field Virtualization.....	46
Fig. 51	Servers module - tab Media Streamer	47
Fig. 52	Servers module - tab Replay Server Address Mapping.....	48
Fig. 53	Servers module - tab Key Management	50
Fig. 54	Servers module - tab Keystore/Virtualization	52
Fig. 55	PBX module - main view.....	53
Fig. 56	Toolbar PBX module.....	53
Fig. 57	Create new PBX - tab Details	54
Fig. 58	Tenants - main view - tab Extensions	55
Fig. 59	Assign extensions to tenants	56
Fig. 60	Remove extensions	57
Fig. 61	Select extensions.....	58
Fig. 62	Tenants - main view - tab PBX Agent ID	59
Fig. 63	Assign PBX Agent IDs to tenants	59
Fig. 64	Select PBX Agent IDs.....	61
Fig. 65	Additional Data module main view.....	62
Fig. 66	Configure additional data	62
Fig. 67	Additional data - configure availability	63
Fig. 68	Integrations - main view	64
Fig. 69	Toolbar Integrations module	64
Fig. 70	Choose file	65
Fig. 71	Upload grammar	65
Fig. 72	Create integration type	66
Fig. 73	Integrations - select PBX	66
Fig. 74	Assign recording architecture - All-in-one Basic	67
Fig. 75	Configuration steps of the integration	67
Fig. 76	Configuration step - Configure Recording Architecture	68
Fig. 77	CTI connection data - tab MiVoice MX-ONE (CSTA)	69
Fig. 78	Configure CTIconnect module	69
Fig. 79	Configure connection data	70
Fig. 80	Configure connection data	70
Fig. 81	Group field Additional Data - free assignment of additional data.....	71
Fig. 82	Configure switching conditions	72

Fig. 83	Configure regular expression for phone type identification.....	73
Fig. 84	Activate CTIconnect connection data for MBG.....	73
Fig. 85	Configure CTIconnect module.....	73
Fig. 86	Group field Connection Data	74
Fig. 87	Configure connection.....	74
Fig. 88	Group field Additional Data - free assignment of additional data.....	76
Fig. 89	Configuration step - configure monitor points.....	76
Fig. 90	Add extension monitor points	77
Fig. 91	Configured extension monitor points	78
Fig. 92	Configuration step - Global Recording Settings.....	79
Fig. 93	Configuration step - Configure recording servers	81
Fig. 94	Configure add-on for MiContact Center Enterprise	82
Fig. 95	Group field Additional Data - free assignment of additional data.....	83
Fig. 96	Overview of the add on of Genesys T-Server.....	84
Fig. 97	Configure add-on for Genesys T-Server.....	86
Fig. 98	Configure connection data	87
Fig. 99	Group field Additional Data - free assignment of additional data.....	88
Fig. 100	Configure miscellaneous settings	89
Fig. 101	Activate integration	89
Fig. 102	Activated integration	90
Fig. 103	Deactivate integration	90
Fig. 104	Recording architectures - main view.....	91
Fig. 105	Toolbar Recording Architectures module	91
Fig. 106	Create recording architecture - All-in-one Failover	93
Fig. 107	Recording architecture - tab Details - All-in-one Failover	93
Fig. 108	Select integration type	94
Fig. 109	Recording Architecture - tab Server Assignment.....	95
Fig. 110	Recording Architecture - assign server - example.....	95
Fig. 111	Recording Architecture - activate recording type.....	96
Fig. 112	Recording architecture - activate recording architecture	96
Fig. 113	Servers - main view	97
Fig. 114	Toolbar Servers module	97
Fig. 115	Add server locations	99
Fig. 116	Delete server location	100
Fig. 117	Servers - tab Details	100
Fig. 118	Servers - tab usage	101
Fig. 119	Group field API Server.....	101
Fig. 120	Select storage expansion	103
Fig. 121	Group field Audio Analysis.....	103
Fig. 122	Select server for emotion detection	104
Fig. 123	Group field Recording Control/Key Management.....	104
Fig. 124	Group field Data Processing.....	105

