

EVOIPneo passive for Mitel MiVoice MX-ONE trunk-side recording



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.....	4
2	Introduction.....	5
3	System requirements	7
3.1	Hardware components.....	7
3.1.1	Recorder	7
3.2	Software components.....	7
3.3	Additional requirements and restrictions.....	7
4	Installation requirements	8
4.1	Licenses.....	8
4.2	Information.....	8
5	Overview of how to install and configure the product.....	9
6	Installation.....	10
7	Configuration	11
7.1	Configure Mitel MiVoice MX-ONE CSTA 3.....	11
7.1.1	Configure CSTA server.....	11
7.1.2	Check functionality.....	12
7.2	System Configuration	13
7.2.1	Start application	13
7.2.2	Configure recording solution All-in-one Basic.....	15
7.2.2.1	Create recording architecture	15
7.2.2.2	Configure server	20
7.2.2.3	Create PBX.....	39
7.2.2.4	Assign recording resources	42
7.2.2.5	Configure additional data.....	45
7.2.2.6	Create integration for All-in-one Basic	47
7.2.2.7	Adjust Neo configuration file	59
7.2.3	Configure Recording Content Validation	60
8	Troubleshooting	63
	List of figures	64
	List of tables.....	66
	Glossary	67

General information

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

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

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

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

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

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

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

2 Introduction

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



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

With the recording solution EVOIP_{neo} passive for Mitel MiVoice MX-ONE trunk-side recording, audio data is sniffed on the SIP trunk of the "Mitel MX-ONE" PBX. This allows unencrypted recording of conversations of external participants and participants registered on the PBX. Only conversations made via the SIP trunk of the Mitel MX-ONE PBX are recorded.

With versions 7.0 and higher, encrypted recording is possible. The CSTA interface then delivers encryption keys to decrypt the recordings.



A SIP trunk is limited to 500 concurrent recordings.

Direct monitoring of the Trunk Line Numbers (trunk ID) on the Mitel MX-ONE PBX provides call information from the CSTA protocol relevant for the recording decision and tagging.

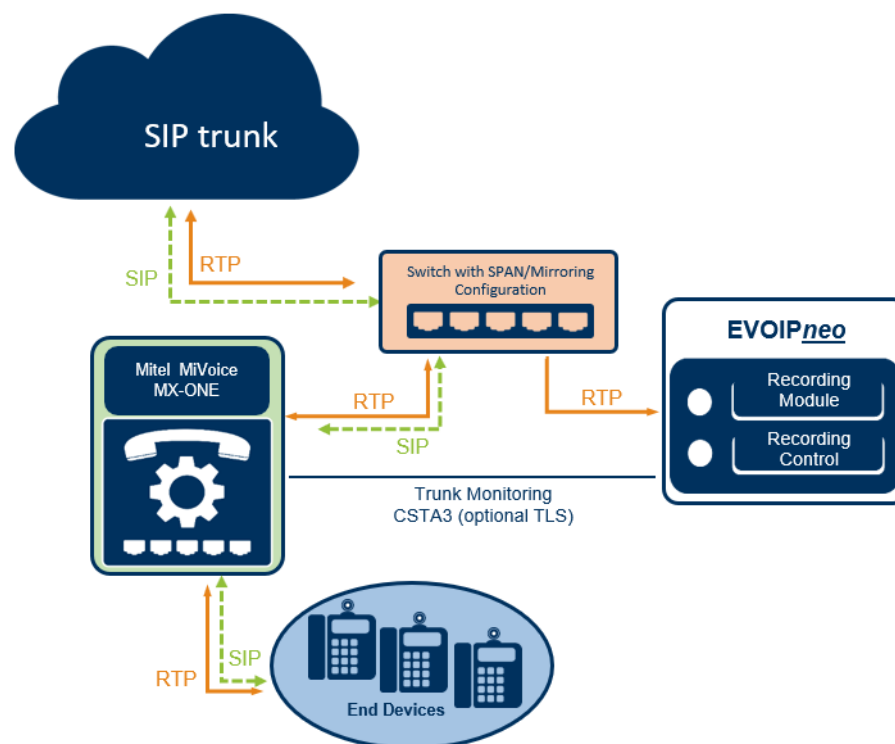


Fig. 1: Recording solution EVOIP_{neo} passive for Mitel MiVoice MX-ONE trunk-side recording



The passive recording solution EVOIP_{neo} passive for Mitel MiVoice MX-ONE trunk-side recording is contained in and configured via the active recording solution EVOIP_{neo} active for Mitel MiVoice MX-ONE (CSTA 3).

