

EVOIPneo active for Mitel MiVoice 5000



Administration manual for system providers

8/11/2022

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 | 8 |
| 3.1 | Hardware components..... | 8 |
| 3.1.1 | Recorder | 8 |
| 3.2 | Software components..... | 8 |
| 3.3 | Mitel system components | 8 |
| 3.4 | Genesys system components (optional)..... | 8 |
| 3.4.1 | Genesys Framework..... | 8 |
| 4 | Installation requirements | 9 |
| 4.1 | Licenses..... | 9 |
| 4.2 | Information..... | 10 |
| 5 | Overview install and configure product | 11 |
| 6 | Installation..... | 12 |
| 7 | Configuration | 13 |
| 7.1 | Configure Mitel MiVoice 5000..... | 13 |
| 7.2 | Configure MiVoice Border Gateway | 14 |
| 7.2.1 | Confirm certificate on MBG..... | 14 |
| 7.3 | System Configuration | 16 |
| 7.3.1 | Start application | 16 |
| 7.3.2 | Configure recording solution..... | 18 |
| 7.3.2.1 | Configure recording solution All-in-one Basic..... | 18 |
| 7.3.3 | Configure Recording Content Validation | 78 |
| 7.3.4 | Configure PHONEapp for Mitel..... | 81 |
| 7.3.4.1 | Configure Servers module | 81 |
| 7.3.4.2 | Configure PHONEapp module..... | 82 |
| 7.3.4.3 | Configure PBX module | 91 |
| 7.3.4.4 | Configure Phones module | 92 |
| 7.3.4.5 | Configure Recording Planner module..... | 95 |
| 7.3.4.6 | Configure function keys on the Mitel phone..... | 96 |
| 7.4 | Configure Genesys T-Server (optional)..... | 99 |
| 7.4.1 | Configure IP address and port of the Genesys T-Server..... | 99 |
| 7.4.2 | Configure IP address and port of the Genesys Configuration Server..... | 100 |
| 7.4.3 | Configure switch instance in the Genesys Configuration Server..... | 101 |
| 7.4.4 | Create users for the Genesys Configuration Server..... | 101 |
| 8 | Troubleshooting | 103 |
| | List of figures | 104 |

| | |
|---------------------|-----|
| List of tables..... | 107 |
| Glossary | 108 |

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 5000 provides the functionality which is necessary for an active IP recording in connection with an Mitel MiVoice 5000 PBX.

The recording server and the PBX communicate via a direct CSTA link. The signaling provides the information about the conversation participants as well as other additional information and controls the streaming of the audio 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.

For the monitored end devices, the recording server receives the conversation data directly from the phones. 2 separate RTP data streams are sent for each recorded end device. Depending on the configuration of the PBX, these streams can also be encrypted. The respective key is provided via the CSTA link.

On one Mitel MiVoice 5000 system, recorded extensions can only benefit from or be monitored by one of following other applications:

- MiCollab
- MiContact Center Business and/or InAttend
- a third-party CSTA application

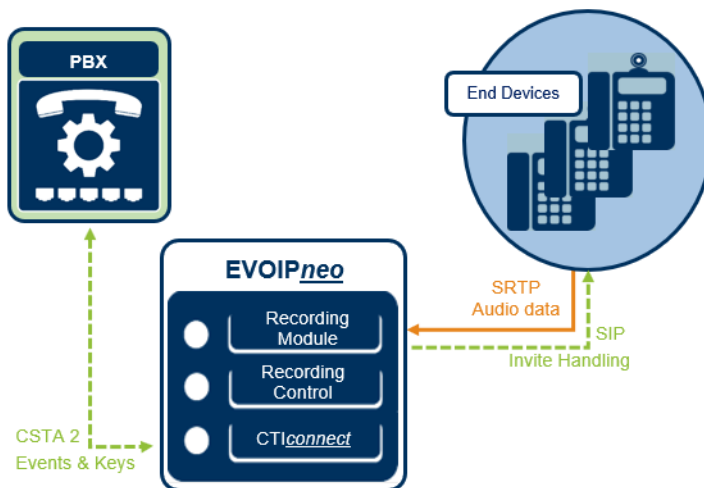


Fig. 1: Overview of the recording solution

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.

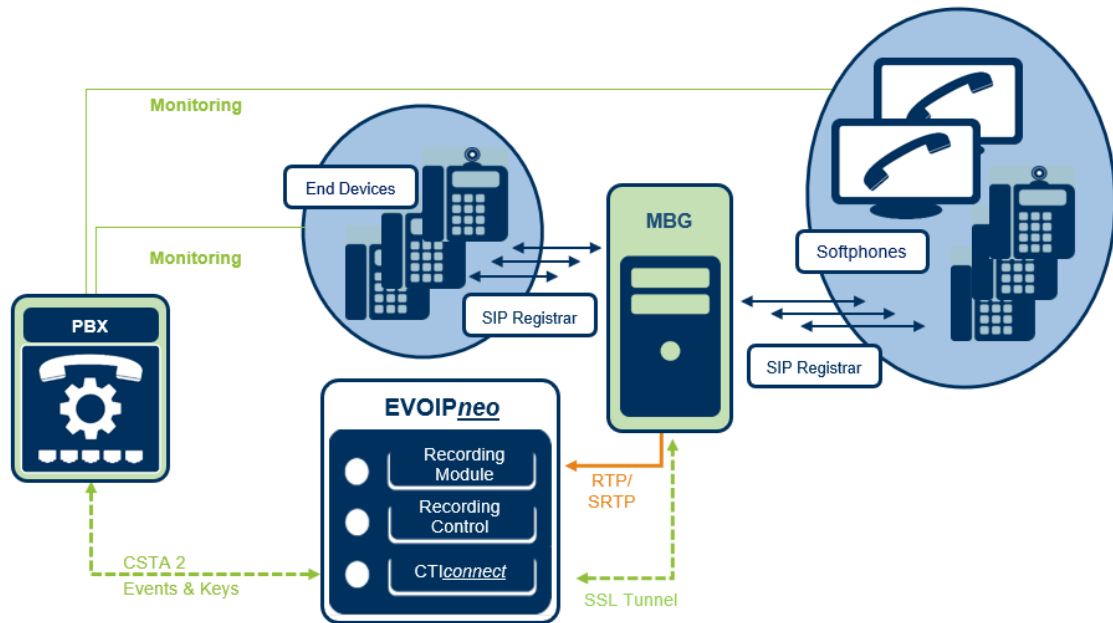


Fig. 2: Overview of the recording solution



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 5000 | 1 license per concurrent recording resource |

Tab. 1: Licenses

| 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

Mitel MiVoice CTI CSTA

| License name | Number |
|--------------|-----------------------------|
| CTI CSTA | 1 license per monitor point |

Tab. 3: Licenses

Licenses for recording via MiVoice Border Gateway

| License name | Number |
|-----------------|------------------------------------|
| MBG tap license | 1 license per concurrent recording |

Tab. 4: Licenses for recording via MiVoice Border Gateway



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

Licenses for the add-on Genesys T-Server (optional)

| License name | Number |
|---|------------------------------------|
| CTI ^{connect} for Genesys T-Server | 1 per recording system |
| Genesys Recording Connector | 1 per monitored recording resource |
| Genesys Universal SDK | 1 per recording server |

Tab. 5: Licenses for Genesys T-Server optional

MiContact Center Business (optional)

| License name | Number |
|---------------------------|--|
| MiContact Center Business | 1 basic package, contains licenses for 500 recording resources |

Tab. 6: Licenses for MiContact Center Business optional

4.2**Information**

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

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

5

Overview install and configure product

The following steps have to be carried out:

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:
Genesys T-Server
MiContact Center Business
 - 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

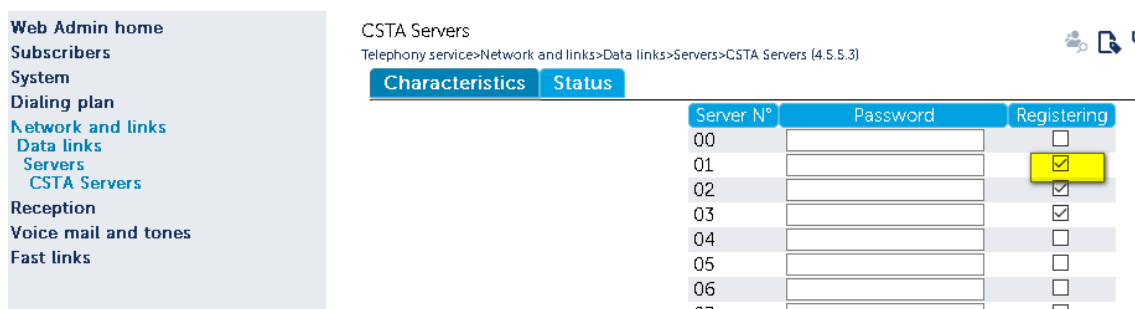
7.1 Configure Mitel MiVoice 5000



A Mitel engineer configures the Mitel MiVoice 5000 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.

The following information is an exemplary configuration:

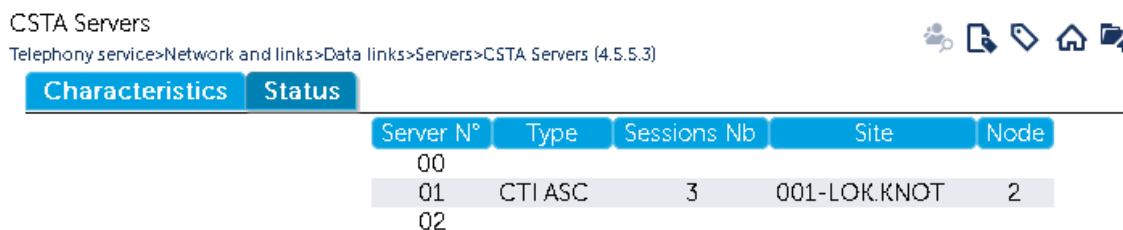
1. Select the menu item *Network and links > Data links > Servers > CSTA Servers*.
2. Activate the registering of the **CSTA** server in this section.



| Server N° | Password | Registering |
|-----------|----------|-------------------------------------|
| 00 | | <input type="checkbox"/> |
| 01 | | <input checked="" type="checkbox"/> |
| 02 | | <input checked="" type="checkbox"/> |
| 03 | | <input checked="" type="checkbox"/> |
| 04 | | <input type="checkbox"/> |
| 05 | | <input type="checkbox"/> |
| 06 | | <input type="checkbox"/> |
| 07 | | <input type="checkbox"/> |

Fig. 3: Mitel MiVoice 5000 - Configure registering

3. If the server has been connected, you can see the type and the location of the server in the tab *Status*.



| Server N° | Type | Sessions Nb | Site | Node |
|-----------|---------|-------------|--------------|------|
| 00 | | | | |
| 01 | CTI ASC | 3 | 001-LOK.KNOT | 2 |
| 02 | | | | |

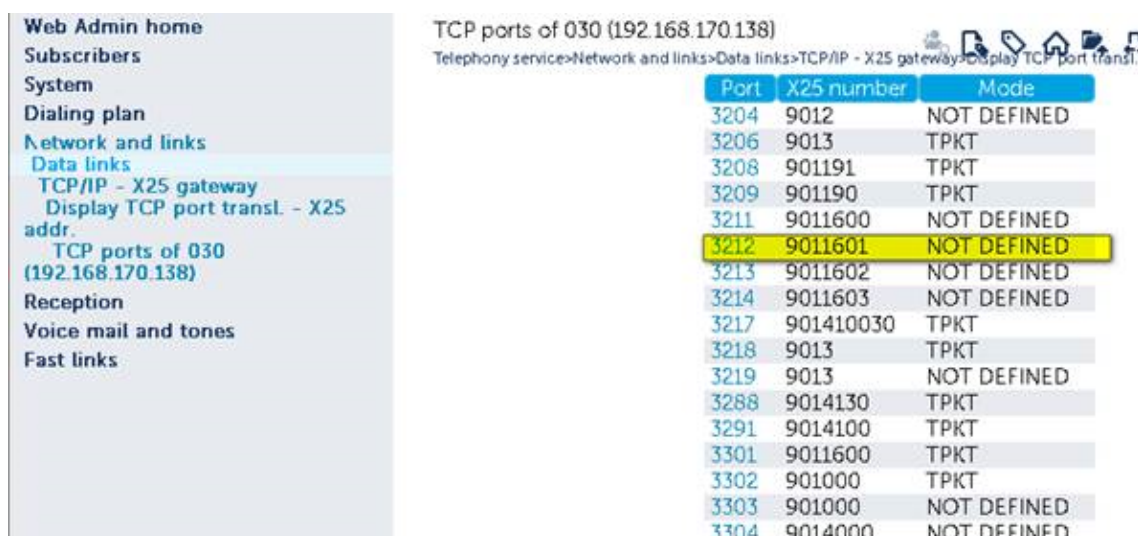
Fig. 4: Mitel MiVoice 5000 - Status of CSTA server

4. Under the menu item *Network and links > Data links > TCP/IP - X25 gateway*, you can configure the port and the number of the gateway.



Fig. 5: Mitel MiVoice 5000 - Configure gateway

In the table, you see the configured **CSTA** links.



Web Admin home
Subscribers
System
Dialing plan
Network and links
Data links
TCP/IP - X25 gateway
Display TCP port transl. - X25 addr.
TCP ports of 030 (192.168.170.138)
Reception
Voice mail and tones
Fast links

TCP ports of 030 (192.168.170.138)
Telephony service>Network and links>Data links>TCP/IP - X25 gateway>Display TCP port transl.

| Port | X25 number | Mode |
|------|------------|-------------|
| 3204 | 9012 | NOT DEFINED |
| 3206 | 9013 | TPKT |
| 3208 | 901191 | TPKT |
| 3209 | 901190 | TPKT |
| 3211 | 9011600 | NOT DEFINED |
| 3212 | 9011601 | NOT DEFINED |
| 3213 | 9011602 | NOT DEFINED |
| 3214 | 9011603 | NOT DEFINED |
| 3217 | 901410030 | TPKT |
| 3218 | 9013 | TPKT |
| 3219 | 9013 | NOT DEFINED |
| 3288 | 9014130 | TPKT |
| 3291 | 9014100 | TPKT |
| 3301 | 9011600 | TPKT |
| 3302 | 901000 | TPKT |
| 3303 | 901000 | NOT DEFINED |
| 3304 | 9014000 | NOT DEFINED |

Fig. 6: Mitel MiVoice 5000 - configured CSTA link

7.2 Configure MiVoice Border Gateway

7.2.1 Confirm certificate on MBG

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



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

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

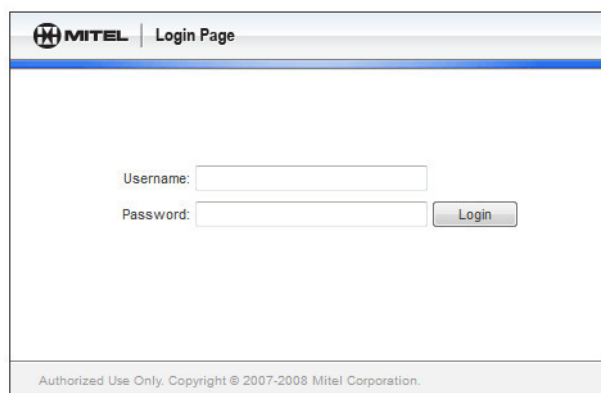
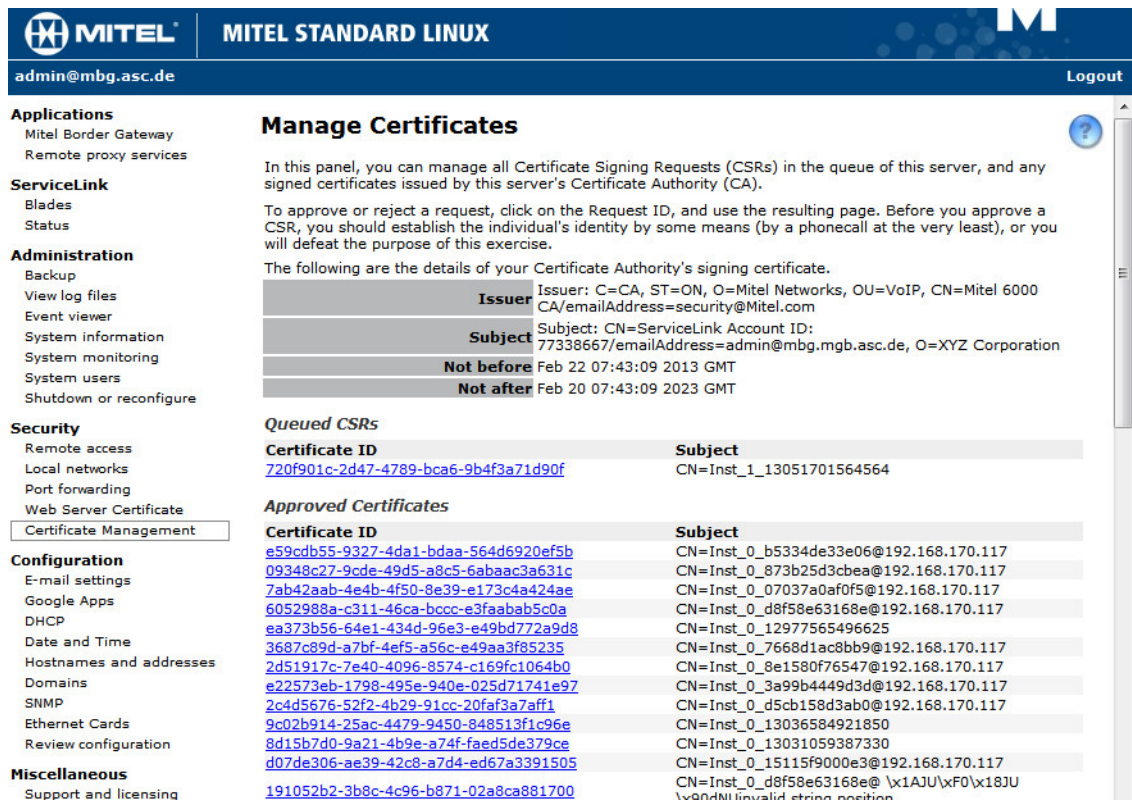


Fig. 7: Login screen MBG

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



MITEL STANDARD LINUX

admin@mbg.asc.de Logout

Applications
 Mitel Border Gateway
 Remote proxy services

ServiceLink
 Blades
 Status

Administration
 Backup
 View log files
 Event viewer
 System information
 System monitoring
 System users
 Shutdown or reconfigure

Security
 Remote access
 Local networks
 Port forwarding
 Web Server Certificate
Certificate Management