Fig. 125	Select server	107
Fig. 126	Group field Replay	107
Fig. 127	Select server	109
Fig. 128	Group field Virtualization.....	109
Fig. 129	Servers module - tab Media Streamer	110
Fig. 130	Servers module - tab Replay Server Address Mapping.....	112
Fig. 131	Servers module - tab Key Management	113
Fig. 132	Servers module - tab Keystore/Virtualization	115
Fig. 133	PBX module - main view.....	116
Fig. 134	Toolbar PBX module.....	116
Fig. 135	Create new PBX - tab Details	118
Fig. 136	Tenants - main view - tab Extensions	119
Fig. 137	Assign extensions to tenants	120
Fig. 138	Remove extensions	121
Fig. 139	Select extensions.....	122
Fig. 140	Tenants - main view - tab PBX Agent ID	123
Fig. 141	Assign PBX Agent IDs to tenants	123
Fig. 142	Select PBX Agent IDs.....	125
Fig. 143	Additional Data module main view.....	126
Fig. 144	Configure additional data	126
Fig. 145	Additional data - configure availability	127
Fig. 146	Integrations - main view	128
Fig. 147	Toolbar Integrations module	128
Fig. 148	Choose file.....	129
Fig. 149	Upload grammar	129
Fig. 150	Create integration type	130
Fig. 151	Integrations - select PBX	130
Fig. 152	Assign recording architecture - All-in-one Failover	131
Fig. 153	Configuration steps of the integration	131
Fig. 154	Configuration step - Configure Recording Architecture	132
Fig. 155	CTI connection data - tab MiVoice MX-ONE (CSTA)	133
Fig. 156	Configure CTIconnect module	133
Fig. 157	Configure connection data	134
Fig. 158	Configure connection data	134
Fig. 159	Group field Additional Data - free assignment of additional data.....	135
Fig. 160	Configure switching conditions	136
Fig. 161	Configure regular expression for phone type identification.....	137
Fig. 162	Activate CTIconnect connection data for MBG	137
Fig. 163	Configure CTIconnect module	137
Fig. 164	Group field Connection Data	138
Fig. 165	Configure connection	138
Fig. 166	Group field Additional Data - free assignment of additional data.....	140

Fig. 167	Configuration step - configure monitor points	140
Fig. 168	Add extension monitor points	141
Fig. 169	Configured extension monitor points	142
Fig. 170	Configuration step - Global Recording Settings.....	143
Fig. 171	Configuration step - Configure recording servers	145
Fig. 172	Tab Extensions	146
Fig. 173	Add extensions	146
Fig. 174	Added extensions	147
Fig. 175	Configuration step - Configure recording servers	147
Fig. 176	Tab Extensions	148
Fig. 177	Add extensions	149
Fig. 178	Added extensions	149
Fig. 179	Configure add-on for MiContact Center Enterprise	151
Fig. 180	Group field Additional Data - free assignment of additional data.....	152
Fig. 181	Overview of the add on of Genesys T-Server.....	153
Fig. 182	Configure add-on for Genesys T-Server.....	154
Fig. 183	Configure connection data	155
Fig. 184	Group field Additional Data - free assignment of additional data.....	156
Fig. 185	Configure miscellaneous settings	157
Fig. 186	Activate integration	158
Fig. 187	Activated integration	158
Fig. 188	Deactivate integration	159
Fig. 189	Recording architectures - main view.....	159
Fig. 190	Toolbar Recording Architectures module	160
Fig. 191	Create recording architecture - All-in-one Parallel Recording	161
Fig. 192	Recording architecture - tab Details - All-in-one Parallel Recording.....	161
Fig. 193	Select integration type	162
Fig. 194	Recording Architecture - tab Server Assignment.....	163
Fig. 195	Recording Architecture - assign server - example.....	163
Fig. 196	Recording Architecture - activate recording type.....	164
Fig. 197	Activate recording architecture	164
Fig. 198	Servers - main view	165
Fig. 199	Toolbar Servers module	165
Fig. 200	Add server locations	166
Fig. 201	Delete server location	167
Fig. 202	Servers - tab Details	168
Fig. 203	Servers - tab usage	168
Fig. 204	Group field API Server	169
Fig. 205	Select storage expansion	170
Fig. 206	Group field Audio Analysis.....	171
Fig. 207	Select server for emotion detection	171
Fig. 208	Group field Recording Control/Key Management.....	171