EVOIP_{neo} passive for Mitel MiVoice MX-ONE trunk-side recording with Mobile/MEX devices

For version 6.7 or higher, the Neo software offers the trunk-side recording solution EVOIP_{neo} passive for Mitel MiVoice MX-ONE trunk-side recording with mobile devices and MEX extensions.

When participant phone numbers can be signaled via different sources with a different number of zeros or a plus sign at the beginning, you can activate the trim function of the Recording Control Service, see [chapter "Adjust Neo configuration file", p. 59](#). This allows removing preceding zeros and the plus sign to standardize the format of the phone numbers.

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 Additional requirements and restrictions

The following recording variants are not supported in this recording solution:

- *Direct Media, (the RTP stream is invisible for the recording server),*

4 Installation requirements



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



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

4.1 Licenses

ASC

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

Tab. 1: Licenses for recording server



The passive recording solution EVOIP^{neo} passive for Mitel MiVoice MX-ONE trunk-side recording is contained in and configured via the active recording solution EVOIP^{neo} active for Mitel MiVoice MX-ONE (CSTA 3). Therefore, the license for EVOIP^{neo} active for Mitel MiVoice MX-ONE (CSTA 3) is required.

Licenses for recording with Mitel MiVoice MX-ONE

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

Tab. 2: Licenses for recording with Mitel MiVoice MX-ONE

4.2 Information

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

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



When updating versions \leq Neo 5.1, the CTI configuration parameter must be adjusted according to the new CSTA 3 connection. See CTIconnect module.

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

5 Overview of how to install and configure the product

The following steps have to be taken:

1. Install ASC 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 PBX 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

6 Installation



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



For information about the installation and configuration of Microsoft Windows refer to the respective installation manual for system providers *Configuration Microsoft Windows Server 2016*, *Configuration Microsoft Windows Server 2019* or *Configuration Microsoft Windows Server 2022*.



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

7 Configuration

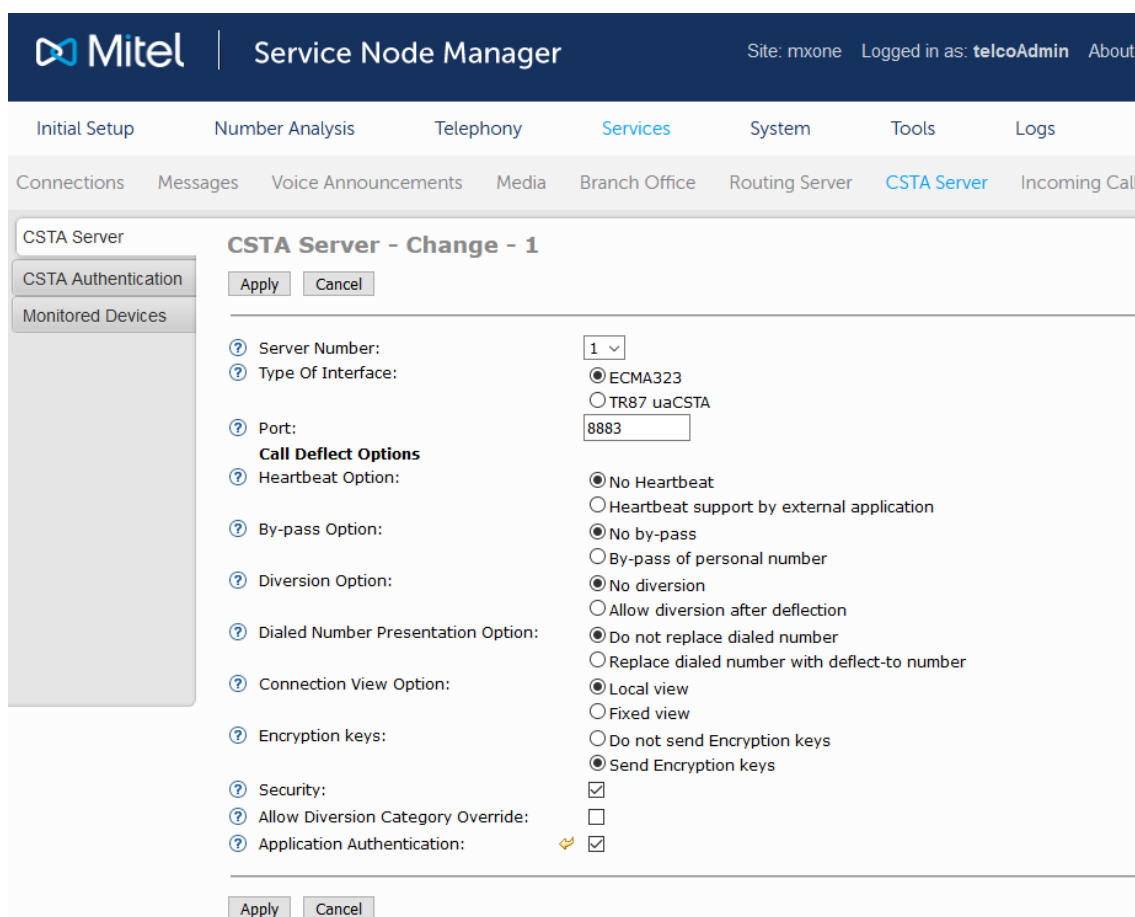
7.1 Configure Mitel MiVoice MX-ONE CSTA 3