Configuration
 E-mail settings
 Google Apps
 DHCP
 Date and Time
 Hostnames and addresses
 Domains
 SNMP
 Ethernet Cards
 Review configuration

Miscellaneous
 Support and licensing

Manage Certificates

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

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

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

| Field | Value |
|-------------------|---|
| 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

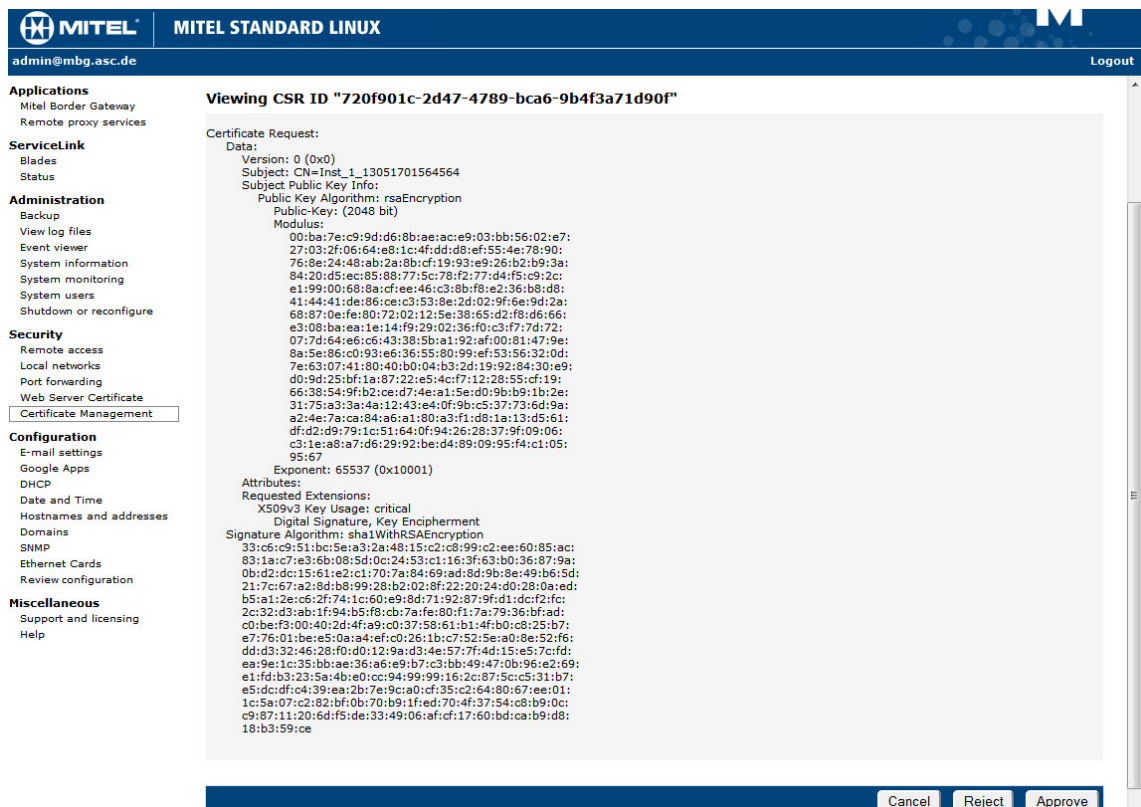
| Certificate ID | Subject |
|--|--------------------------|
| 720f901c-2d47-4789-bca6-9b4f3a71d90f | CN=Inst_1_13051701564564 |

Approved Certificates

| Certificate ID | Subject |
|--|--|
| e59cdb55-9327-4da1-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@192.168.170.117 |

Fig. 8: Certificate Management

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



MITEL STANDARD LINUX

admin@mbg.asc.de Logout

Applications
 Mitel Border Gateway
 Remote proxy services

ServiceLink
 Blades
 Status

Administration
 Backup
 View log files
 Event viewer
 System information
 System monitoring
 System users
 Shutdown or reconfigure

Security
 Remote access
 Local networks
 Port forwarding
 Web Server Certificate
Certificate Management

Configuration
 E-mail settings
 Google Apps
 DHCP
 Date and Time
 Hostnames and addresses
 Domains
 SNMP
 Ethernet Cards
 Review configuration

Miscellaneous
 Support and licensing
 Help

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

Certificate Request:

Data:

Version: 0 (0x0)

Subject: CN=Inst_1_13051701564564

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public Key: (2048 bit)

Modulus:

```
00:ba:7e:c9:9d:d6:8b:ae:ac:e9:03:bb:56:02:e7:
27:03:2f:06:64:e8:1c:4f:dd:d8:ef:55:4e:78:90:
76:8e:24:48:ab:2a:8b:cf:19:93:e9:26:b2:b9:3a:
84:20:d5:ec:85:88:77:5c:78:f2:77:d4:f5:c9:2c:
e1:99:00:68:8a:cf:ee:46:c3:8b:f8:e2:36:b8:d8:
41:44:41:de:86:ce:c3:53:8e:2d:02:9f:6e:9d:2a:
68:87:0e:fe:80:72:02:12:5e:38:65:d2:f8:6d:66:
e3:08:ba:ea:1e:14:f9:29:02:36:f0:c3:f7:7d:72:
07:7d:64:e6:c6:43:38:5b:a1:92:af:00:81:47:9e:
8a:5e:86:c0:93:a6:36:55:80:99:ef:53:56:32:0d:
7e:63:07:41:80:40:b0:04:b3:2d:19:92:84:30:e9:
d0:9d:25:bf:1a:87:22:e5:4c:f7:12:28:55:cf:19:
66:38:54:9f:b2:ce:d7:4e:a1:5e:d0:9b:b9:1b:2e:
31:75:a3:3e:4a:12:43:e4:0f:9b:c5:37:73:6d:9a:
a2:4e:7a:ca:84:a6:a1:80:a3:f1:d8:1a:13:d5:61:
d7:d2:d9:79:1c:51:64:0f:94:26:28:37:9f:09:06:
c3:1e:a8:a7:d6:29:92:be:d4:89:09:95:f4:c1:05:
95:67
```

Exponent: 65537 (0x10001)

Attributes:

Requested Extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

Signature Algorithm: sha1WithRSAEncryption

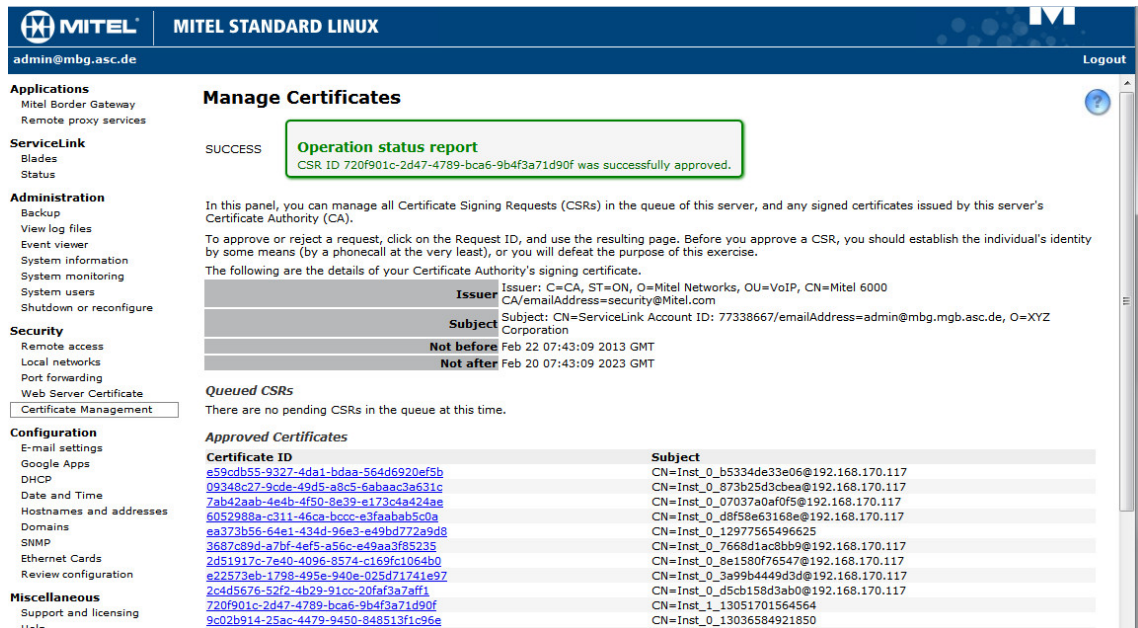
```
33:c6:c9:51:bc:5e:a3:2a:48:15:c2:c8:99:c2:ee:60:85:ac:
83:1a:c7:e3:6b:08:5d:0c:24:53:c1:16:3f:63:b0:36:87:9a:
0b:d2:dc:15:61:e2:c1:70:7a:84:69:ad:8b:9b:8e:49:b6:5d:
21:7c:67:a2:8d:b8:99:28:b2:02:8f:22:20:24:d0:28:0a:ed:
b5:a1:2e:c6:2f:74:1c:60:e9:8d:71:92:87:9f:d1:dc:2f:fc:
2c:32:d3:ab:1f:94:b5:f8:cb:7a:fe:80:f1:7a:79:36:bf:ad: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

Cancel Reject Approve

Fig. 9: Confirm selected certificate

5. Click on the button *Approve*.

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



The screenshot shows the MITEL STANDARD LINUX web interface. The left sidebar contains navigation links for Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled "Manage Certificates" and displays a "SUCCESS" message with a green box containing the text: "Operation status report: CSR ID 720f901c-2d47-4789-bca6-9b4f3a71d90f was successfully approved." Below this, there is a section for "Queued CSRs" (showing none) and a table of "Approved Certificates".

| Certificate ID | Subject |
|---------------------------------------|--|
| e59cd855-9327-4da1-bdaa-564d6920ef5b | CN=Inst_0_b5334de33e06@192.168.170.117 |
| 09348e27-9a0de-49d5-a8c5-6a0aac3a531c | CN=Inst_0_873b25d3cbea@192.168.170.117 |
| 7ab42aab-4e4b-4f50-8a39-e173c4a4249a | 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 |
| 720f901c-2d47-4789-bca6-9b4f3a71d90f | CN=Inst_1_13051701564564 |
| 9c02b914-25ac-4479-9450-848513f1c96e | CN=Inst_0_13036584921850 |

Fig. 10: 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.

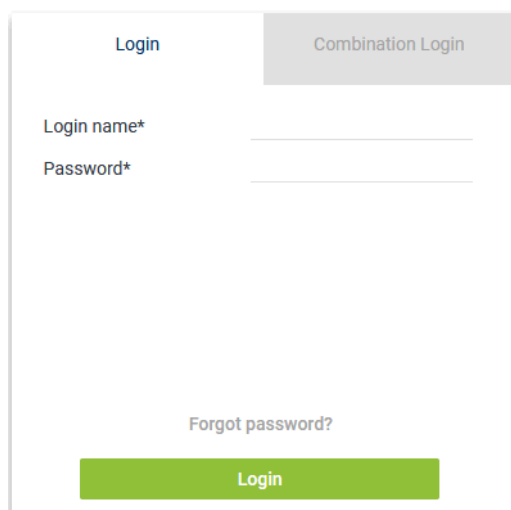
1. To start the application directly on the server, double-click on the shortcut System Configuration.

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.



The login form has two tabs: 'Login' (active) and 'Combination Login'. Under the 'Login' tab, there are two input fields: 'Login name*' and 'Password*'. Below these fields is a link 'Forgot password?'. At the bottom is a green 'Login' button.

Fig. 11: System Configuration - Web interface

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

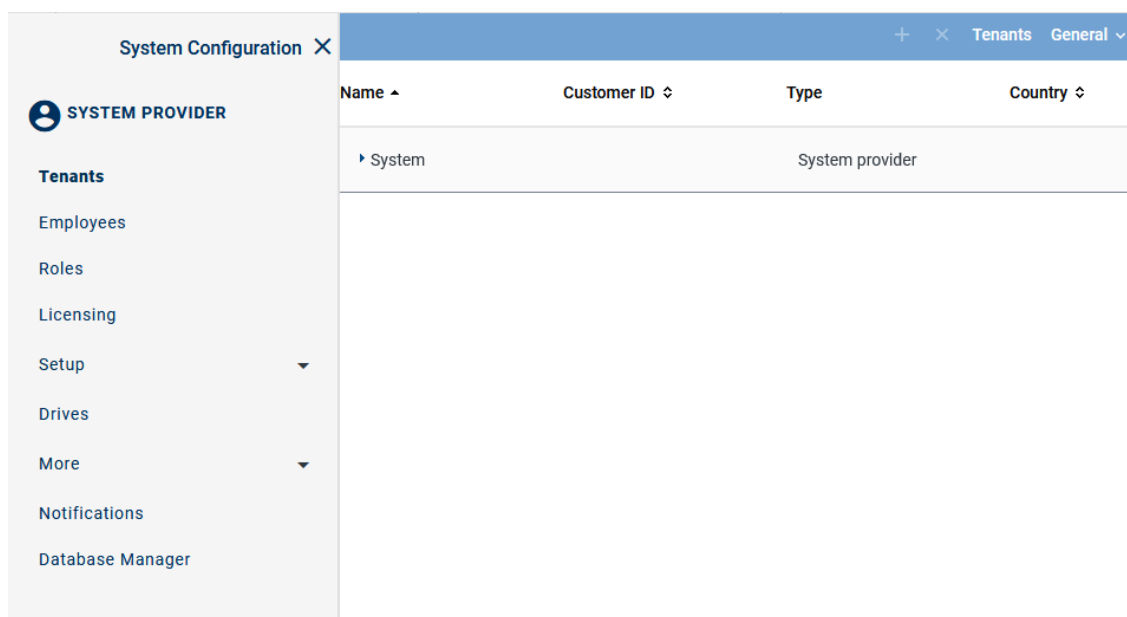
Login data for the administrator of the system provider:

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

Tab. 7: Login data - system provider

2. Log in to the web interface.

⇒ The main window System Configuration appears.



The main view of the System Configuration window. It features a sidebar on the left with a 'SYSTEM PROVIDER' icon and a list of menu items: Tenants, Employees, Roles, Licensing, Setup (with a dropdown arrow), Drives, More (with a dropdown arrow), Notifications, and Database Manager. The main area on the right has a blue header with '+', '×', 'Tenants', and 'General' (with a dropdown arrow). Below the header is a table with columns: Name ▲, Customer ID ⇅, Type, and Country ⇅. The table contains one entry: 'System' with type 'System provider'.

Fig. 12: System Configuration - main view

7.3.2 Configure recording solution

Supported recording architectures

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

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

7.3.2.1 Configure recording solution All-in-one Basic

7.3.2.1.1 Create recording architecture

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

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

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

⇒ The following window appears:

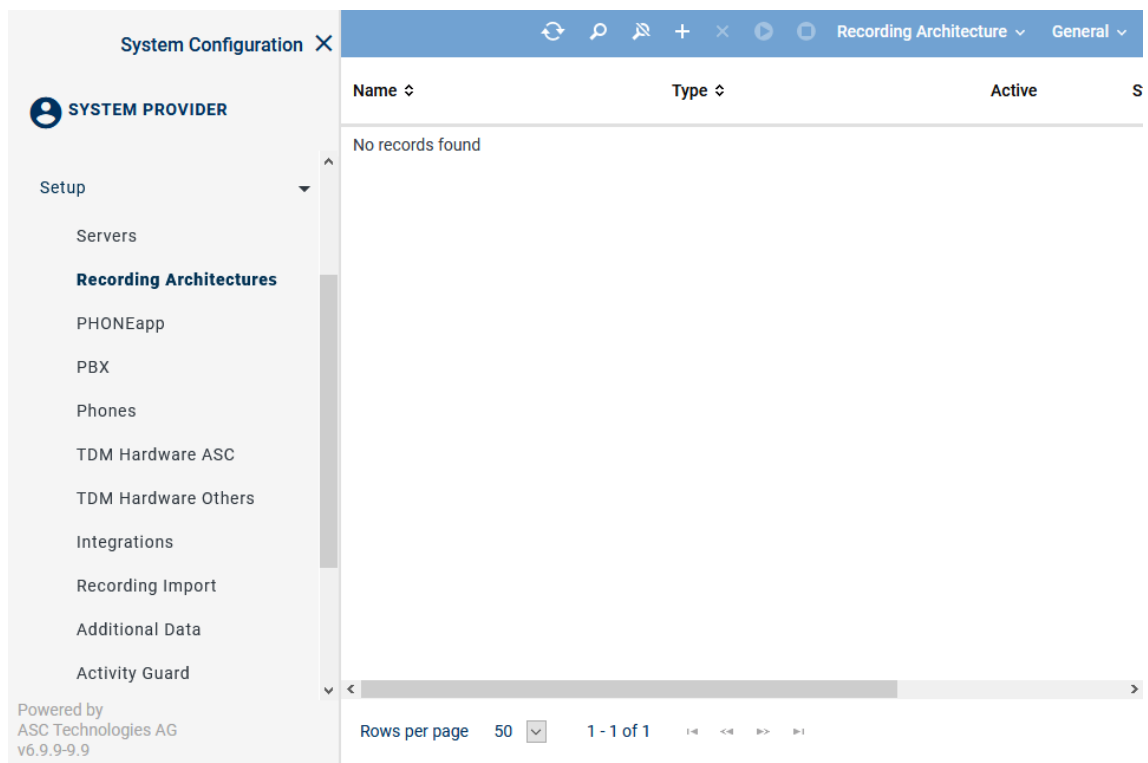




Fig. 13: Recording architectures - main view

| | |
|---------------|--|
| Name | Name of the recording architecture |
| Type | Type of the recording architecture |
| Active | Shows whether the recording architecture has been activated and is ready to be used for the recording. <div> ✓ = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar. ✗ = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar. </div> |

| | |
|-----------------------|--|
| <i>Standby Active</i> | Shows whether the standby server is active for one or several recording components in the recording architecture. <div> ✓ = At least 1 standby server is active. ✗ = No standby server is active or no standby server has been defined. </div> |
| <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. 14: Toolbar Recording Architectures module


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

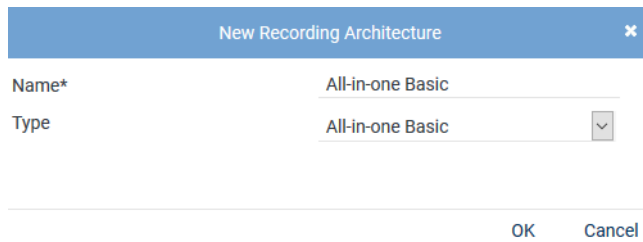


Fig. 15: Create recording architecture - All-in-one Basic Recording

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

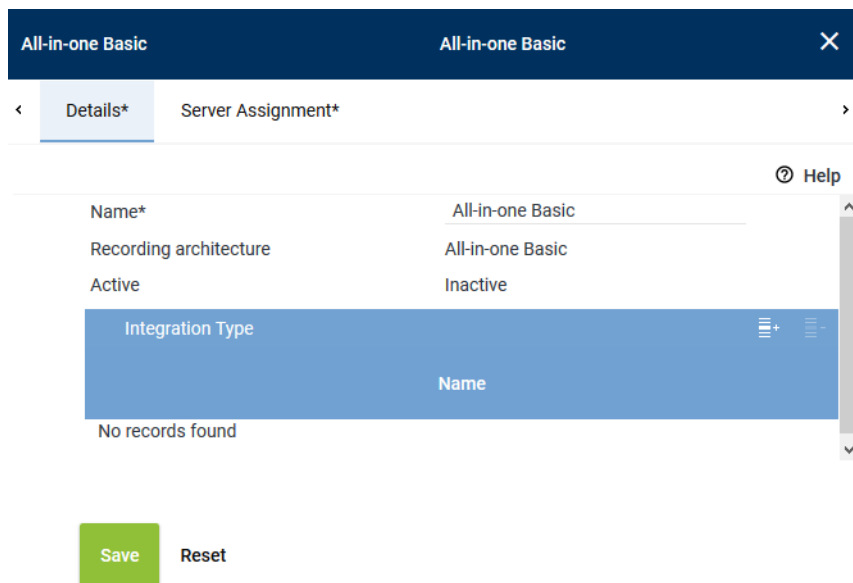



Fig. 16: Recording architecture - tab Details

Add integration type

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

Integration Type

×

Name

Mitel MiVoice 5000 active

Add

Cancel

Fig. 17: 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 5000* from the list of the available integration types and click on the button *Add*.
⇒ The name of the integration type now appears in the list in the detail view.

Assign server for All-in-one Basic

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

×

Details*

Server Assignment*

Server*

REC-01

+

-

Used in activated architecture

No

Recording type

☐ VoIP/Video
☐ TDM
☐ Screen
☐ Chat

Save

Reset

Fig. 18: Recording architecture - tab Server Assignment

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

| Servers | | | × |
|---------|-----------------|--------|---|
| | | | <div style="display: flex; gap: 5px;"> <div>📄</div> <div>📊</div> </div> |
| Name ↕ | IP Address ↕ | Path ↕ | |
| REC-01 | 192.168.173.171 | C:\ | |

Rows per page 20 ▼
 1 - 8 of 8

⏪
<<
>>
⏩

Add

Cancel

Fig. 19: Recording architecture - assign server

3. Select the respective server.



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

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

Recording type

☒ VoIP/Video

☐ TDM

☐ Screen

☐ Chat




Save Reset

Fig. 20: 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. 21: 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:

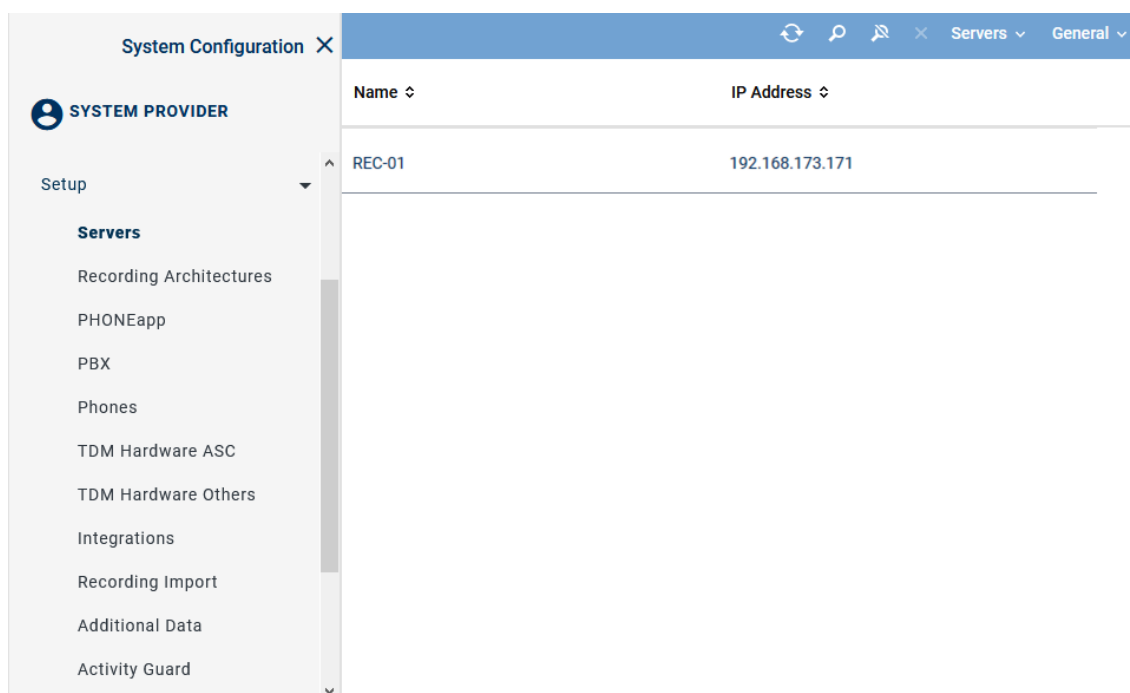


Fig. 22: Servers - main view

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

| | |
|----------------------|---|
| <i>Name</i> | Name of the server. |
| <i>IP address</i> | IP address of the server. |
| <i>Creation Date</i> | Date on which the server was configured. |
| <i>Updated</i> | Date on which the settings for 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. 23: 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. 25. |
| | <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.

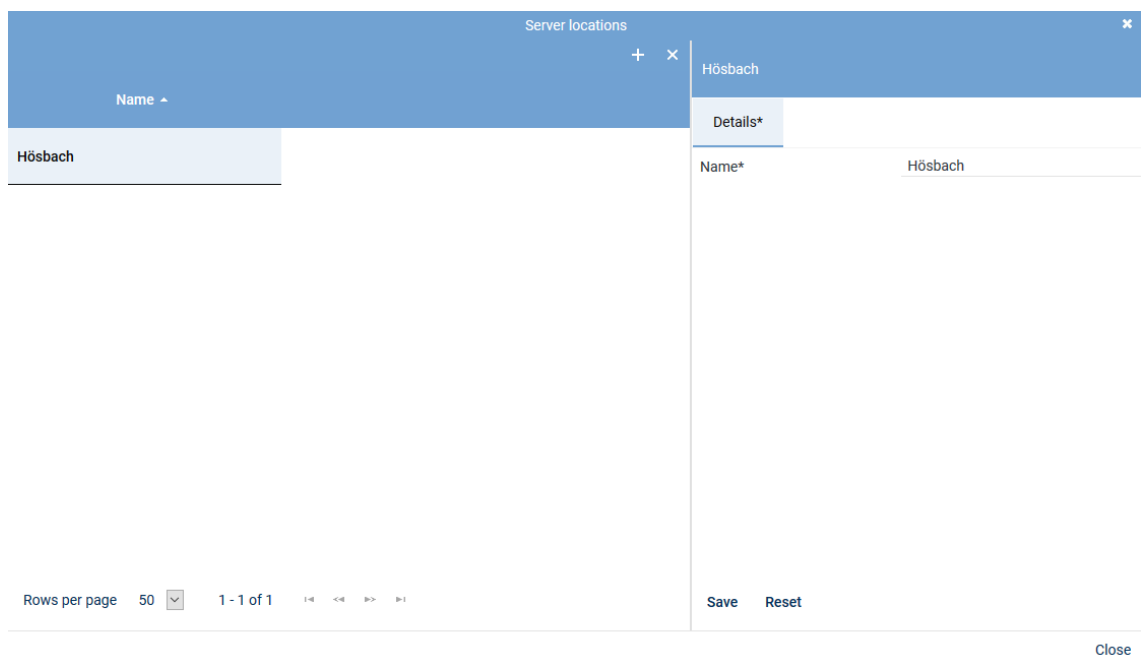



Fig. 24: Add server locations

- 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.

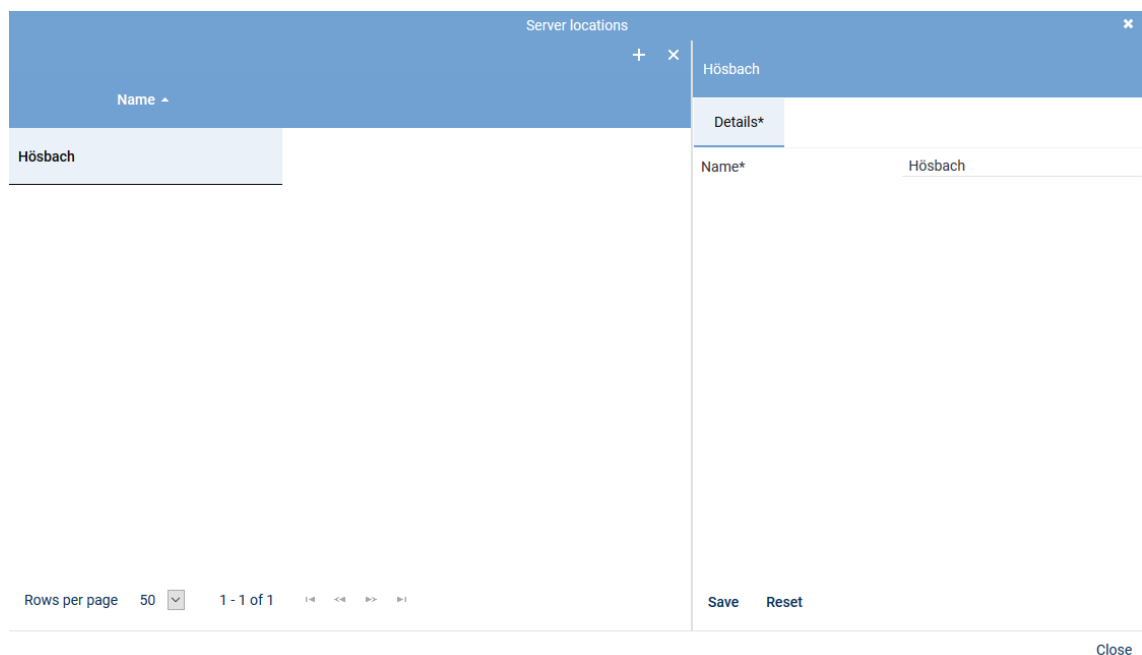



Fig. 25: Delete server location

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. 26: 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. 27: Servers - tab usage

Group field API Server

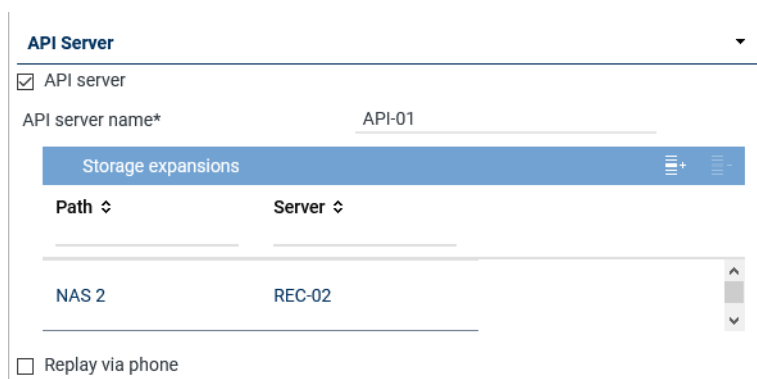




Fig. 28: Group field API Server

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. 38.</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. 29. 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. 36. 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. 29: 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. 30: 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. 8: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

Rows per page 20 ▾ 1 - 8 of 8 ⏪ ⏩ ⏴ ⏵

Add **Cancel**

Fig. 31: 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. 32: 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. 9: Configure recording control/key management

Group field Data Processing

Data Processing ▼

☒ Data storage

☐ Transfer data for replay

Target Server

| Name | IP Address ↕ |
|------------------|--------------|