Fig. 209	Group field Data Processing	172
Fig. 210	Select server	174
Fig. 211	Group field Replay	175
Fig. 212	Select server	176
Fig. 213	Group field Virtualization	177
Fig. 214	Servers module - tab Media Streamer	178
Fig. 215	Servers module - tab Replay Server Address Mapping	179
Fig. 216	Servers module - tab Key Management	181
Fig. 217	Servers module - tab Keystore/Virtualization	183
Fig. 218	PBX module - main view	184
Fig. 219	Toolbar PBX module	184
Fig. 220	Create new PBX - tab Details	185
Fig. 221	Tenants - main view - tab Extensions	186
Fig. 222	Assign extensions to tenants	187
Fig. 223	Remove extensions	188
Fig. 224	Select extensions	189
Fig. 225	Tenants - main view - tab PBX Agent ID	190
Fig. 226	Assign PBX Agent IDs to tenants	190
Fig. 227	Select PBX Agent IDs	192
Fig. 228	Additional Data module main view	193
Fig. 229	Configure additional data	193
Fig. 230	Additional data - configure availability	194
Fig. 231	Integrations - main view	195
Fig. 232	Toolbar Integrations module	195
Fig. 233	Choose file	196
Fig. 234	Upload grammar	196
Fig. 235	Create integration type	197
Fig. 236	Integrations - select PBX	197
Fig. 237	Assign recording architecture - All-in-one Parallel	198
Fig. 238	Configuration steps of the integration	198
Fig. 239	Configuration step - Configure Recording Architecture	199
Fig. 240	Configure tab MiVoice MX-ONE (CSTA)	200
Fig. 241	Configure CTIconnect module	200
Fig. 242	Configure connection data	201
Fig. 243	Configure connection data	201
Fig. 244	Group field Additional Data - free assignment of additional data	202
Fig. 245	Configure switching conditions	203
Fig. 246	Configure regular expression for phone type identification	204
Fig. 247	Activate CTIconnect connection data for MBG	204
Fig. 248	Configure CTIconnect module	205
Fig. 249	Group field Connection Data	205
Fig. 250	Configure connection	206

Fig. 251	Group field Additional Data - free assignment of additional data.....	207
Fig. 252	Configuration step - configure monitor points	208
Fig. 253	Add extension monitor points	208
Fig. 254	Configured extension monitor points	210
Fig. 255	Configuration step - Global Recording Settings.....	211
Fig. 256	Configuration step - Configure recording servers	212
Fig. 257	Configure add-on for MiContact Center Enterprise	214
Fig. 258	Group field Additional Data - free assignment of additional data.....	215
Fig. 259	Overview of the add on of Genesys T-Server.....	216
Fig. 260	Configure add-on for Genesys T-Server.....	217
Fig. 261	Configure connection data	218
Fig. 262	Group field Additional Data - free assignment of additional data.....	219
Fig. 263	Configure miscellaneous settings	220
Fig. 264	Activate integration	221
Fig. 265	Activated integration	221
Fig. 266	Deactivate integration	222
Fig. 267	Recording architectures - main view.....	222
Fig. 268	Create recording architecture - Multi-Server Recording	223
Fig. 269	Recording architecture - tab Details - Multi-Server Recording	224
Fig. 270	Select integration type	225
Fig. 271	Recording architecture - tab Server Assignment.....	226
Fig. 272	Recording architecture - assign server - example	226
Fig. 273	Add recording server	227
Fig. 274	Recording architecture - activate recording architecture	228
Fig. 275	Servers - main view	229
Fig. 276	Toolbar Servers module	229
Fig. 277	Add server locations	230
Fig. 278	Delete server location	231
Fig. 279	Servers - tab Details	232
Fig. 280	Servers - tab usage	232
Fig. 281	Group field API Server.....	233
Fig. 282	Select storage expansion	234
Fig. 283	Group field Audio Analysis.....	235
Fig. 284	Select server for emotion detection	235
Fig. 285	Group field Recording Control/Key Management.....	235
Fig. 286	Group field Data Processing.....	236
Fig. 287	Select server.....	238
Fig. 288	Group field Replay	239
Fig. 289	Select server.....	240
Fig. 290	Group field Virtualization.....	241
Fig. 291	Servers module - tab Media Streamer.....	242
Fig. 292	Servers module - tab Replay Server Address Mapping.....	243