A Mitel engineer configures the Mitel MiVoice MX-ONE PBX. The IP address of the recording server must be entered in the configuration file of the PBX so that the RTP data can be sent to the recording server.

7.1.1 Configure CSTA server

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



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

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

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

CSTA Server

CSTA Authentication

Monitored Devices

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

Server Number: 1

Type Of Interface: ☒ ECMA323 ☐ TR87 uaCSTA

Port: 8883

Call Deflect Options

Heartbeat Option: ☒ No Heartbeat ☐ Heartbeat support by external application

By-pass Option: ☒ No by-pass ☐ By-pass of personal number

Diversion Option: ☒ No diversion ☐ Allow diversion after deflection

Dialed Number Presentation Option: ☒ Do not replace dialed number ☐ Replace dialed number with deflect-to number

Connection View Option: ☒ Local view ☐ Fixed view

Encryption keys: ☐ Do not send Encryption keys ☒ Send Encryption keys

Security: ☒

Allow Diversion Category Override: ☐

Application Authentication: ☒

[Apply] [Cancel]

Fig. 2: Configure CSTA server

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

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

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

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



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

7.1.2

Check functionality

Check license status

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

The following login data is valid by default:

Username	<i>admin</i>
Password	<i>22222</i>

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

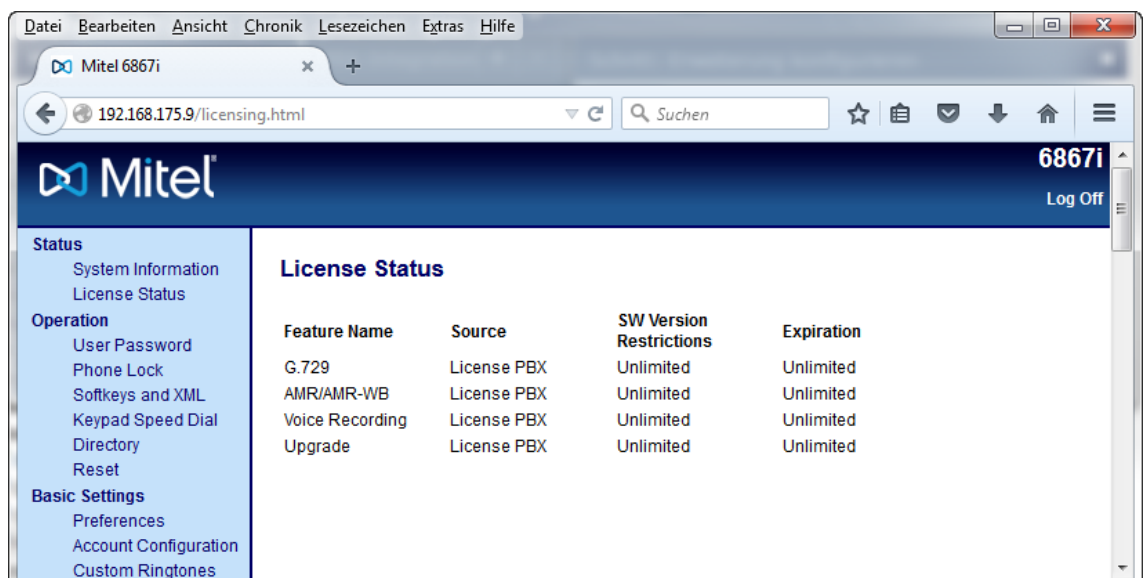


Fig. 3: Check license status

Check server, path and port

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

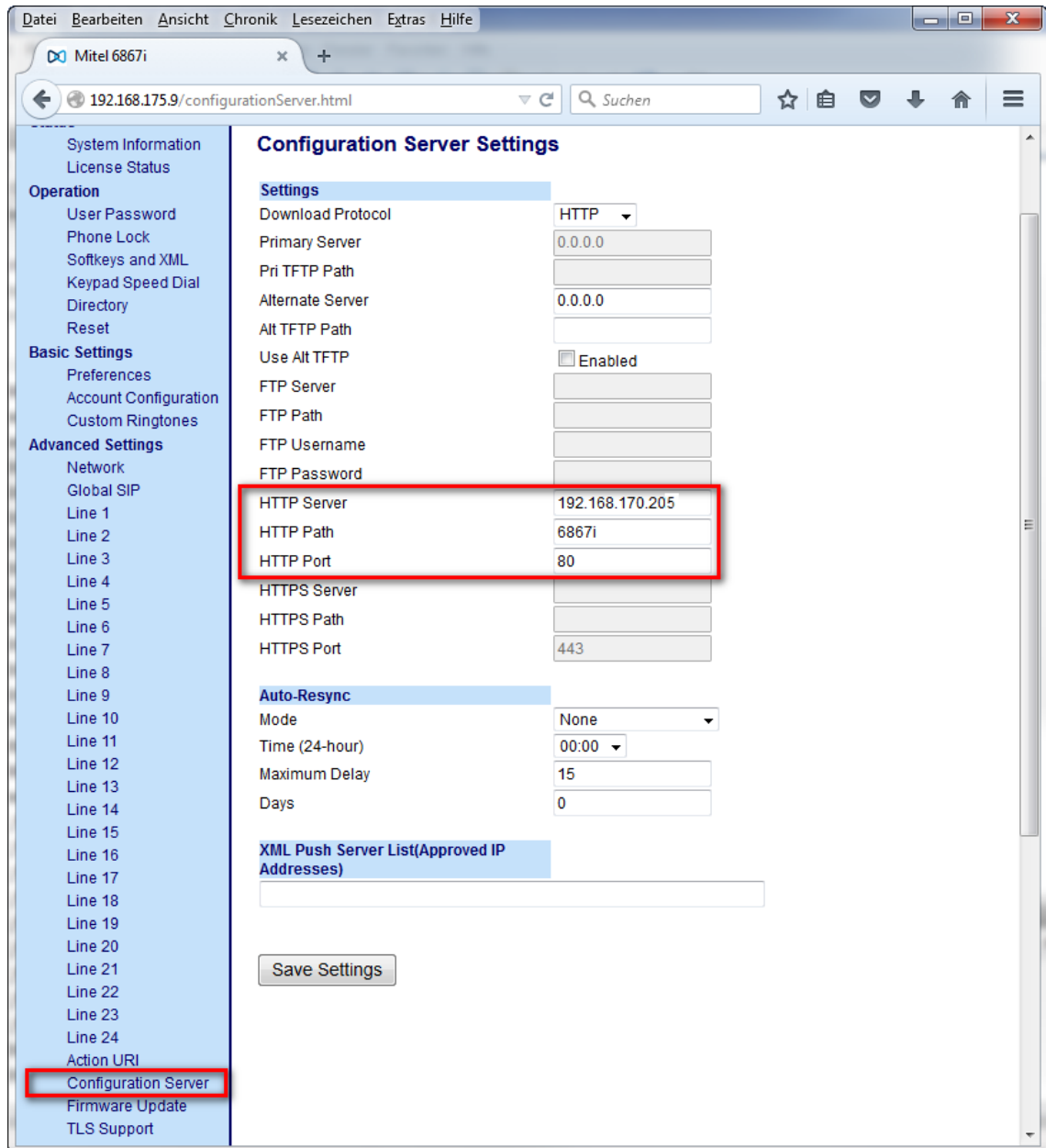


Fig. 4: Check server, path and port

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

7.2

System Configuration



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

7.2.1

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 ad-

dress bar of the browser:

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

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

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

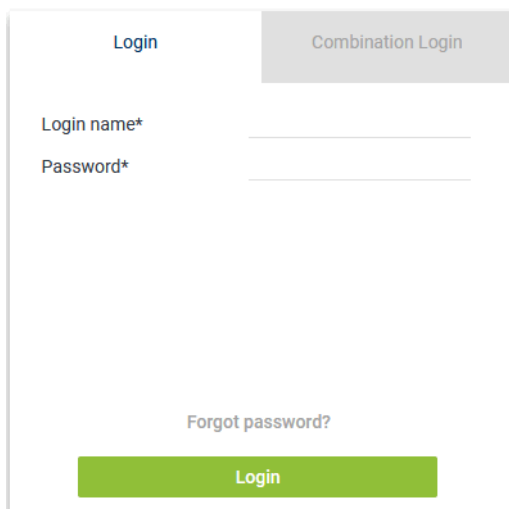


Fig. 5: System Configuration - Web interface

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

Login data for the administrator of the system provider:

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

Tab. 3: Login data - system provider

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

System Configuration X			
<div> <div>SYSTEM PROVIDER</div> <div> <div>Tenants</div> <div>Employees</div> <div>Roles</div> <div>Licensing</div> <div>Setup</div> <div>Drives</div> <div>More</div> <div>Notifications</div> <div>Database Manager</div> </div> </div>			
Name ^	Customer ID ↕	Type	Country ↕
System		System provider	

Fig. 6: System Configuration - main view

7.2.2 Configure recording solution All-in-one Basic

7.2.2.1 Create recording architecture

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

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

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







⇒ The following window appears:

System Configuration X			
<div> <div>SYSTEM PROVIDER</div> <div> <div>Setup</div> <div> <div>Servers</div> <div>Recording Architectures</div> <div>PHONEapp</div> <div>PBX</div> <div>Phones</div> <div>TDM Hardware ASC</div> <div>TDM Hardware Others</div> <div>Integrations</div> <div>Recording Import</div> <div>Additional Data</div> <div>Activity Guard</div> </div> </div> </div>			
Name ↕	Type ↕	Active	S
No records found			

Powered by
 ASC Technologies AG
 v6.9.9-9.9

Rows per page 50 1 - 1 of 1

Fig. 7: Recording architectures - main view

<i>Name</i>	Name of the recording architecture
<i>Type</i>	Type of the recording architecture
<i>Active</i>	Shows whether the recording architecture has been activated and is ready to be used for the recording.  = Recording architecture is active and ready to be used for recording. It can be deactivated by clicking on the icon  (<i>Deactivate</i>) in the toolbar.  = Recording architecture is not active. It can be activated by clicking on the icon  (<i>Activate</i>) in the toolbar.
<i>Standby Active</i>	Shows whether the standby server is active for one or several recording components in the recording architecture.  = At least 1 standby server is active.  = No standby server is active or no standby server has been defined.
<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*.

7.2.2.1.1 Toolbar of the Recording Architectures module

The toolbar offers the following functions.



Fig. 8: 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*.