| No records found | |

☒ Transfer data for data storage

Target Server

| Name | IP Address ↕ |
|------------------|--------------|
| No records found | |

Activate period of time ☒

Start

End

Receives data from

| Name | Only Replay |
|------------------|-------------|
| No records found | |

☐ Archiving

☒ Export







Replay server

☒ Import

Recording architecture

Fig. 33: 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. 33. 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. 33. 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*

replay1

WebSocket port*
(max. 5 characters)

4040

API server*


+


-

Name

Connection Status

Fig. 35: 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. 35. |

| 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. 11: Configure replay


Search and replay functions



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

Add API server to a list

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

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

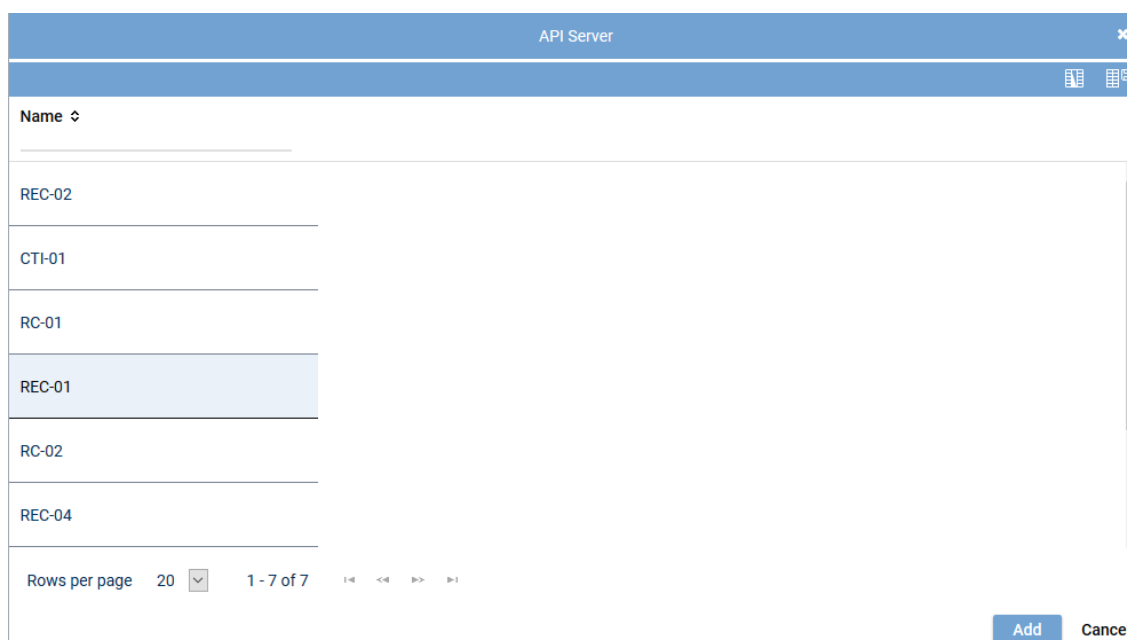


Fig. 36: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 28](#).

- 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. 37: 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. 12: 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. 38: 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 UDP = unencrypted TLS = encrypted</p> <p>If an external analog gateway has been integrated, select UDP in the drop-down list.</p> |
| <i>SIP signaling port</i> | <p>Enter the port for the SIP communication.</p> <p>Port for data exchange: 5062</p> |
| <i>User name</i> | Enter the user name for the authentication on the SIP server. |
| <i>Password</i> | Enter the password for the authentication on the SIP server. |
| <i>PBX IP address</i> | 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*.

<
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. 39: 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. 40: 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*

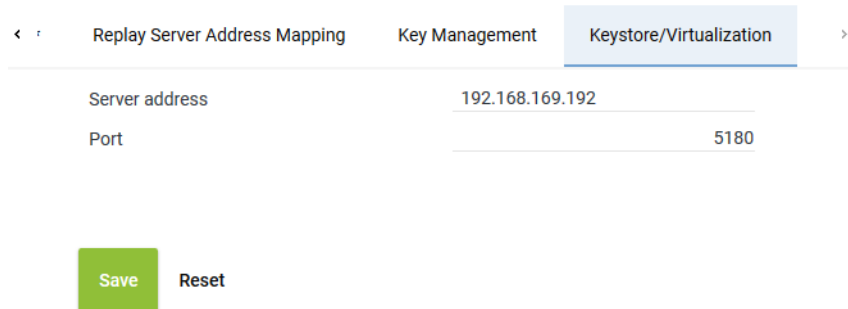
Alternatively, you can install a *Trusted Virtualization License* to authenticate licensing; you do not require Internet access for this.

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. 41: 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:

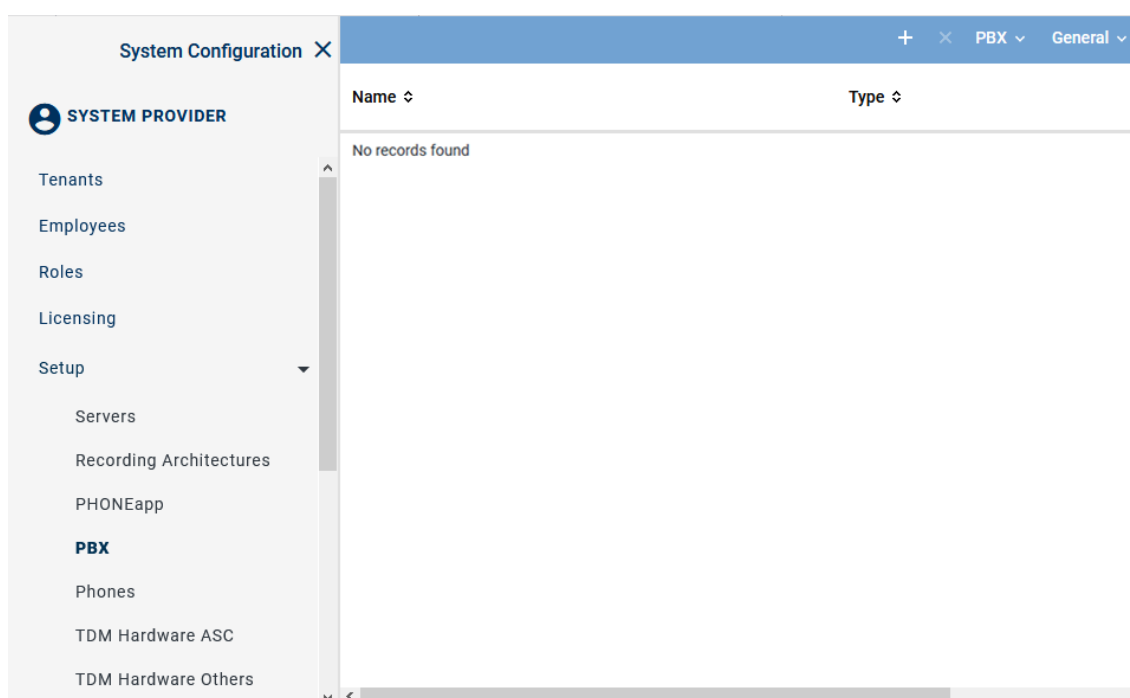




Fig. 42: PBX module - main view

Toolbar of the PBX module

The toolbar offers the following functions.




Fig. 43: Toolbar PBX module

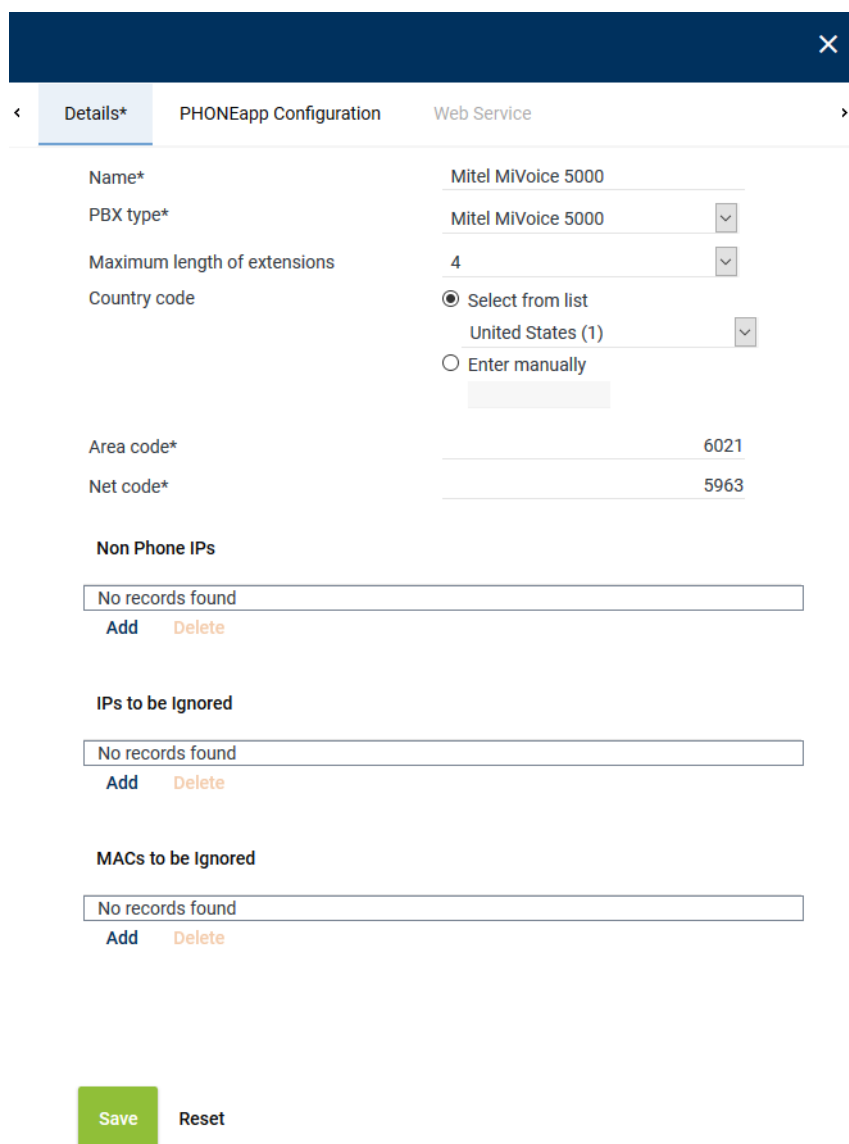
| | | |
|---|---------------------------------------|--|
|  | <i>Create</i> | In the detail view, you can enter the parameters of the new PBX. |
|  | <i>Delete</i> | Deletes the selected PBX configuration. A PBX can only be deleted if it is not used in any configuration. |
| <i>PBX</i> | <i>Phone Configuration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

- 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 5000

PBX type* Mitel MiVoice 5000

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. 44: 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. 13: 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.

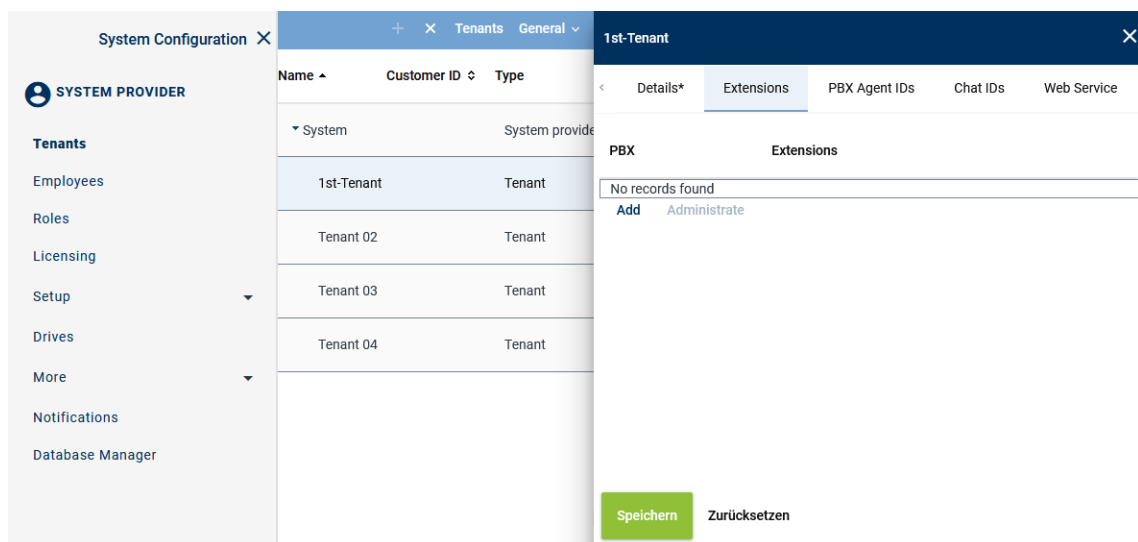


Fig. 45: Tenants - main view - tab Extensions

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. 46: 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 5000 - Neo 7.x Rev. 5

46 / 109

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.

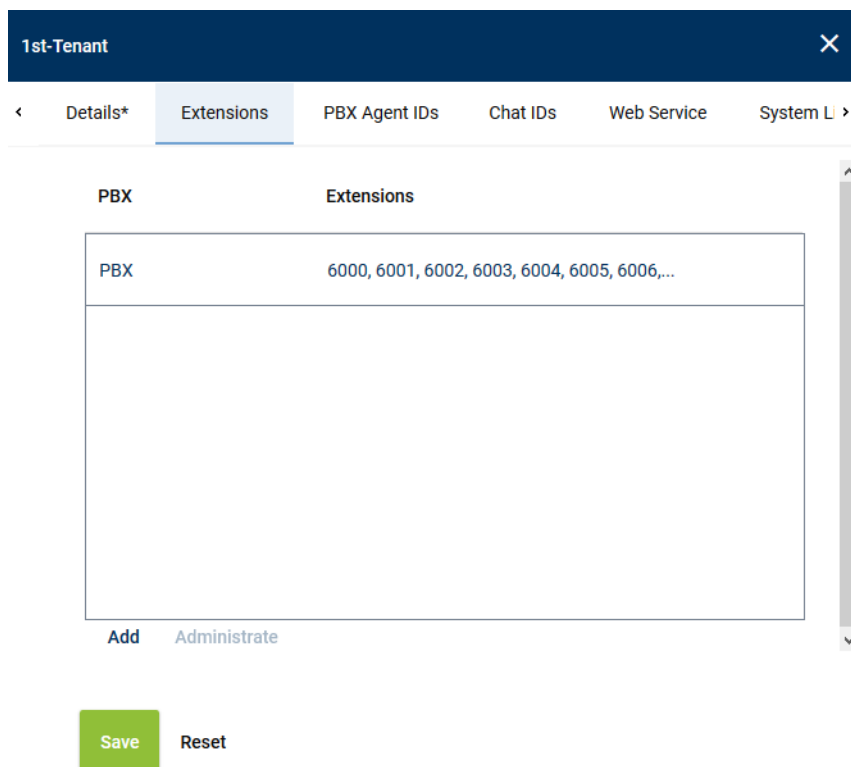


Fig. 47: Remove extensions

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. 48: 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.

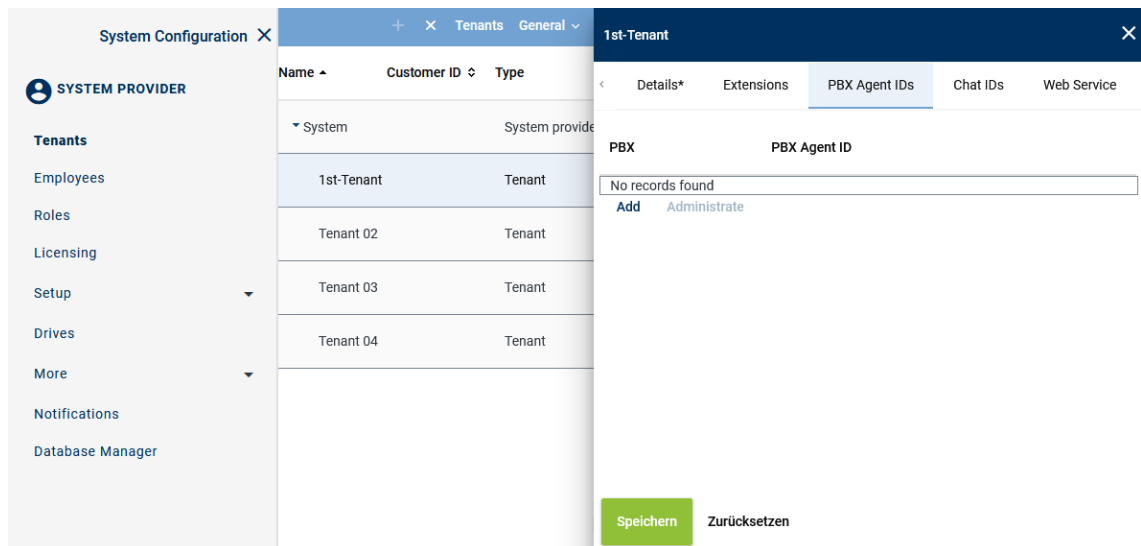
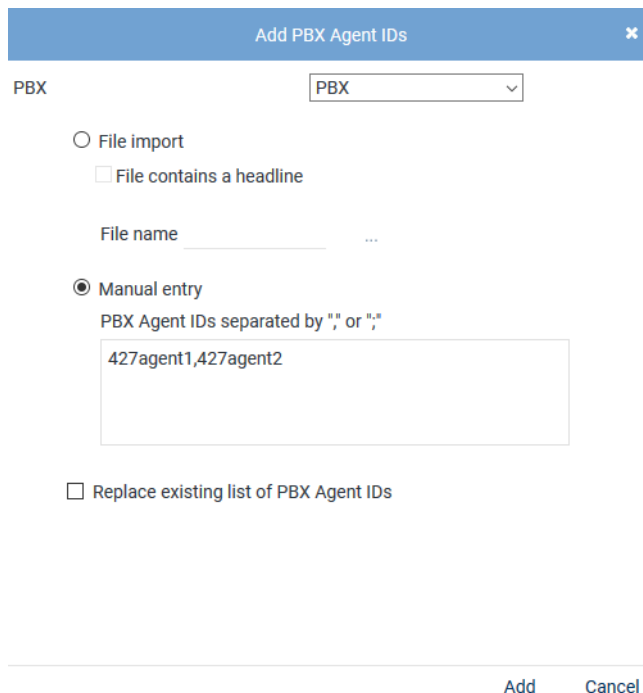


Fig. 49: Tenants - main view - tab PBX Agent ID

Add PBX Agent ID

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

⇒ The following window appears:



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

Fig. 50: 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.

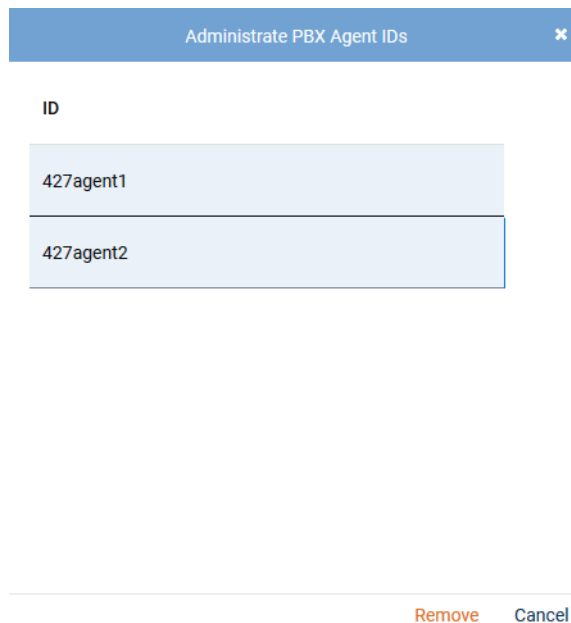


Fig. 51: Select PBX Agent IDs

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 be used in the Recording Planner for instance to control recording behavior. The additional data can be displayed in the search and replay applications, too.

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. 52: 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 | Displayed Name | |
| ar_SA | customCP01 | ✎ |
| bg_BG | customCP01 | ✎ |
| cs_CZ | customCP01 | ✎ |
| de_DE | customCP01 | ✎ |
| en_GB | customCP01 | ✎ |
| en_US | <input type="text" value="customCP01"/> | ✓ ✕ |

Fig. 53: Configure additional data

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

Availability

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

Save
Reset

Fig. 54: 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:

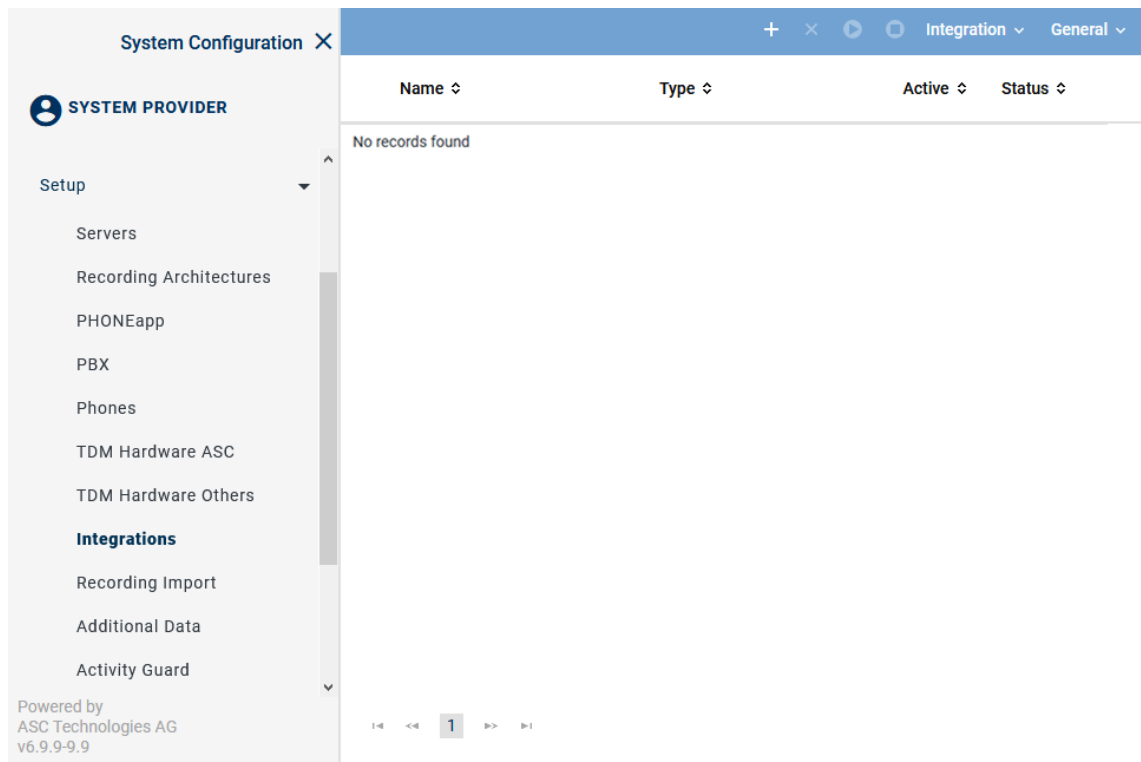




Fig. 55: Integrations - main view

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. 56: 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.

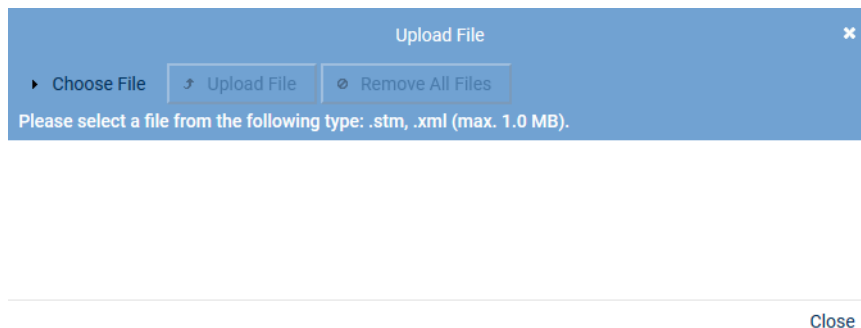


Fig. 57: Choose file

- 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*.

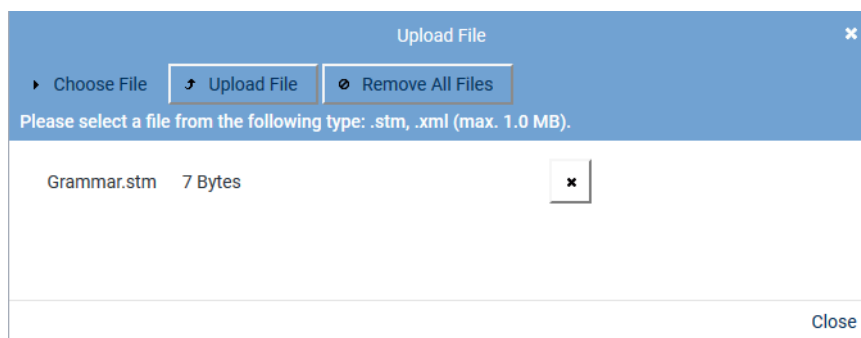




Fig. 58: Upload grammar

- 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.

New Integration

Integrationstyp Aufzeichnungsarchitektur

Name* Mitel MiVoice 5000


Integration type* Mitel MiVoice 5000 active

PBX +

PBX* Mitel MiVoice 5000 + -

Cancel Back Next

Fig. 59: Create integration type

2. Enter the following parameters:
3. To assign the PBX, click on the button  behind the field *PBX*.
⇒ The window *PBX* appears.

PBX

| Name ↕ | Type ↕ |
|--------------------|--------------------|
| Mitel MiVoice 5000 | Mitel MiVoice 5000 |

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 60: Integrations - select PBX

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

Assign recording architecture for All-in-one Basic

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



New Integration

Integration Type Recording Architecture

Recording Architecture

Recording architecture* All-in-one Basic

Save Cancel Back Next

Fig. 61: 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 5000 | | Mitel MiVoice 5000 active | ✗ | ✓ |
|----------------------------------|---------------|---------------------------|---|---|
| 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. 62: 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.

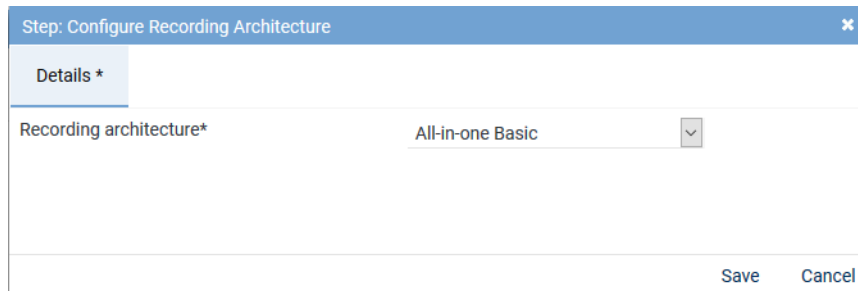



Fig. 63: Configuration step - Configure Recording Architecture

- 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 5000

In this tab, you can configure the CTI~~connect~~ module for the recording variant via Mitel MiVoice 5000.

Step: Configure CTI Connection Data

MiVoice 5000 (CSTA)*
MBG

CTIconnect Module

TypeCTIconnect active
Grammar name*standard
Grammar version*2.00.02

Connection Data

Additional Data

SaveCancel

Fig. 64: CTI connection data - tab MiVoice 5000 (CSTA)

Group field CTIconnect Module

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

CTIconnect Module

TypeCTIconnect active
Grammar name*standard
Grammar version*2.00.04

Fig. 65: 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. 14: Configure CTIconnect module

Group field Connection Data

In this group field, you can enter the link to the CTIconnect module of the recording server.

Connection Data

Connection data

No records found

AddEditDelete

Fig. 66: Group field Connection Data

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

⇒ The following window appears:



Fig. 67: Configure connection data

2. Enter the following parameters:

| Parameter | Value/Description |
|-----------------|--|
| Connection data | Enter the IP address of the PBX. |
| PBX port | Enter the port for the PBX connection. |

Tab. 15: Configure connection data



Until version 7.1, the PBX Mitel MiVoice 5000 does not support more than 2 [CSTA](#) links.