Fig. 293 Servers module - tab Key Management	245
Fig. 294 Servers module - tab Keystore/Virtualization	247
Fig. 295 PBX module - main view.....	248
Fig. 296 Toolbar PBX module.....	248
Fig. 297 Create new PBX - tab Details	249
Fig. 298 Tenants - main view - tab Extensions	250
Fig. 299 Assign extensions to tenants	251
Fig. 300 Remove extensions	252
Fig. 301 Select extensions.....	253
Fig. 302 Tenants - main view - tab PBX Agent ID	254
Fig. 303 Assign PBX Agent IDs to tenants	254
Fig. 304 Select PBX Agent IDs.....	256
Fig. 305 Additional Data module main view.....	257
Fig. 306 Configure additional data.....	257
Fig. 307 Additional data - configure availability	258
Fig. 308 Integrations - main view	259
Fig. 309 Toolbar Integrations module	259
Fig. 310 Choose file.....	260
Fig. 311 Upload grammar	260
Fig. 312 Create integration type	261
Fig. 313 Integrations - select PBX	261
Fig. 314 Assign recording architecture - Multi-Server Recording	262
Fig. 315 Configuration steps of the integration	262
Fig. 316 Configuration step - Configure Recording Architecture	263
Fig. 317 CTI connection data - tab MiVoice MX-ONE (CSTA)	264
Fig. 318 Configure CTIconnect module.....	264
Fig. 319 Configure connection data.....	265
Fig. 320 Configure connection data.....	265
Fig. 321 Group field Additional Data - free assignment of additional data.....	266
Fig. 322 Configure switching conditions	267
Fig. 323 Configure regular expression for phone type identification.....	268
Fig. 324 Activate CTIconnect connection data for MBG.....	268
Fig. 325 Configure CTIconnect module.....	268
Fig. 326 Group field Connection Data	269
Fig. 327 Configure connection.....	269
Fig. 328 Group field Additional Data - free assignment of additional data.....	271
Fig. 329 Configuration step - configure monitor points	271
Fig. 330 Add extension monitor points	272
Fig. 331 Configured extension monitor points	273
Fig. 332 Configuration step - Global Recording Settings.....	274
Fig. 333 Configuration step - Configure recording servers	276
Fig. 334 Tab Extensions	277