7.2.2.1.2 Create recording architecture All-in-one Basic

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

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

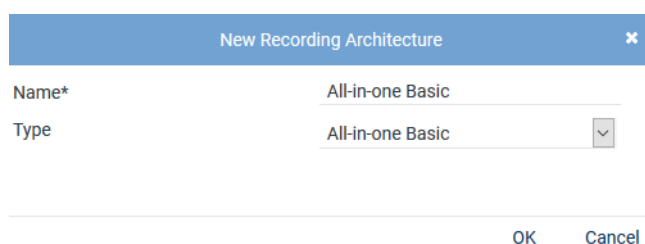
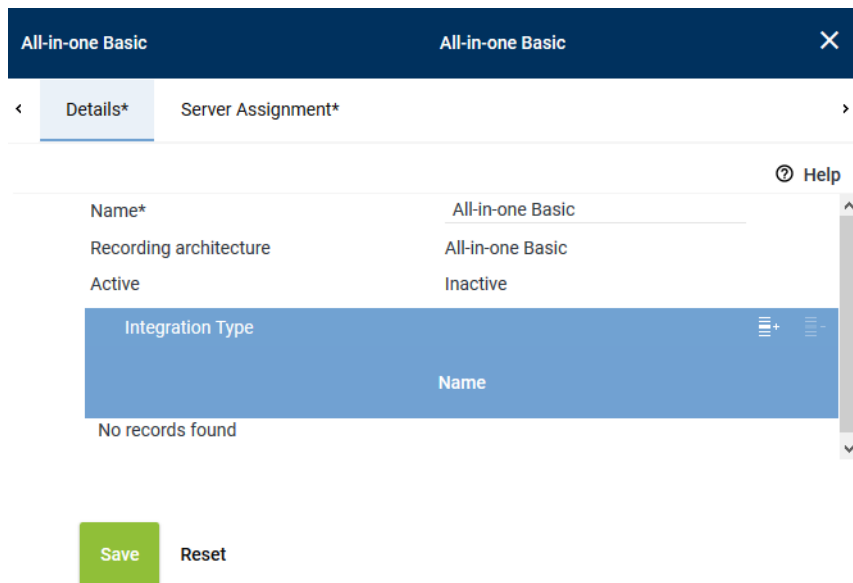