3. Click on the button *Add* to apply the entries and to close the window.

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.

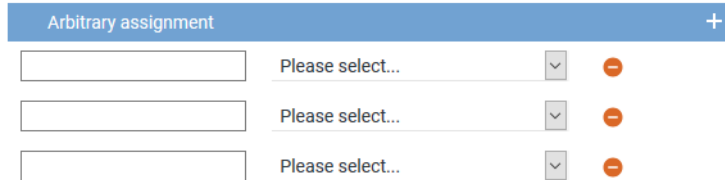


Fig. 68: Group field Additional Data - free assignment of additional data

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.

Tab MBG

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

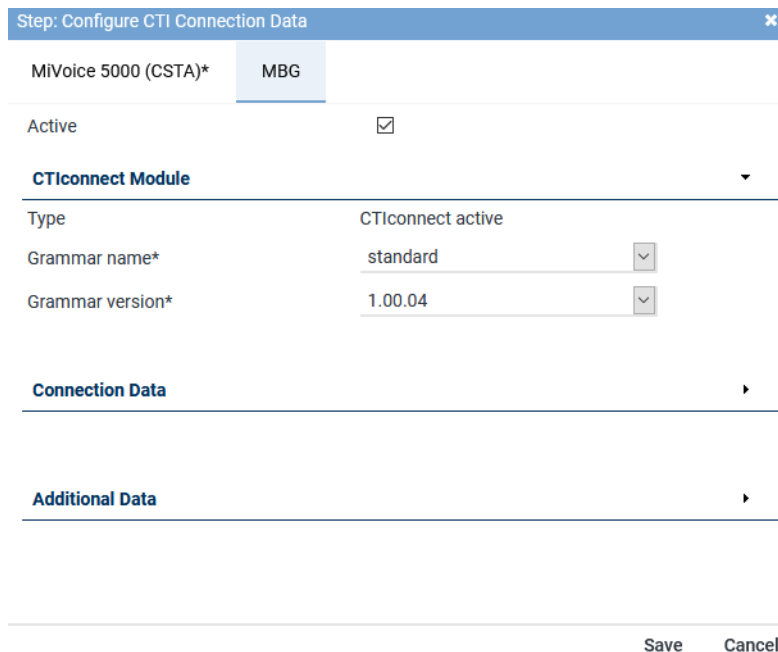


Fig. 69: Configure CTIconnect connection data to **MBG**



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* | 2.00.04 |

Fig. 70: 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. 16: Configure CTIconnect module

Group field Connection Data

In this group field, you can enter the link to the CTIconnect module of the recording server.

| Connection Data |
|---|
| Connection data |
| No records found |
| Add Edit Delete |

Fig. 71: Group field Connection Data

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

Configure Connection
✕

| | |
|------------------|-----------------|
| Connection data* | 192.168.170.227 |
| PBX port* | 3211 |

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

Fig. 72: Configure connection data

2. Enter the following parameters:

| Parameter | Value/Description |
|------------------------|--|
| <i>Connection data</i> | Enter the IP address of the PBX. |
| <i>PBX port</i> | Enter the port for the PBX connection. |

Tab. 17: Configure connection data



Until version 7.1, the PBX Mitel MiVoice 5000 does not support more than 2 [CSTA](#) links.

3. Click on the button *Add* to apply the entries and to close the window.

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.

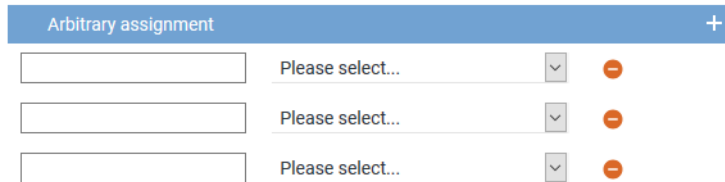



Fig. 73: Group field Additional Data - free assignment of additional data

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 monitor points

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

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

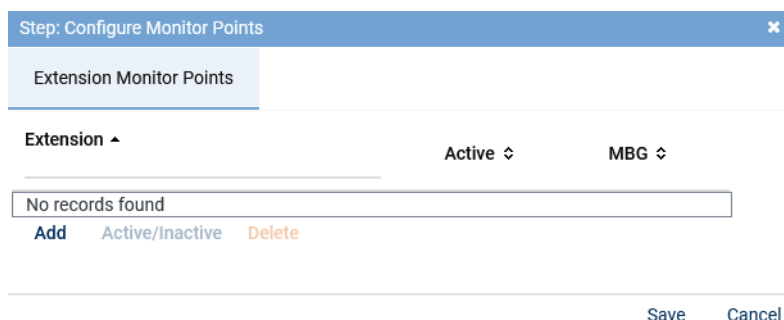


Fig. 74: Configuration step - configure monitor points

Configure tab Extension Monitor Points

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. 75: 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 ⇅ | MBG ⇅ |
| 6000 | ✓ | <input checked="" type="checkbox"/> |
| 6001 | ✓ | <input checked="" type="checkbox"/> |
| 6002 | ✓ | <input checked="" type="checkbox"/> |
| 6003 | ✓ | <input checked="" type="checkbox"/> |
| 6004 | ✓ | <input checked="" type="checkbox"/> |
| 6005 | ✓ | <input checked="" type="checkbox"/> |
| 6006 | ✓ | <input checked="" type="checkbox"/> |
| Add Active/Inactive Delete | | |
| Save Cancel | | |

Fig. 76: Configured extension monitor points

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

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

MBG To record extensions via the **MBG**, you must activate the check box for the corresponding extension in the column **MBG**.

☒ = Extension has been activated.


☐ = Extension has not been activated.



By activating the check box for recording via the **MBG**, the monitored participants are recorded exclusively via the **MBG**; recording via ACTIVE VoIP is not attempted. For participants logging in with a phone number to the **SIP** hardware phones which have not been registered on the **MBG**, the check box must not be activated.

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

Global recording settings

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

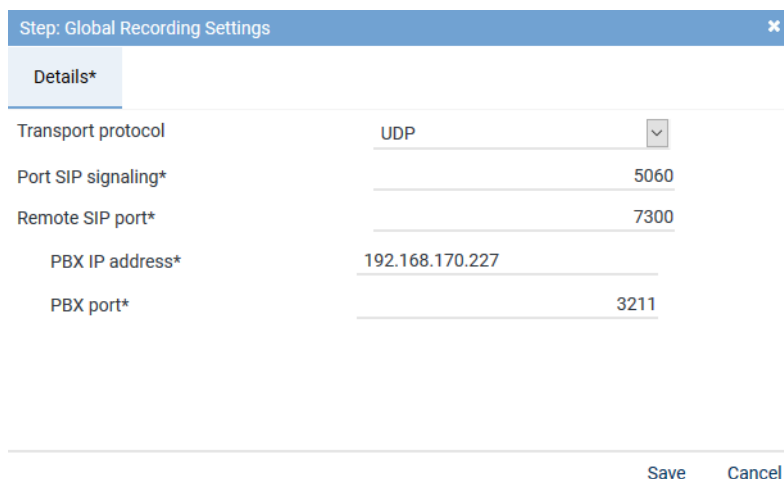


Fig. 77: Configuration step - Global Recording Settings


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

| Parameter | Value/Description |
|---------------------------|--|
| <i>Transport protocol</i> | Select the used protocol, e. g. <i>UDP</i> . |
| <i>Port SIP signaling</i> | Enter the port for the SIP signaling, where the signaling is received. The default value is <i>5060</i> . |
| <i>Remote SIP port</i> | Enter the port for the end devices, here <i>7300</i> . |
| <i>PBX IP address</i> | Enter the IP address for the connection to the PBX here. |
| <i>PBX port</i> | Enter the port for the connection to the PBX, here <i>3211</i> . |

Tab. 18: Global recording settings

3. Click on the button *Save* to finish the configuration in this step.

Configure recording servers

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

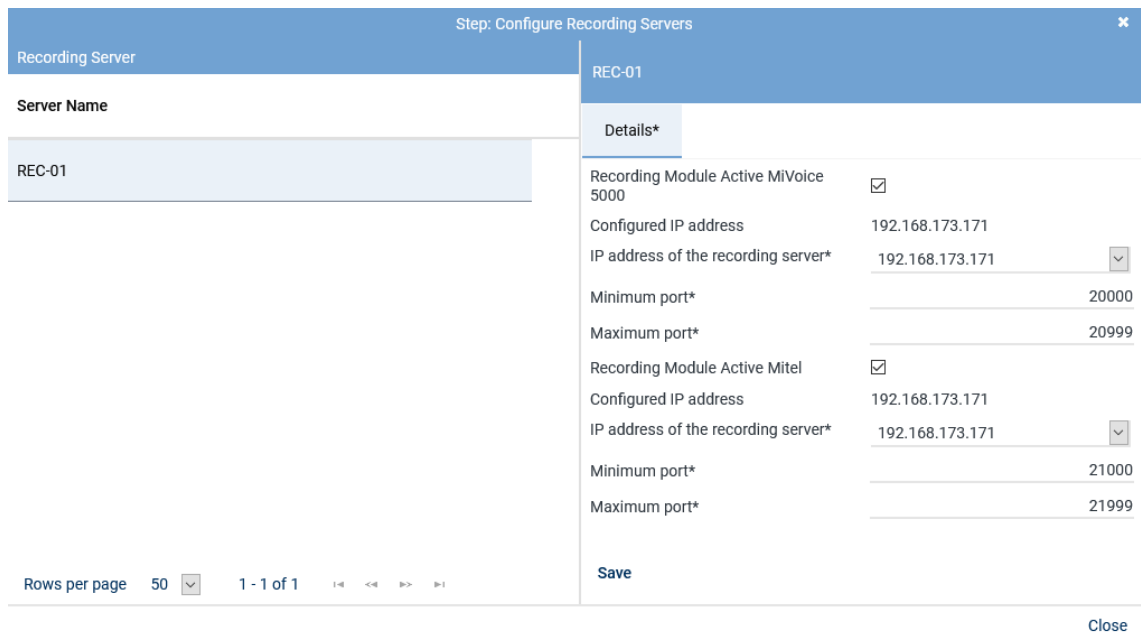


Fig. 78: Configuration step - Configure recording servers

For ACTIVE VoIP recording and recording by means of the **MBG**, you must activate both recording variants.

- Activate the two recording modules:

Recording Module Active MiVoice 5000

Recording Module Active Mitel

- For each module, select the IP address of the recording server from the drop-down list.
- For each recording variant, select a separate port range to receive the **RTP** data, e. g.

Recording Module Active MiVoice 5000

Port range 20000-20999

Recording Module Active Mitel

Port range 21000-21999



For stereo recording, reckon with 4 ports as only even ports are used to receive **RTP**.
In addition, stereo recording requires more storage space.



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.

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 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

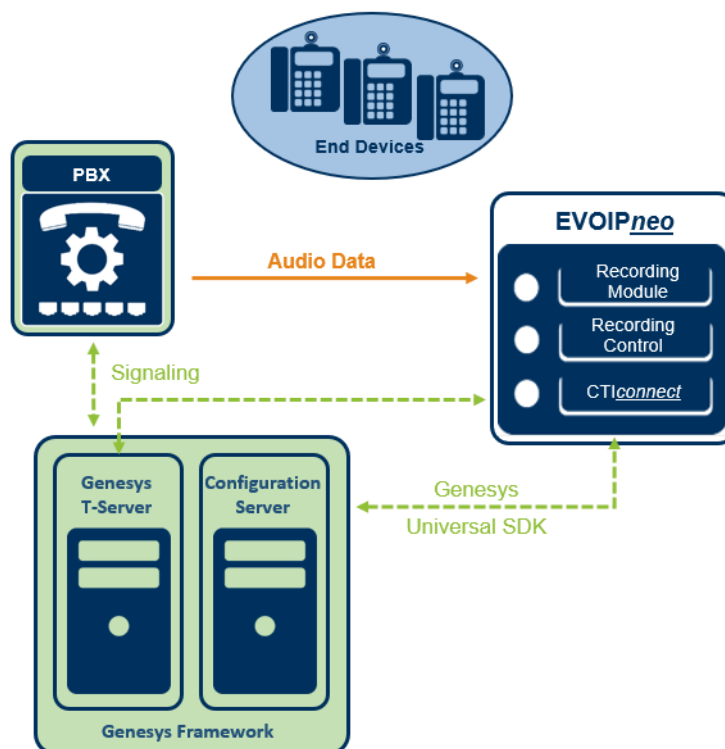


Fig. 79: Overview of the add on of Genesys T-Server



For further information about the configuration of Genesys T-Servers, see [chapter "Configure Genesys T-Server \(optional\)", p. 99](#).

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

Group field CTIconnect Module

- 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 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. 19: 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:

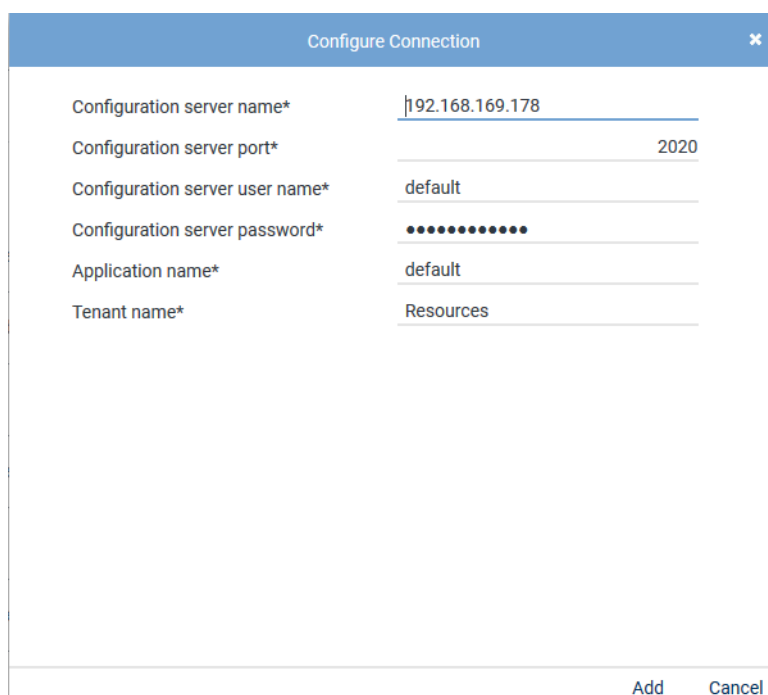


Fig. 81: Configure connection data

- 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. 20: 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.

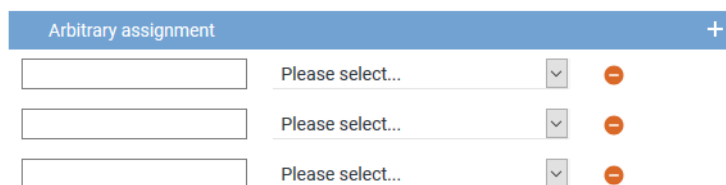



Fig. 82: Group field Additional Data - free assignment of additional data

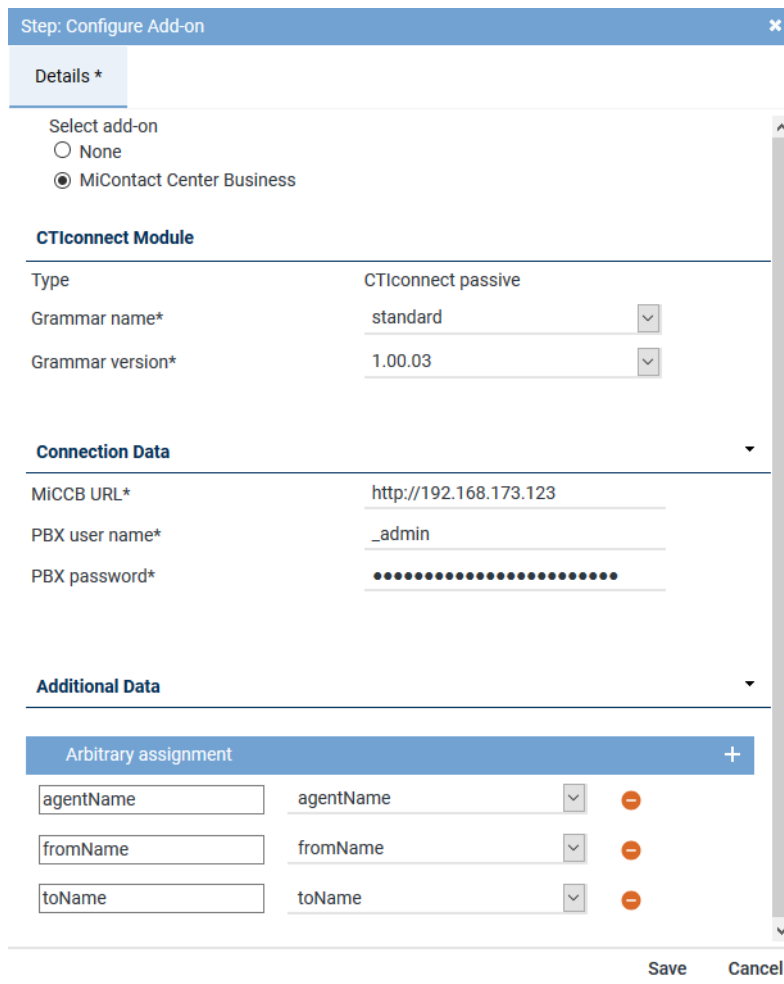
2. Enter the name of the additional data type from the protocol in the entry field on the left. Observe the exact spelling like it is used in the protocol. The information read out of the protocol is displayed in the columns in the players.
3. From the drop-down list, select the respective display name 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 MiContact Center Business

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

The integration runs in combination with the PBX and the recording server which is responsible for the actual conversation recording. The CTIconnect Service receives the information of the assigned monitor points that have been registered in the MiContact Center Business via a connection to MiContact Center Business. After registering successfully, MiContact Center Business sends the agents' additional data to the recording server.

1. In the detail view, select the add-on *MiContact Center Business*.



Step: Configure Add-on

Details *

Select add-on

☐ None

☒ MiContact Center Business

CTIconnect Module

Type CTIconnect passive

Grammar name* standard

Grammar version* 1.00.03

Connection Data

MiCCB URL* http://192.168.173.123

PBX user name* _admin

PBX password*

Additional Data

Arbitrary assignment +

| | | | |
|-----------|-----------|--|---|
| agentName | agentName | | - |
| fromName | fromName | | - |
| toName | toName | | - |

Save Cancel

Fig. 83: Configure add-on for MiContact Center Business

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. 21: Configure CTIconnect module

Group field Connection Data

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

| Parameter | Value/Description |
|----------------------|---|
| <i>MiCCB URL</i> | Enter the URL that MiContact Center Business runs on, e. g. http://192.168.173.123/miccsdk . |