Fig. 335 Add extensions	277
Fig. 336 Added extensions	278
Fig. 337 Configure add-on for MiContact Center Enterprise	279
Fig. 338 Group field Additional Data - free assignment of additional data.....	280
Fig. 339 Overview of the add on of Genesys T-Server.....	281
Fig. 340 Configure add-on for Genesys T-Server.....	282
Fig. 341 Configure connection data	283
Fig. 342 Group field Additional Data - free assignment of additional data.....	284
Fig. 343 Configure miscellaneous settings	285
Fig. 344 Activate integration	286
Fig. 345 Activated integration	286
Fig. 346 Deactivate integration	287
Fig. 347 Recording architectures - main view.....	287
Fig. 348 Toolbar Recording Architectures module	288
Fig. 349 Create recording architecture - Multi-Server Failover	289
Fig. 350 Recording architecture - tab Details - Multi-Server Failover	289
Fig. 351 Select integration type	290
Fig. 352 Recording Architecture - tab Server Assignment.....	291
Fig. 353 Recording Architecture - assign server - example.....	292
Fig. 354 Add Recording Server	293
Fig. 355 Recording architecture - activate recording architecture	294
Fig. 356 Servers - main view	294
Fig. 357 Toolbar Servers module	295
Fig. 358 Add server locations	296
Fig. 359 Delete server location.....	297
Fig. 360 Servers - tab Details	297
Fig. 361 Servers - tab usage	298
Fig. 362 Group field API Server.....	298
Fig. 363 Select storage expansion	300
Fig. 364 Group field Audio Analysis.....	300
Fig. 365 Select server for emotion detection	301
Fig. 366 Group field Recording Control/Key Management.....	301
Fig. 367 Group field Data Processing.....	302
Fig. 368 Select server.....	304
Fig. 369 Group field Replay	304
Fig. 370 Select server.....	306
Fig. 371 Group field Virtualization.....	306
Fig. 372 Servers module - tab Media Streamer.....	307
Fig. 373 Servers module - tab Replay Server Address Mapping.....	309
Fig. 374 Servers module - tab Key Management	310
Fig. 375 Servers module - tab Keystore/Virtualization	312
Fig. 376 PBX module - main view.....	313

Fig. 377	Toolbar PBX module.....	313
Fig. 378	Create new PBX - tab Details	315
Fig. 379	Tenants - main view - tab Extensions	316
Fig. 380	Assign extensions to tenants	317
Fig. 381	Remove extensions	318
Fig. 382	Select extensions.....	319
Fig. 383	Tenants - main view - tab PBX Agent ID	320
Fig. 384	Assign PBX Agent IDs to tenants	320
Fig. 385	Select PBX Agent IDs.....	322
Fig. 386	Additional Data module main view.....	323
Fig. 387	Configure additional data	323
Fig. 388	Additional data - configure availability	324
Fig. 389	Integrations - main view	325
Fig. 390	Toolbar Integrations module	325
Fig. 391	Choose file.....	326
Fig. 392	Upload grammar	326
Fig. 393	Create integration type	327
Fig. 394	Integrations - select PBX	327
Fig. 395	Assign recording architecture - Multi-Server Failover.....	328
Fig. 396	Configuration steps of the integration	328
Fig. 397	Configuration step - Configure Recording Architecture	329
Fig. 398	CTI connection data - tab MiVoice MX-ONE (CSTA)	330
Fig. 399	Configure CTIconnect module	330
Fig. 400	Configure connection data.....	331
Fig. 401	Configure connection data.....	331
Fig. 402	Group field Additional Data - free assignment of additional data.....	332
Fig. 403	Configure switching conditions	333
Fig. 404	Configure regular expression for phone type identification.....	334
Fig. 405	Activate CTIconnect connection data for MBG.....	334
Fig. 406	Configure CTIconnect module	334
Fig. 407	Group field Connection Data	335
Fig. 408	Configure connection	335
Fig. 409	Group field Additional Data - free assignment of additional data.....	337
Fig. 410	Configuration step - configure monitor points	337
Fig. 411	Add extension monitor points	338
Fig. 412	Configured extension monitor points	339
Fig. 413	Configuration step - Global Recording Settings.....	340
Fig. 414	Configuration step - Configure recording servers	342
Fig. 415	Tab Extensions	343
Fig. 416	Add extensions	343
Fig. 417	Added extensions	344
Fig. 418	Configure add-on for MiContact Center Enterprise	345

Fig. 419	Group field Additional Data - free assignment of additional data.....	346
Fig. 420	Overview of the add on of Genesys T-Server.....	347
Fig. 421	Configure add-on for Genesys T-Server.....	348
Fig. 422	Configure connection data.....	349
Fig. 423	Group field Additional Data - free assignment of additional data.....	350
Fig. 424	Configure miscellaneous settings	351
Fig. 425	Activate integration	352
Fig. 426	Activated integration	352
Fig. 427	Deactivate integration.....	353
Fig. 428	Recording architectures - main view.....	353
Fig. 429	Toolbar Recording Architectures module	354
Fig. 430	Create recording architecture - Multi-Server Parallel Recording	355
Fig. 431	Recording architecture - tab Details - Multi-Server Parallel Recording	356
Fig. 432	Select integration type	357
Fig. 433	Recording architecture - server assignment device group 1	358
Fig. 434	Recording architecture - assign server - example	358
Fig. 435	Add recording server	359
Fig. 436	Recording architecture - activate recording architecture - example	360
Fig. 437	Servers - main view	361
Fig. 438	Toolbar Servers module	361
Fig. 439	Add server locations	362
Fig. 440	Delete server location.....	363
Fig. 441	Servers - tab Details	364
Fig. 442	Servers - tab usage	364
Fig. 443	Group field API Server.....	365
Fig. 444	Select storage expansion	366
Fig. 445	Group field Audio Analysis.....	367
Fig. 446	Select server for emotion detection	367
Fig. 447	Group field Recording Control/Key Management.....	367
Fig. 448	Group field Data Processing.....	368
Fig. 449	Select server.....	370
Fig. 450	Group field Replay	371
Fig. 451	Select server.....	372
Fig. 452	Group field Virtualization.....	373
Fig. 453	Servers module - tab Media Streamer.....	374
Fig. 454	Servers module - tab Replay Server Address Mapping.....	375
Fig. 455	Servers module - tab Key Management	377
Fig. 456	Servers module - tab Keystore/Virtualization	379
Fig. 457	PBX module - main view.....	380
Fig. 458	Toolbar PBX module.....	380
Fig. 459	Create new PBX - tab Details	381
Fig. 460	Tenants - main view - tab Extensions.....	382

Fig. 461	Assign extensions to tenants	383
Fig. 462	Remove extensions	384
Fig. 463	Select extensions.....	385
Fig. 464	Tenants - main view - tab PBX Agent ID	386
Fig. 465	Assign PBX Agent IDs to tenants	386
Fig. 466	Select PBX Agent IDs.....	388
Fig. 467	Additional Data module main view.....	389
Fig. 468	Configure additional data.....	389
Fig. 469	Additional data - configure availability	390
Fig. 470	Integrations - main view	391
Fig. 471	Toolbar Integrations module	391
Fig. 472	Choose file.....	392
Fig. 473	Upload grammar	392
Fig. 474	Create integration type	393
Fig. 475	Integrations - select PBX	393
Fig. 476	Assign recording architecture - Multi-Server Parallel.....	394
Fig. 477	Configuration steps of the integration	394
Fig. 478	Configuration step - Configure Recording Architecture	395
Fig. 479	Configure tab MiVoice MX-ONE (CSTA)	396
Fig. 480	Configure CTIconnect module.....	396
Fig. 481	Configure connection data.....	397
Fig. 482	Configure connection data.....	397
Fig. 483	Group field Additional Data - free assignment of additional data.....	398
Fig. 484	Configure switching conditions	399
Fig. 485	Configure regular expression for phone type identification.....	400
Fig. 486	Configure CTIconnect connection data to MBG	401
Fig. 487	Configure CTIconnect module.....	401
Fig. 488	Group field Connection Data	402
Fig. 489	Configure connection.....	402
Fig. 490	Group field Additional Data - free assignment of additional data.....	403
Fig. 491	Configuration step - configure monitor points	404
Fig. 492	Add extension monitor points	405
Fig. 493	Configured extension monitor points	406
Fig. 494	Configuration step - Global Recording Settings.....	407
Fig. 495	Configuration step - Configure recording servers	409
Fig. 496	Configure add-on for MiContact Center Enterprise	410
Fig. 497	Group field Additional Data - free assignment of additional data.....	411
Fig. 498	Overview of the add on of Genesys T-Server.....	412
Fig. 499	Configure add-on for Genesys T-Server.....	414
Fig. 500	Configure connection data.....	415
Fig. 501	Group field Additional Data - free assignment of additional data.....	416
Fig. 502	Configure miscellaneous settings	417