| <i>PBX user name</i> | Enter the user name required to authenticate on MiContact Center Business. |
| <i>PBX password</i> | Enter the password required to authenticate on MiContact Center Business. |

Tab. 22: Configure connection data

Group field Additional Data

Depending on the configuration, the following additional data is delivered with the protocol when using MiContact Center Business:

| MiCCB additional data type | Example |
|--|--|
| <i>queueId</i> | "333168d9-ce96-4c0b-80eb-0cd524-ca379f" |
| <i>targetTimeForServiceLevel</i> | "00:02:00" |
| <i>timeOfferedToAgent</i> | "2019-10-11T09:54:13+02:00" |
| <i>supplementalDetails_toName</i> | "Sample, John" |
| <i>type</i> | "Queued" |
| <i>transferCount</i> | "1.0" |
| <i>toAddress</i> | "7104" |
| <i>supplementalDetailsDisplayName_toAddress</i> | "ToAddress" |
| <i>mediaServerId</i> | "26e821d1-8bc1-40c8-b65a-55ce35d2716b" |
| <i>supplementalDetailsDisplayName_fromName</i> | "FromName" |
| <i>timeOfLastAgentResponse</i> | "2019-10-11T09:54:19+02:00" |
| <i>supplementalDetails_fromAddress</i> | "7001" |
| <i>toName</i> | "Sample, John" |
| <i>timeOfferedToSystem</i> | "0001-01-01T00:00:00+00:00" |
| <i>supplementalDetails_callIds</i> | "446" |
| <i>fromName</i> | "John" |
| <i>agentFirstName</i> | "Nebel Carmen" |
| <i>mediaFolder</i> | "Inbox" |
| <i>lastAgentAction</i> | "Receive" |
| <i>supplementalDetails_fromName</i> | "Nebel Carmen" |
| <i>supplementalDetailsDisplayName_callIds</i> | "CallIds" |
| <i>classificationCodeRequired</i> | "false" |
| <i>agentLastName</i> | "Sample" |
| <i>mediaSpecificInfo</i> | "MitaiVoiceCommand 1 7104 446 {"G CID":"3BB49626471B011E59AA","P C ID":"3BB49626471B011E592E","SCI D":""}" |
| <i>agentName</i> | "Sample, John" |
| <i>mediaType</i> | "Voice" |
| <i>supplementalDetailsDisplayName_isConference</i> | "IsConference" |

| MiCCB additional data type | Example |
|--|--|
| <i>timeOfLastCustomerResponse</i> | "0001-01-01T00:00:00+00:00" |
| <i>conversationState</i> | "Ended" |
| <i>folder</i> | "Inbox" |
| <i>allowAgentPreview</i> | "true" |
| <i>supplementalDetails_toAddress</i> | "7104" |
| <i>mediaServerType</i> | "Mcd" |
| <i>supplementalDetails_isConference</i> | "False" |
| <i>agentId</i> | "5705bff7-957c-4c23-8ad1-9ed45922a7b4" |
| <i>supplementalDetailsDisplayName_fromAddress</i> | "FromAddress" |
| <i>workTimer</i> | "00:00:00" |
| <i>native</i> | "true" |
| <i>fromAddress</i> | "7001" |
| <i>direction</i> | "Incoming" |
| <i>conversationId</i> | "3BB49626471B011E5924" |
| <i>queueIsWrapUpTimeEnabled</i> | "false" |
| <i>timeOfferedToQueue</i> | "0001-01-01T00:00:00+00:00" |
| <i>agentReporting</i> | "7104" |
| <i>failedRouteReason</i> | "None" |
| <i>supplementalDetails_callParticipants</i> | "7104 7001 " |
| <i>supplementalDetailsDisplayName_callParticipants</i> | "ToName" |
| <i>supplementalDetailsDisplayName_toName</i> | "CallParticipants" |

The following additional fields are available if the communication runs via an [IVR](#) system:

| MiCCB additional data type | Example |
|--|----------------------|
| <i>supplementalDetails_ani</i> | "7001" |
| <i>supplementalDetailsDisplayName_recording_Decision</i> | "Recording_Decision" |
| <i>supplementalDetailsDisplayName_phoneNumber</i> | "PhoneNumber" |
| <i>queueDialable</i> | "7500" |
| <i>queueReporting</i> | "P112" |
| <i>supplementalDetails_recording_Decision</i> | "Yes" |
| <i>supplementalDetailsDisplayName_ani</i> | "ANI" |
| <i>supplementalDetails_phoneNumber</i> | "7001" |
| <i>queueName</i> | "Testqueue_1" |


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.

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

Fig. 84: 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 miscellaneous settings




Configuring these settings is not required for this recording solution. Even without this configuration step, the integration has been configured comprehensively and can be activated.

Activate integration

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

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

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

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











| Mitel MiVoice 5000 | | Mitel MiVoice 5000 active | ✗ | ✓ |
|----------------------------------|---|---------------------------|---|---|
| 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. 85: 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 5000 | Mitel MiVoice 5000 active |  |  |

Fig. 86: Activated integration



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



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






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

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

Deactivate/Delete integration

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

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







| + ×   Integration ▾ General | | | |
|---|---------------------------|---|---|
| Name ↕ | Type ▲ | Active ↕ | Status ↕ |
|  Mitel MiVoice 5000 | Mitel MiVoice 5000 active |  |  |

Fig. 87: 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.

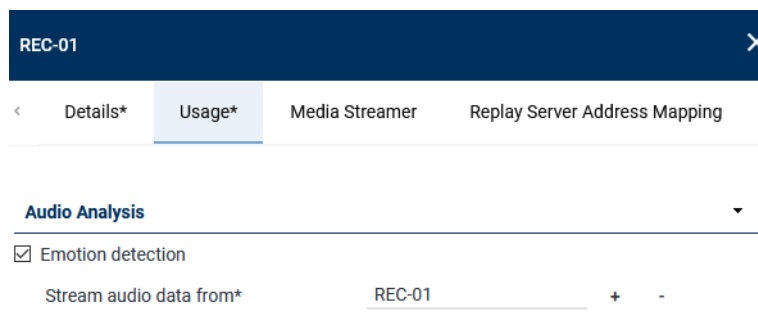
Preconditions for validation:

- 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*.



REC-01

< Details* Usage* Media Streamer Replay Server Address Mapping

Audio Analysis

☒ Emotion detection

Stream audio data from* REC-01 + -

Fig. 88: Servers module - Activate emotion detection

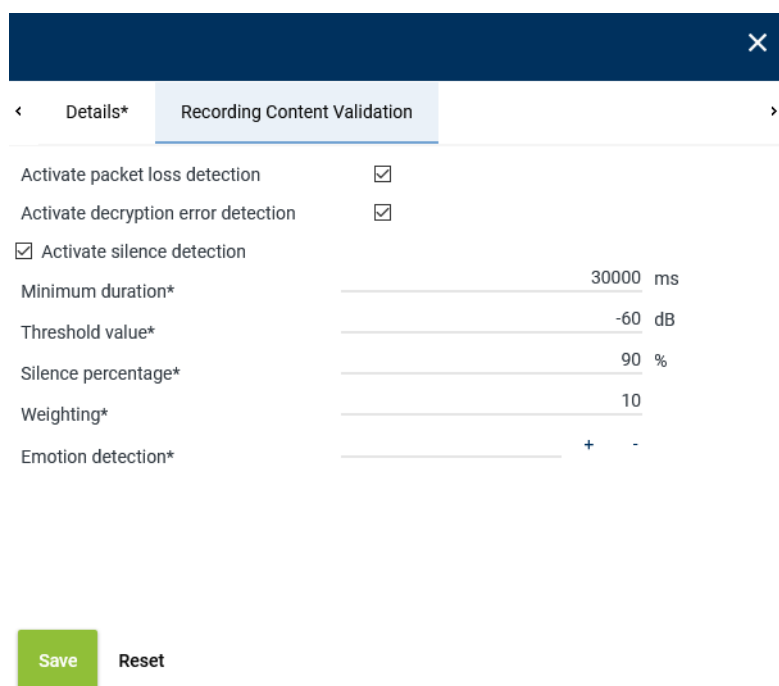
5. Activate the function *Emotion detection*.
6. By clicking on the icon **+**, select the server that emotion detection runs on.
 - ⇒ This server will then appear in the list in the Integrations module in the tab *Recording Content Validation* to configure silence detection.

Configuration in the Integrations module

1. In the main view, select the integration for which you would like to check the validity of recording.
2. Select the tab *Recording Content Validation*.

The following criteria are available to check proper recording:

- *Packet loss detection*
- *Decryption error detection*
- *Silence detection*



Details* Recording Content Validation

Activate packet loss detection ☒

Activate decryption error detection ☒

☒ Activate silence detection

Minimum duration* 30000 ms

Threshold value* -60 dB

Silence percentage* 90 %


Weighting* 10

Emotion detection* + -

Save Reset

Fig. 89: Create integration - tab Recording Content Validation

Activate packet loss detection ☒ 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 (30 seconds). |
| <i>Threshold value</i> | Enter a threshold value of the audio level in dB under which the section is supposed to be considered a silence section. Default value is -60 dB. |
| <i>Silence percentage</i> | Enter the percentage of silence in a recording which is supposed to trigger a notification. Default value is 90 %. |
| <i>Weighting</i> | Enter the smoothing factor defining to which extent the audio curves (samples) are supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 0-10000 can be recommended. |
| <i>Emotion detection server</i> | By clicking on the icon  , select the server that emotion detection runs on. The speech analysis software recognizes whether there are silence sections in the recording. |

NOTICE! The list only displays servers which have been configured for audio analysis and have been assigned in the Servers module.

- Select the respective server from the list of available servers.

Emotion Detection

Name

REC-01

Rows per page 20

1 - 8 of 8

1-8

<<

>>

8-1

Add

Cancel

Fig. 90: Select server for emotion detection

- 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 PHONE_{app} configuration
 - Configure PBX-specific parameters
 - Phones module
 - Configure the parameters for the assignment of the phone, e. g. extension, PBX phone ID, computer name, address for replay via phone, phone type, and time slot.
 - Recording Planner module
 - Configure operation modes

7.3.4.1 Configure Servers module

To be able to control the recording by means of PHONE_{app}, 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*.

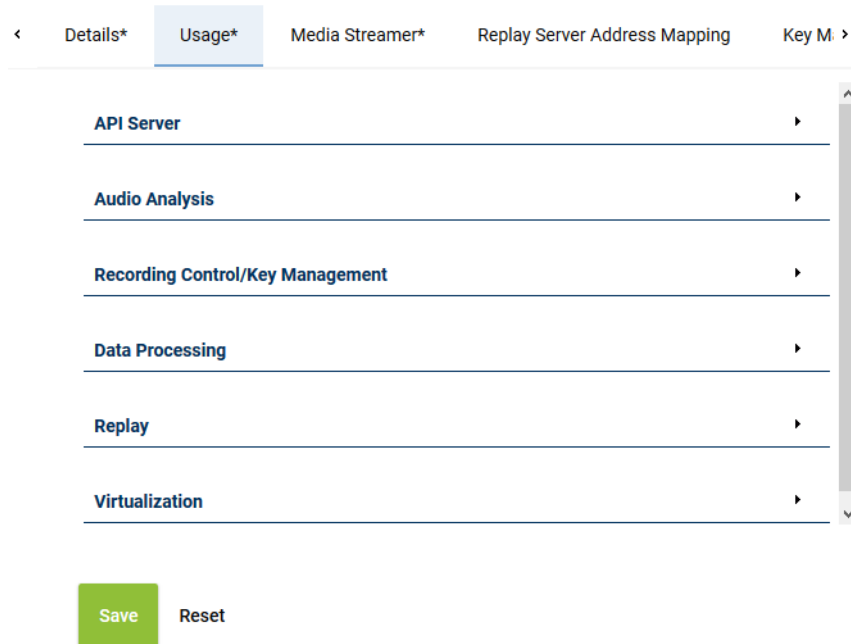


Fig. 91: Servers - tab Usage

3. Open the group field *Recording Control/Key Management*.

7.3.4.1.1 Group field Recording Control/Key Management

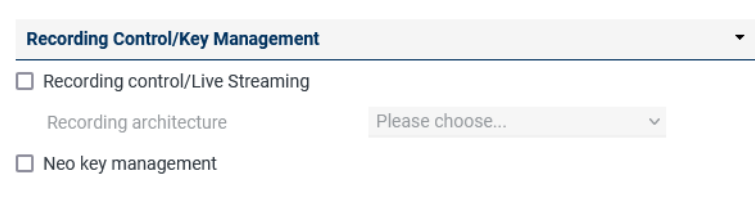


Fig. 92: Group field Recording Control/Key Management

| 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. 23: 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:

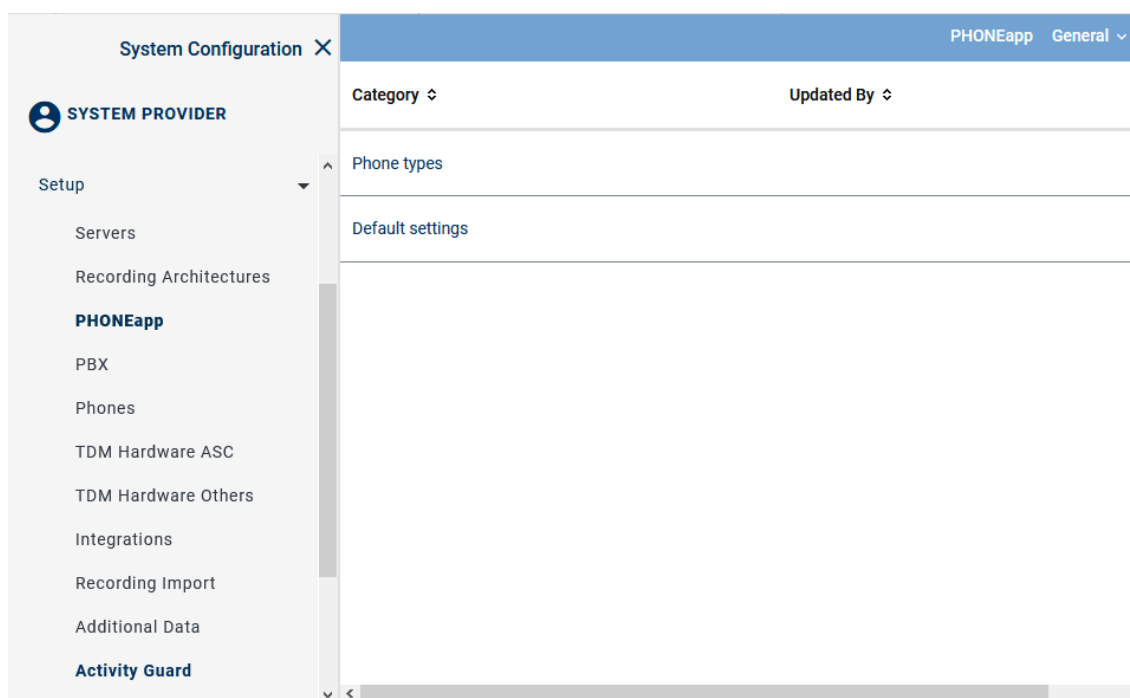


Fig. 93: PHONEapp - main view:

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. 94: 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. 95: 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. 96: 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. 97: 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. 98: 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. 99: 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. 100: 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*

Predefined Tagging Fields


☒ Activated



Tagging Field

Request

Fig. 101: Configure tagging fields


2. Activate the check box *Activated*.
3. Click on the icon  (*Edit*).
⇒ The window *Tagging Fields* appears.

Tagging Fields

| 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 | |

Apply **Cancel**

Fig. 102: 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.

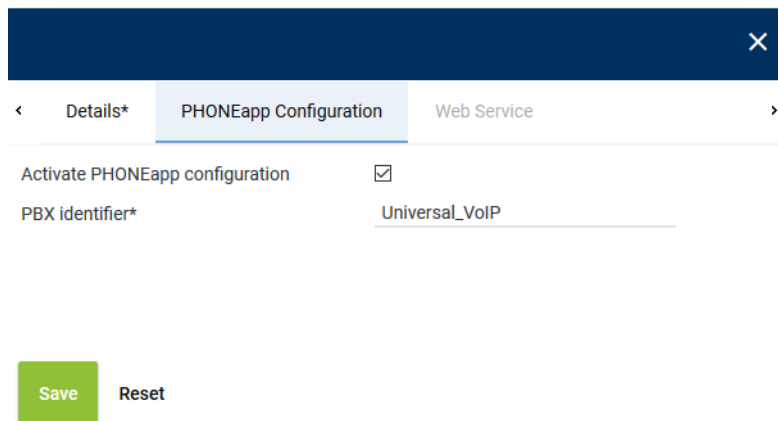


Fig. 103: Activate PHONEapp configuration

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. |

- 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.

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

⇒ The following window appears:

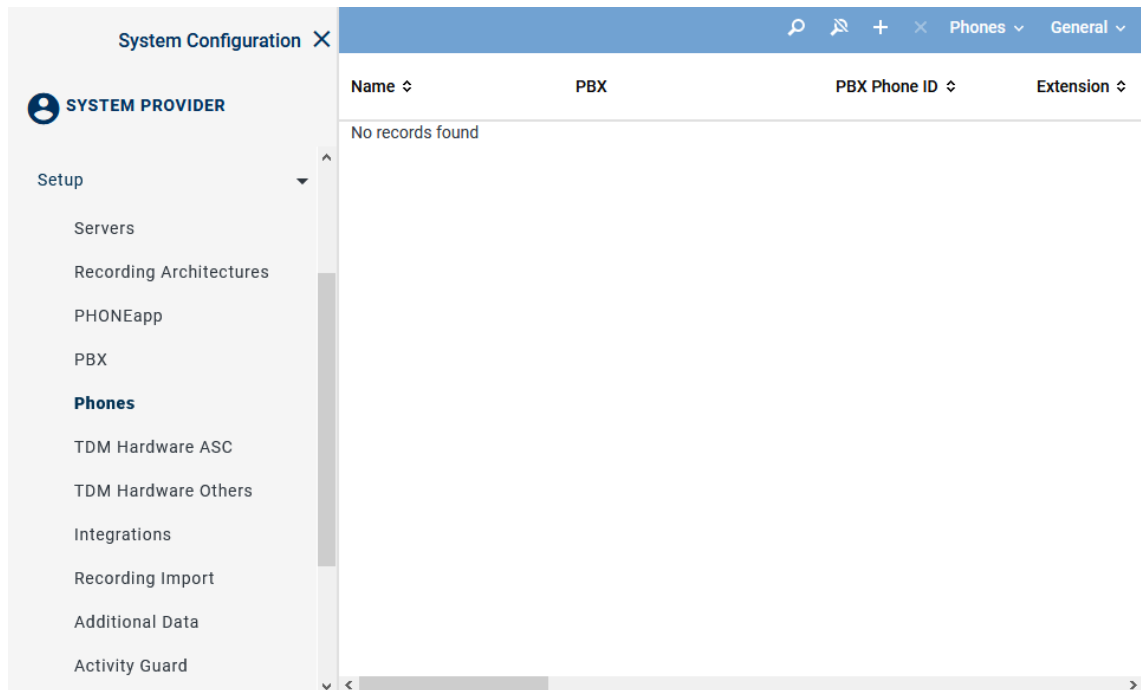


Fig. 104: Phones - main view

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. 105: Toolbar


| | | |
|---|---------------|-------------------------------------|
|  | <i>Create</i> | Creates a new phone. Available are: |
|---|---------------|-------------------------------------|

| | | |
|---|---------------------------------|--|
| | | <ul style="list-style-type: none"> • IP phone • TDM phone |
|  | <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, see Search.</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 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> | <p>Opens a window where you can adjust the following settings for the main view:</p> <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.

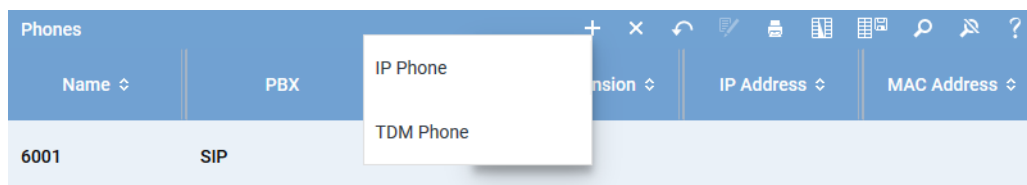


Fig. 106: Create phone

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. 107: 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. 24: 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.

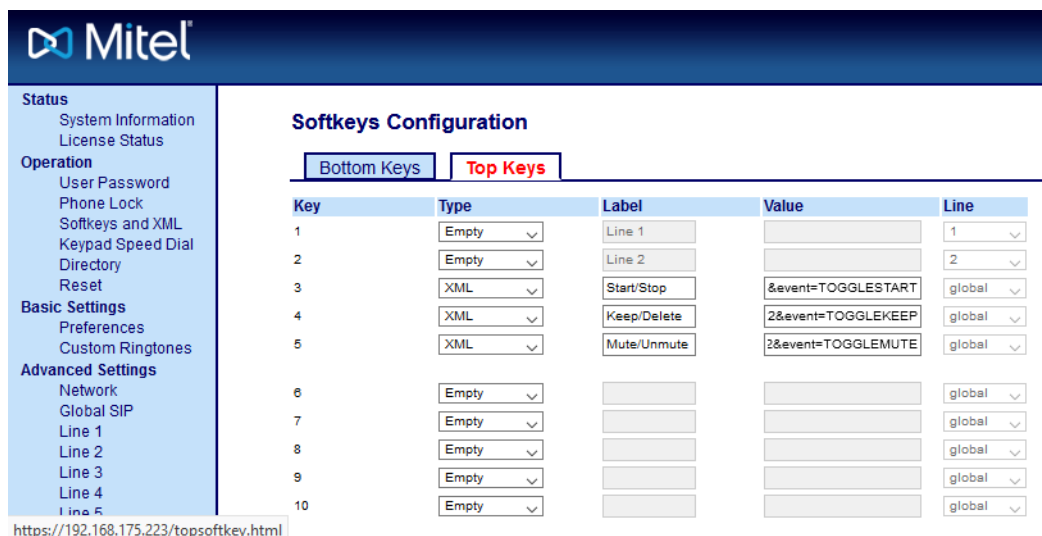


For information about the Recording Planner module refer to the administration manual for tenants *Recording Planner*.

7.3.4.6 Configure function keys on the Mitel phone

To be able to use the keys and the **LED** display on the phone, you must configure the function keys 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=TOGGLEMUTE | global |
| 6 | Empty | | | global |
| 7 | Empty | | | global |
| 8 | Empty | | | global |
| 9 | Empty | | | global |
| 10 | Empty | | | global |

<https://192.168.175.223/topsoftkey.html>

Fig. 108: Configure function keys 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.

The parameter `FS` stands for Free Seating to allow the assignment of the extension even if the IP address changes.

Replace the entry `<RECORDER-IP>` with the IP address of the XML Push Server.

| | |
|-------------|--|
| Start/Stop | <code>http://<RECORDER-IP>/PHONEapp/MitelPHONEApp?deviceExtension=\$\$SIPUSERNAME\$\$&event=TOGGLESTART&FS=true</code> |
| Keep/Delete | <code>http://<RECORDER-IP>/PHONEapp/MitelPHONEApp?deviceExtension=\$\$SIPUSERNAME\$\$&event=TOGGLEKEEP&FS=true</code> |
| Mute/Unmute | <code>http://<RECORDER-IP>/PHONEapp/MitelPHONEApp?deviceExtension=\$\$SIPUSERNAME\$\$&event=TOGGLEMUTE&FS=true</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. 109: Configure HTTPS settings

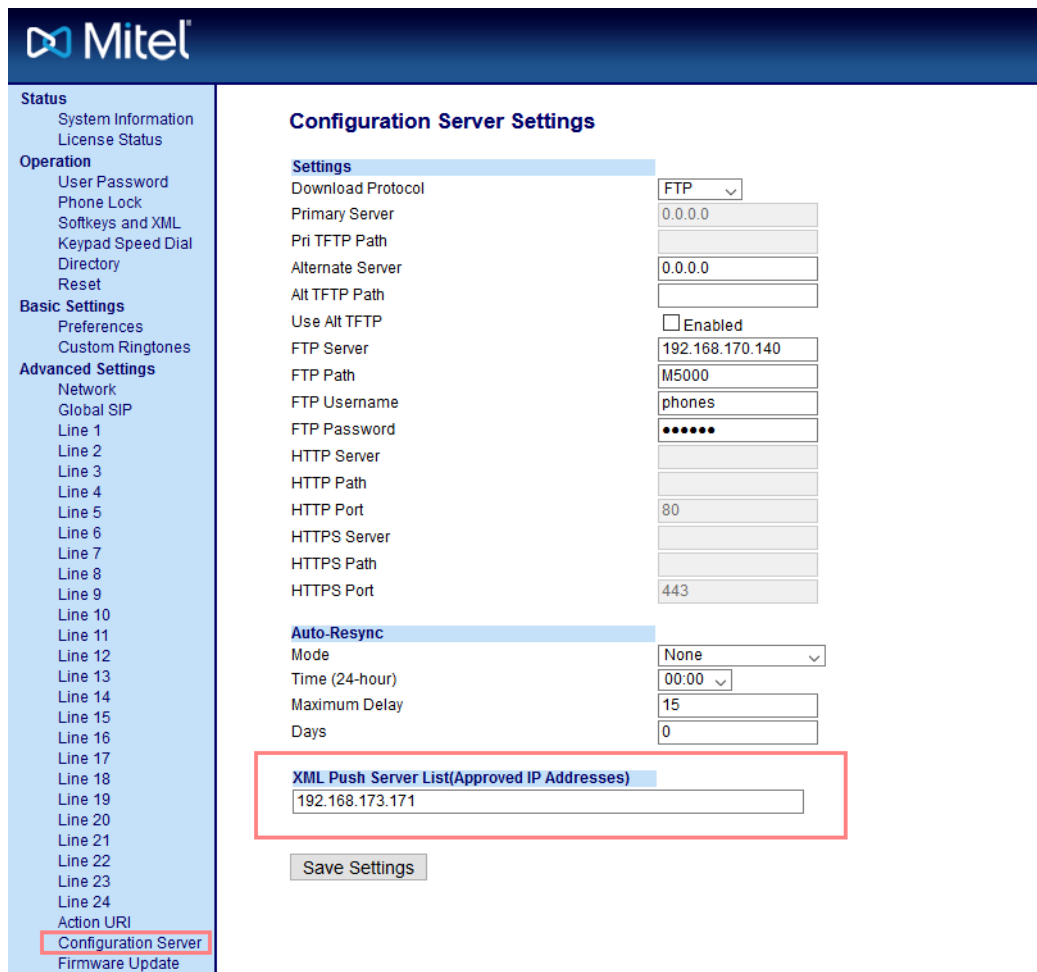
2. Deactivate the check box for the following parameters:

- 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.



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
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
Firmware Update

Configuration Server Settings

Settings

Download Protocol: FTP

Primary Server: 0.0.0.0

Pri TFTP Path:

Alternate Server: 0.0.0.0

Alt TFTP Path:

Use Alt TFTP: ☐ Enabled

FTP Server: 192.168.170.140

FTP Path: M5000

FTP Username: phones

FTP Password:

HTTP Server:

HTTP Path:

HTTP Port: 80

HTTPS Server:

HTTPS Path:

HTTPS Port: 443

Auto-Resync

Mode: None

Time (24-hour): 00:00

Maximum Delay: 15

Days: 0

XML Push Server List (Approved IP Addresses)

192.168.173.171

Save Settings

Fig. 110: Configure XML Push Server

- In the section *XML Push Server List (Approved IP Addresses)*, enter the IP address of the recording server.
- Click on the button *Save Settings* to apply the entries.
⇒ In the display of the phone, the LED indicator shows the respective status.



L1: 22002

Line 1

Line 2

Recording

Mute

Keep

test

15:41
6 Feb 2020

Kein Dienst

Fig. 111: Assignment of the top keys and displayed status of the recording

7.4 Configure Genesys T-Server (optional)

7.4.1 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.

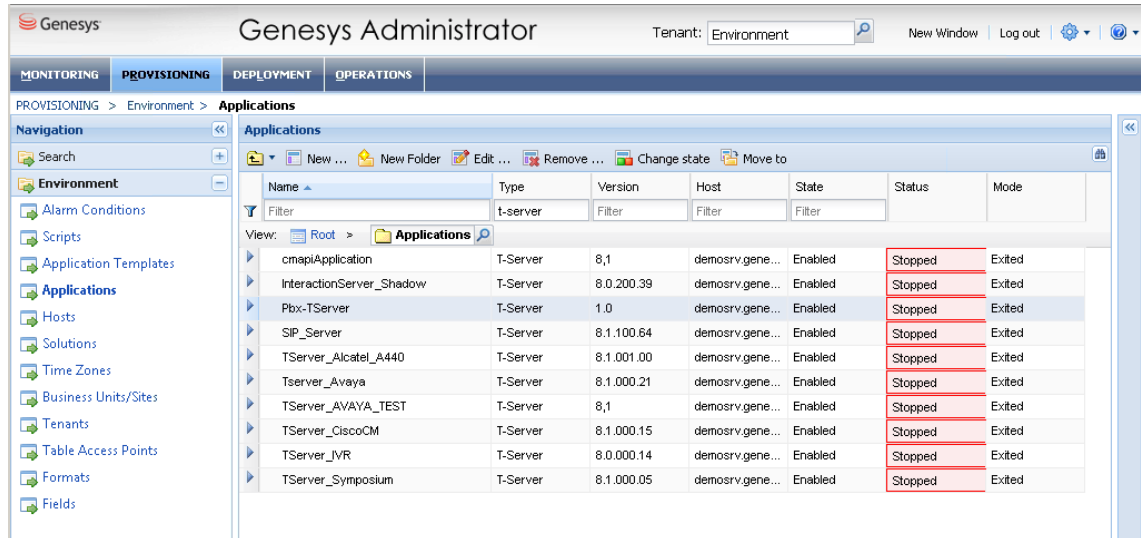


Fig. 112: Genesys Administrator - select T-Server

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*.

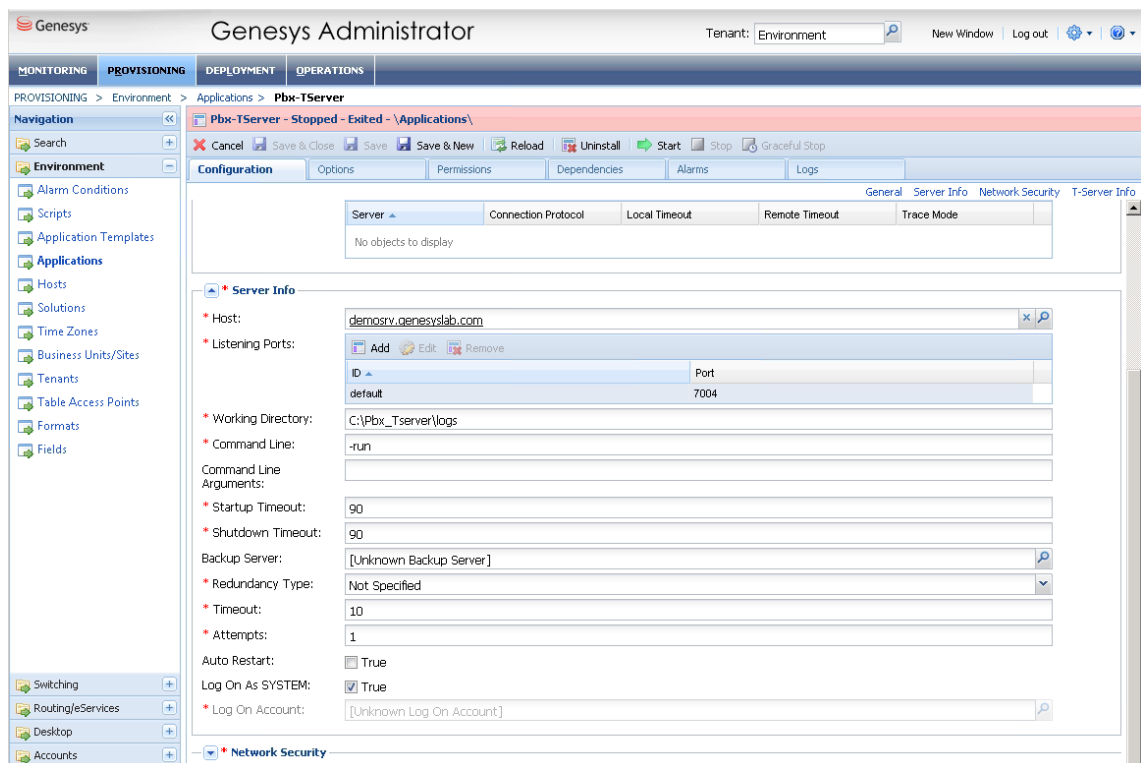


Fig. 113: Genesys Administrator - configure T-Server

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.

7.4.2 Configure IP address and port of the Genesys Configuration Server

1. Click on the menu item *Environment > Applications* in the navigation bar.

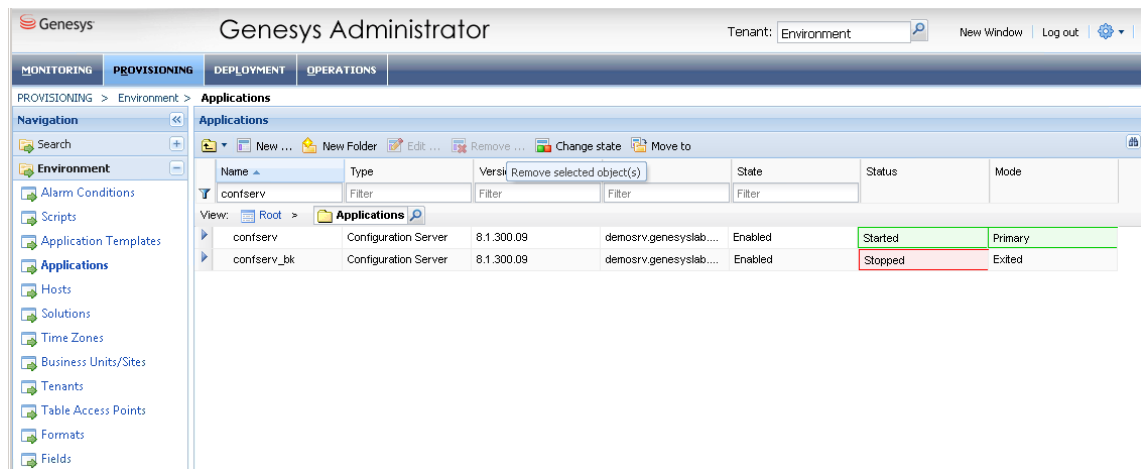


Fig. 114: Genesys Administrator - select configuration server

2. Double-click on the entry Configuration Server, e. g. *confserv*.
⇒ The window *Configuration* appears.
3. Expand the area *Server Info*.

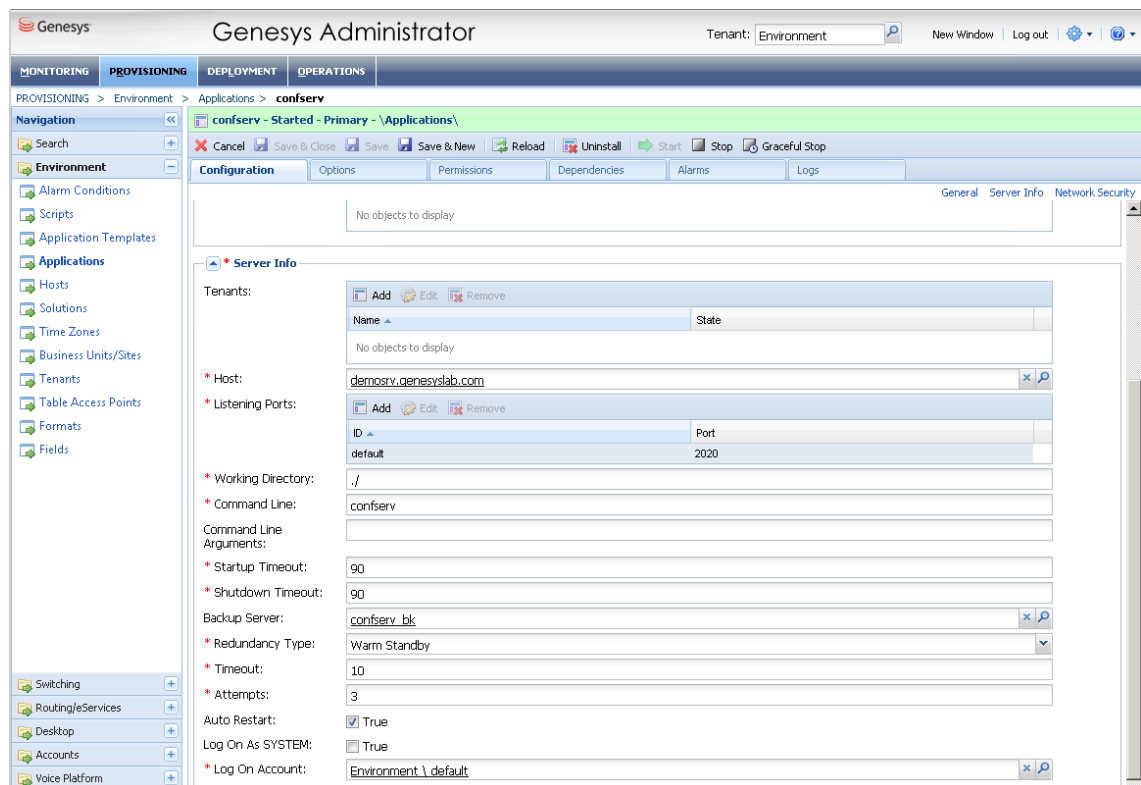


Fig. 115: Genesys Administrator - configure configuration server

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*.

7.4.3 Configure switch instance in the Genesys Configuration Server

1. Click on the menu item *Switching > Switches* in the navigation bar.

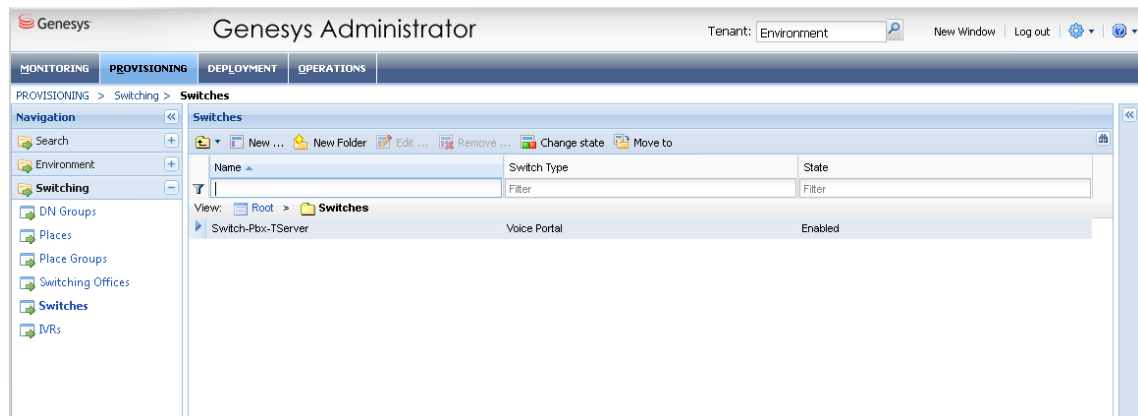


Fig. 116: Genesys Administrator - switch instances

2. Double-click on the entry of the switch instance.
⇒ The window *Configuration > General* appears.

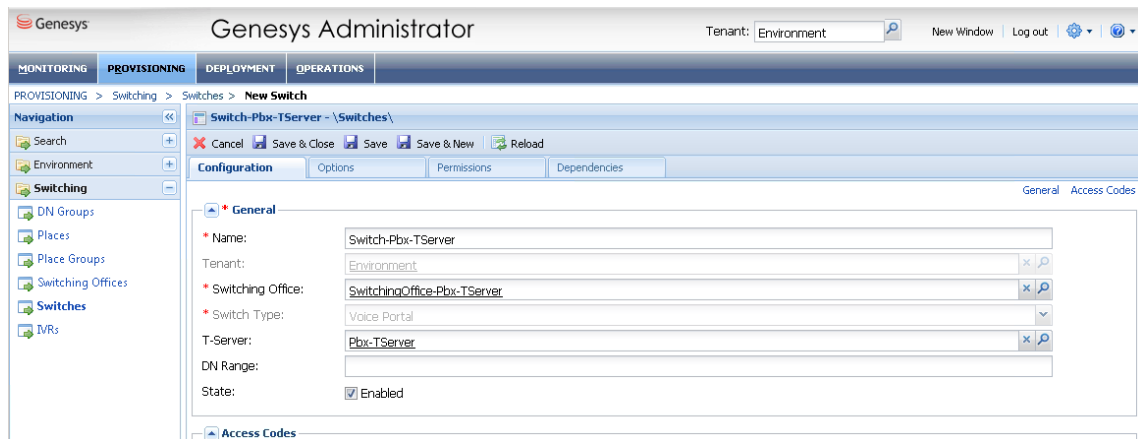


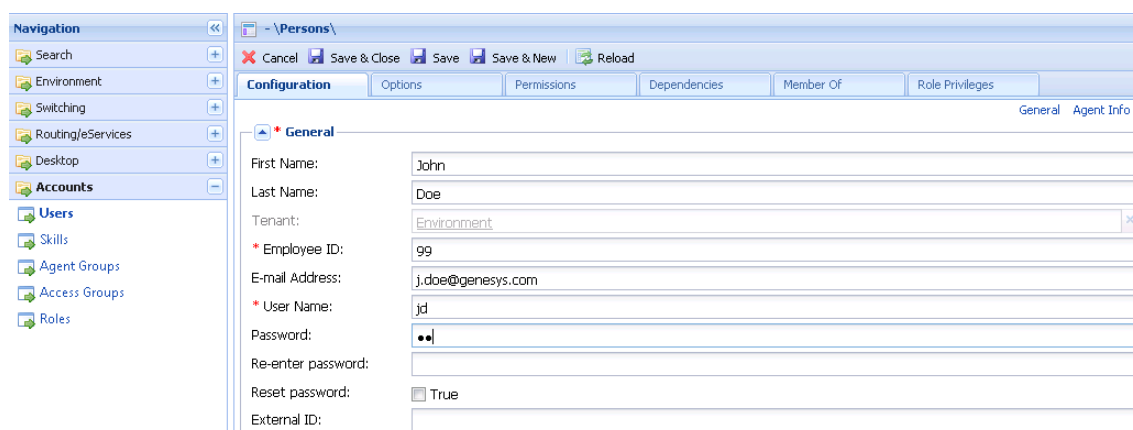
Fig. 117: Genesys Administrator - configure switch instance

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.

7.4.4 Create users for the Genesys Configuration Server

To access the Genesys Configuration Server, you have to create a user.

1. Click on the menu item *Account > Users* in the navigation bar.
2. Click on the button *New*.
⇒ The window *Configuration > General* appears.



Navigation: Search, Environment, Switching, Routing/Services, Desktop, Accounts, Users, Skills, Agent Groups, Access Groups, Roles

Configuration: Options, Permissions, Dependencies, Member Of, Role Privileges

General Agent Info

* General

First Name: John

Last Name: Doe

Tenant: Environment

* Employee ID: 99

E-mail Address: j.doe@genesys.com

* User Name: jd

Password: [Masked]

Re-enter password: [Masked]

Reset password: ☐ True

External ID: [Empty]

Fig. 118: 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 | Overview of the recording solution | 6 |
| Fig. 2 | Overview of the recording solution | 7 |
| Fig. 3 | Mitel MiVoice 5000 - Configure registering..... | 13 |
| Fig. 4 | Mitel MiVoice 5000 - Status of CSTA server | 13 |