Fig. 503	Activate integration	417
Fig. 504	Activated integration	418
Fig. 505	Deactivate integration	418
Fig. 506	Servers module - Activate emotion detection	419
Fig. 507	Create integration - tab Recording Content Validation	420
Fig. 508	Select server for emotion detection	421
Fig. 509	Servers - tab Usage	422
Fig. 510	Group field Recording Control/Key Management	422
Fig. 511	PHONEapp - main view:	423
Fig. 512	Detail view phone types	424
Fig. 513	Display of the properties	424
Fig. 514	Detail view Default settings	425
Fig. 515	Group field Tagging Attributes	427
Fig. 516	Edit tagging attributes	428
Fig. 517	Group field Register Fields	428
Fig. 518	Edit register fields	429
Fig. 519	Configure tagging fields	430
Fig. 520	Edit tagging fields	430
Fig. 521	Activate PHONEapp configuration	431
Fig. 522	Phones - main view	432
Fig. 523	Toolbar	432
Fig. 524	Create phone	433
Fig. 525	Create phones - activate PHONEapp	434
Fig. 526	Configure key function via the web interface	436
Fig. 527	Configure HTTPS settings	437
Fig. 528	Configure XML Push Server	438
Fig. 529	Assignment of the top keys and displayed status of the recording	438
Fig. 530	Synchronize recording control	439
Fig. 531	Menu item Manage Synchronization Configurations	440
Fig. 532	Configure synchronization configurations	441
Fig. 533	Create synchronization configuration	442
Fig. 534	Tab Detect Duplicates (integration)	444
Fig. 535	Map additional data	445
Fig. 536	Select additional data	446
Fig. 537	Delete additional data assignment	446
Fig. 538	Configure standby management	447
Fig. 539	Switch server	448
Fig. 540	Menu of the standby management	449
Fig. 541	Switch server	449
Fig. 542	Genesys Administrator - select T-Server	451
Fig. 543	Genesys Administrator - configure T-Server	452
Fig. 544	Genesys Administrator - select configuration server	452

Fig. 545 Genesys Administrator - configure configuration server	453
Fig. 546 Genesys Administrator - switch instances	453
Fig. 547 Genesys Administrator - configure switch instance	454
Fig. 548 Genesys administrator - create user	454

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	27
Tab. 10	Configure audio analysis	40
Tab. 11	Configure recording control/key management.....	41
Tab. 12	Data storage	41
Tab. 13	Configure replay	44
Tab. 14	Configure virtualization	46
Tab. 15	Create PBX.....	54
Tab. 16	Create integration type	66
Tab. 17	Configure CTIconnect module.....	69
Tab. 18	Configure connection data.....	70
Tab. 19	Configure CTIconnect module.....	74
Tab. 20	Configure connection data.....	75
Tab. 21	Global recording settings	80
Tab. 22	Configure recording servers	81
Tab. 23	Configure CTIconnect module.....	83
Tab. 24	Configure connection data.....	83
Tab. 25	Configure add-on for Genesys T-Server.....	86
Tab. 26	Configure connection data.....	87
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	130
Tab. 34	Configure CTIconnect module.....	133
Tab. 35	Configure connection data.....	134
Tab. 36	Configure CTIconnect module.....	138
Tab. 37	Configure connection data.....	139
Tab. 38	Global recording settings	144
Tab. 39	Configure recording servers	145
Tab. 40	Configure recording servers	147
Tab. 41	Configure CTIconnect module.....	151