| Fig. 5 | Mitel MiVoice 5000 - Configure gateway | 13 |
| Fig. 6 | Mitel MiVoice 5000 - configured CSTA link | 14 |
| Fig. 7 | Login screen MBG | 14 |
| Fig. 8 | Certificate Management..... | 15 |
| Fig. 9 | Confirm selected certificate | 15 |
| Fig. 10 | Success notification for shared certificate | 16 |
| Fig. 11 | System Configuration - Web interface | 17 |
| Fig. 12 | System Configuration - main view | 17 |
| Fig. 13 | Recording architectures - main view..... | 18 |
| Fig. 14 | Toolbar Recording Architectures module | 19 |
| Fig. 15 | Create recording architecture - All-in-one Basic Recording..... | 20 |
| Fig. 16 | Recording architecture - tab Details | 20 |
| Fig. 17 | Select integration type | 21 |
| Fig. 18 | Recording architecture - tab Server Assignment..... | 22 |
| Fig. 19 | Recording architecture - assign server | 22 |
| Fig. 20 | Recording architecture - activate recording variant | 23 |
| Fig. 21 | Recording architecture - activate recording architecture | 23 |
| Fig. 22 | Servers - main view | 24 |
| Fig. 23 | Toolbar Servers module | 24 |
| Fig. 24 | Add server locations | 25 |
| Fig. 25 | Delete server location | 26 |
| Fig. 26 | Servers - tab Details | 27 |
| Fig. 27 | Servers - tab usage | 27 |
| Fig. 28 | Group field API Server..... | 28 |
| Fig. 29 | Select storage expansion | 29 |
| Fig. 30 | Group field Audio Analysis..... | 30 |
| Fig. 31 | Select server for emotion detection | 30 |
| Fig. 32 | Group field Recording Control/Key Management..... | 30 |
| Fig. 33 | Group field Data Processing..... | 31 |
| Fig. 34 | Select server..... | 33 |
| Fig. 35 | Group field Replay | 34 |
| Fig. 36 | Select server..... | 35 |
| Fig. 37 | Group field Virtualization..... | 36 |
| Fig. 38 | Servers module - tab Media Streamer..... | 37 |
| Fig. 39 | Servers module - tab Replay Server Address Mapping..... | 38 |
| Fig. 40 | Servers module - tab Key Management | 40 |
| Fig. 41 | Servers module - tab Keystore/Virtualization | 42 |

| | | |
|---------|---|----|
| Fig. 42 | PBX module - main view..... | 43 |
| Fig. 43 | Toolbar PBX module..... | 43 |
| Fig. 44 | Create new PBX - tab Details | 44 |
| Fig. 45 | Tenants - main view - tab Extensions | 45 |
| Fig. 46 | Assign extensions to tenants | 46 |
| Fig. 47 | Remove extensions | 47 |
| Fig. 48 | Select extensions..... | 48 |
| Fig. 49 | Tenants - main view - tab PBX Agent ID | 49 |
| Fig. 50 | Assign PBX Agent IDs to tenants | 49 |
| Fig. 51 | Select PBX Agent IDs..... | 51 |
| Fig. 52 | Additional Data module main view..... | 52 |
| Fig. 53 | Configure additional data..... | 52 |
| Fig. 54 | Additional data - configure availability | 53 |
| Fig. 55 | Integrations - main view | 54 |
| Fig. 56 | Toolbar Integrations module | 54 |
| Fig. 57 | Choose file..... | 55 |
| Fig. 58 | Upload grammar | 55 |
| Fig. 59 | Create integration type | 56 |
| Fig. 60 | Integrations - select PBX | 56 |
| Fig. 61 | Assign recording architecture - All-in-one Basic | 57 |
| Fig. 62 | Configuration steps of the integration | 57 |
| Fig. 63 | Configuration step - Configure Recording Architecture | 58 |
| Fig. 64 | CTI connection data - tab MiVoice 5000 (CSTA)..... | 59 |
| Fig. 65 | Group field CTIconnect Module | 59 |
| Fig. 66 | Group field Connection Data | 59 |
| Fig. 67 | Configure connection data | 60 |
| Fig. 68 | Group field Additional Data - free assignment of additional data..... | 61 |
| Fig. 69 | Configure CTIconnect connection data to MBG | 61 |
| Fig. 70 | Group field CTIconnect Module | 62 |
| Fig. 71 | Group field Connection Data | 62 |
| Fig. 72 | Configure connection data | 63 |
| Fig. 73 | Group field Additional Data - free assignment of additional data..... | 64 |
| Fig. 74 | Configuration step - configure monitor points | 64 |
| Fig. 75 | Add extension monitor points | 65 |
| Fig. 76 | Configured extension monitor points | 66 |
| Fig. 77 | Configuration step - Global Recording Settings..... | 67 |
| Fig. 78 | Configuration step - Configure recording servers | 68 |
| Fig. 79 | Overview of the add on of Genesys T-Server..... | 69 |
| Fig. 80 | Configure add-on for Genesys T-Server..... | 71 |
| Fig. 81 | Configure connection data | 72 |
| Fig. 82 | Group field Additional Data - free assignment of additional data..... | 73 |
| Fig. 83 | Configure add-on for MiContact Center Business | 74 |

| | | |
|----------|---|-----|
| Fig. 84 | Group field Additional Data - free assignment of additional data..... | 77 |
| Fig. 85 | Activate integration | 77 |
| Fig. 86 | Activated integration | 78 |
| Fig. 87 | Deactivate integration | 78 |
| Fig. 88 | Servers module - Activate emotion detection | 79 |
| Fig. 89 | Create integration - tab Recording Content Validation | 79 |
| Fig. 90 | Select server for emotion detection | 80 |
| Fig. 91 | Servers - tab Usage | 82 |
| Fig. 92 | Group field Recording Control/Key Management | 82 |
| Fig. 93 | PHONEapp - main view:..... | 83 |
| Fig. 94 | Detail view phone types | 84 |
| Fig. 95 | Display of the properties | 84 |
| Fig. 96 | Detail view Default settings..... | 85 |
| Fig. 97 | Group field Tagging Attributes | 87 |
| Fig. 98 | Edit tagging attributes | 88 |
| Fig. 99 | Group field Register Fields | 88 |
| Fig. 100 | Edit register fields | 89 |
| Fig. 101 | Configure tagging fields | 90 |
| Fig. 102 | Edit tagging fields | 90 |
| Fig. 103 | Activate PHONEapp configuration..... | 91 |
| Fig. 104 | Phones - main view | 92 |
| Fig. 105 | Toolbar..... | 92 |
| Fig. 106 | Create phone | 93 |
| Fig. 107 | Create phones - activate PHONEapp | 94 |
| Fig. 108 | Configure function keys via the web interface | 96 |
| Fig. 109 | Configure HTTPS settings | 97 |
| Fig. 110 | Configure XML Push Server | 98 |
| Fig. 111 | Assignment of the top keys and displayed status of the recording..... | 98 |
| Fig. 112 | Genesys Administrator - select T-Server | 99 |
| Fig. 113 | Genesys Administrator - configure T-Server | 99 |
| Fig. 114 | Genesys Administrator - select configuration server | 100 |
| Fig. 115 | Genesys Administrator - configure configuration server | 100 |
| Fig. 116 | Genesys Administrator - switch instances | 101 |
| Fig. 117 | Genesys Administrator - configure switch instance | 101 |
| Fig. 118 | Genesys administrator - create user..... | 102 |

List of tables

| | | |
|---------|---|----|
| Tab. 1 | Licenses..... | 9 |
| Tab. 2 | Licenses for the phone application (optional) | 9 |
| Tab. 3 | Licenses..... | 9 |
| Tab. 4 | Licenses for recording via MiVoice Border Gateway | 9 |
| Tab. 5 | Licenses for Genesys T-Server optional..... | 9 |
| Tab. 6 | Licenses for MiContact Center Business optional | 10 |
| Tab. 7 | Login data - system provider | 17 |
| Tab. 8 | Configure audio analysis | 30 |
| Tab. 9 | Configure recording control/key management..... | 31 |
| Tab. 10 | Data storage | 31 |
| Tab. 11 | Configure replay | 34 |
| Tab. 12 | Configure virtualization | 36 |
| Tab. 13 | Create PBX..... | 44 |
| Tab. 14 | Configure CTIconnect module..... | 59 |
| Tab. 15 | Configure connection data..... | 60 |
| Tab. 16 | Configure CTIconnect module..... | 62 |
| Tab. 17 | Configure connection data..... | 63 |
| Tab. 18 | Global recording settings | 67 |
| Tab. 19 | Configure add-on for Genesys T-Server..... | 71 |
| Tab. 20 | Configure connection data..... | 72 |
| Tab. 21 | Configure CTIconnect module..... | 74 |
| Tab. 22 | Configure connection data..... | 75 |
| Tab. 23 | Configure recording control/key management..... | 82 |
| Tab. 24 | Add phone | 94 |

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)

IP

Internet Protocol, basic protocol for Internet communication

IVR

Interactive Voice Response is a voice dialog system allowing a computer to interact with humans through the use of voice and DTMF tones input via the keypad.

LCR

Last Conversation Repeat

LED

Light-emitting diode

MBG

MiVoice Border Gateway

PBX

Private Branch Exchange

RTP

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

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