Tab. 42	Configure connection data	152
Tab. 43	Configure add-on for Genesys T-Server.....	154
Tab. 44	Configure connection data	156
Tab. 45	Configure audio analysis	171
Tab. 46	Configure recording control/key management.....	172
Tab. 47	Data storage	172
Tab. 48	Configure replay	175
Tab. 49	Configure virtualization	177
Tab. 50	Create PBX.....	185
Tab. 51	Create integration type	197
Tab. 52	Configure CTIconnect module	200
Tab. 53	Configure connection data	201
Tab. 54	Configure CTIconnect module	205
Tab. 55	Configure connection data	206
Tab. 56	Global recording settings	211
Tab. 57	Configure recording servers	212
Tab. 58	Configure CTIconnect module	214
Tab. 59	Configure connection data	215
Tab. 60	Configure add-on for Genesys T-Server.....	217
Tab. 61	Configure connection data	219
Tab. 62	Configure audio analysis	235
Tab. 63	Configure recording control/key management.....	236
Tab. 64	Data storage	236
Tab. 65	Configure replay	239
Tab. 66	Configure virtualization	241
Tab. 67	Create PBX.....	249
Tab. 68	Create integration type	261
Tab. 69	Configure CTIconnect module	264
Tab. 70	Configure connection data	265
Tab. 71	Configure CTIconnect module	269
Tab. 72	Configure connection data	270
Tab. 73	Global recording settings	275
Tab. 74	Configure recording servers	276
Tab. 75	Configure CTIconnect module	279
Tab. 76	Configure connection data	280
Tab. 77	Configure add-on for Genesys T-Server.....	282
Tab. 78	Configure connection data	284
Tab. 79	Configure audio analysis	300
Tab. 80	Configure recording control/key management.....	301
Tab. 81	Data storage	302
Tab. 82	Configure replay	304
Tab. 83	Configure virtualization	306

Tab. 84	Create PBX.....	315
Tab. 85	Create integration type	327
Tab. 86	Configure CTIconnect module.....	330
Tab. 87	Configure connection data.....	331
Tab. 88	Configure CTIconnect module.....	335
Tab. 89	Configure connection data.....	336
Tab. 90	Global recording settings	341
Tab. 91	Configure recording servers	342
Tab. 92	Configure CTIconnect module.....	345
Tab. 93	Configure connection data.....	346
Tab. 94	Configure add-on for Genesys T-Server.....	348
Tab. 95	Configure connection data.....	350
Tab. 96	Configure audio analysis	367
Tab. 97	Configure recording control/key management.....	368
Tab. 98	Data storage	368
Tab. 99	Configure replay	371
Tab. 100	Configure virtualization	373
Tab. 101	Create PBX.....	381
Tab. 102	Create integration type	393
Tab. 103	Configure CTIconnect module.....	396
Tab. 104	Configure connection data.....	397
Tab. 105	Configure CTIconnect module.....	401
Tab. 106	Configure connection data.....	402
Tab. 107	Global recording settings	407
Tab. 108	Configure recording servers	409
Tab. 109	Configure CTIconnect module.....	411
Tab. 110	Configure connection data.....	411
Tab. 111	Configure add-on for Genesys T-Server.....	414
Tab. 112	Configure connection data.....	415
Tab. 113	Configure recording control/key management.....	423
Tab. 114	Add phone	434
Tab. 115	Deletion criteria for duplicates	444

Glossary

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.

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)

FQDN

Fully Qualified Domain Name

ICP

Internet Communications Platform

IP

Internet Protocol, basic protocol for Internet communication

LCR

Last Conversation Repeat

LED

Light-emitting diode

MBG

MiVoice Border Gateway

MIR

Mitel Interaction Recording

PBX

Private Branch Exchange

PSK

The pre-shared key is required for using a Web Proxy in connection with a MiVoice Border Gateway.

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, protected data transmission

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 Socket 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