Fig. 9: Create recording architecture - All-in-one Basic Recording

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



All-in-one Basic X

< **Details*** Server Assignment* >

Help

Name* All-in-one Basic

Recording architecture All-in-one Basic


Active Inactive

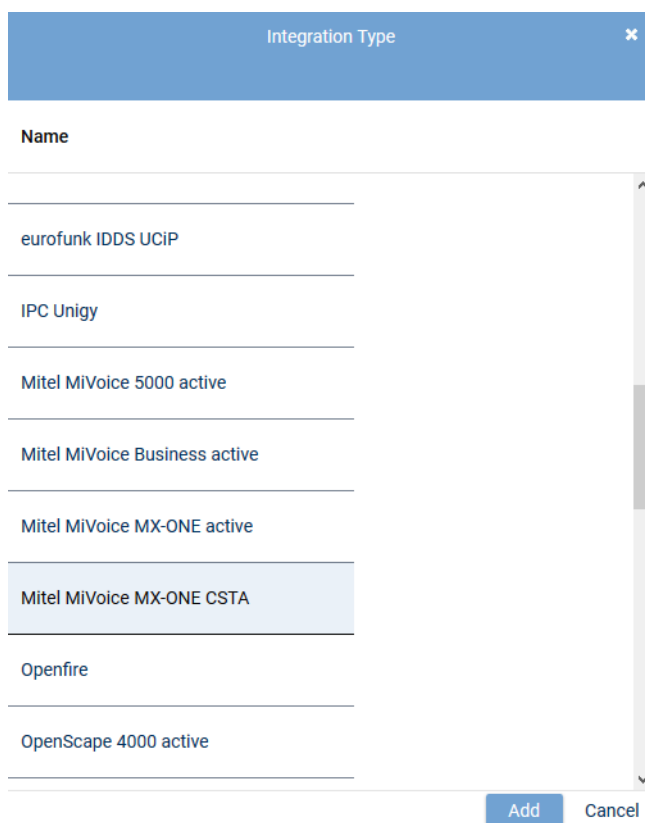
Integration Type	Name
No records found	

Save **Reset**

Fig. 10: 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 X

Name

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

Add **Cancel**

Fig. 11: Select integration type



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



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

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

Assign server for All-in-one Basic

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

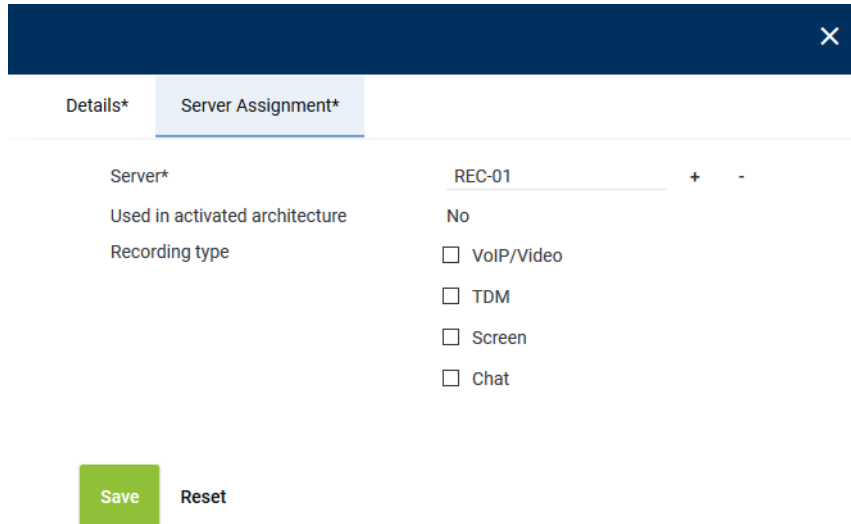


Fig. 12: Recording architecture - tab Server Assignment

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



Fig. 13: 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

Fig. 14: 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. 15: 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.

7.2.2.2

Configure server

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

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

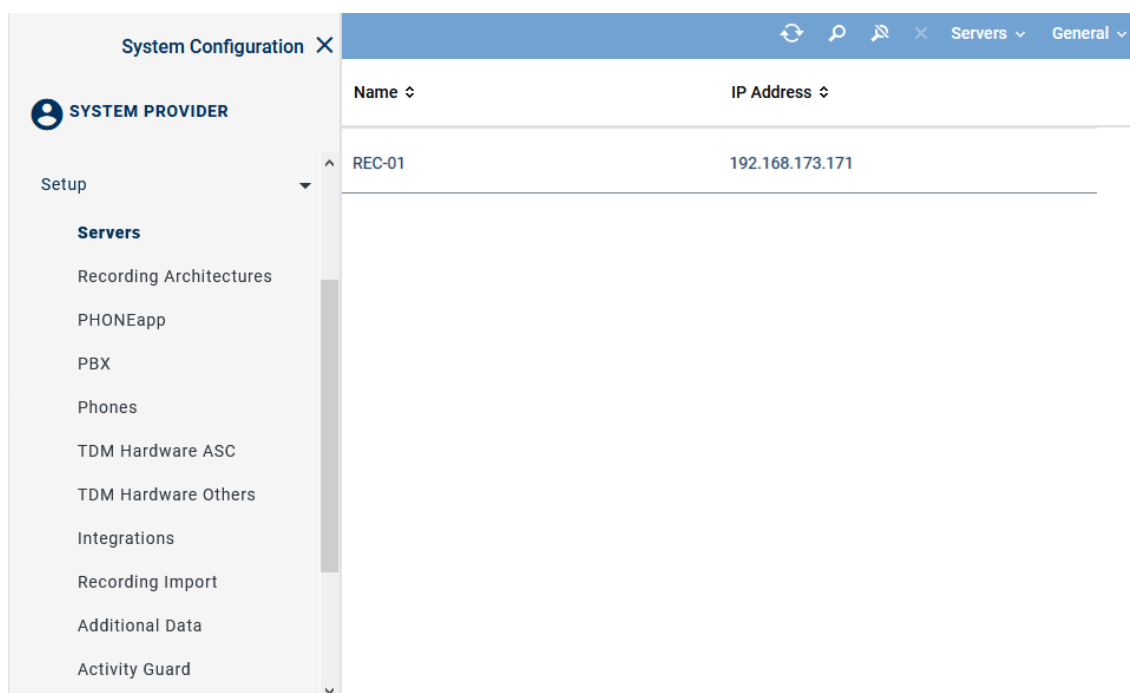


Fig. 16: Servers - main view

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*.

7.2.2.2.1 Toolbar of the Servers module

The toolbar offers the following functions.

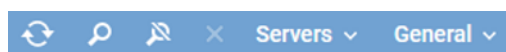







Fig. 17: Toolbar Servers module

	<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.

Server	<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. 22.
	<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.
General	<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*.

7.2.2.2.2 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.

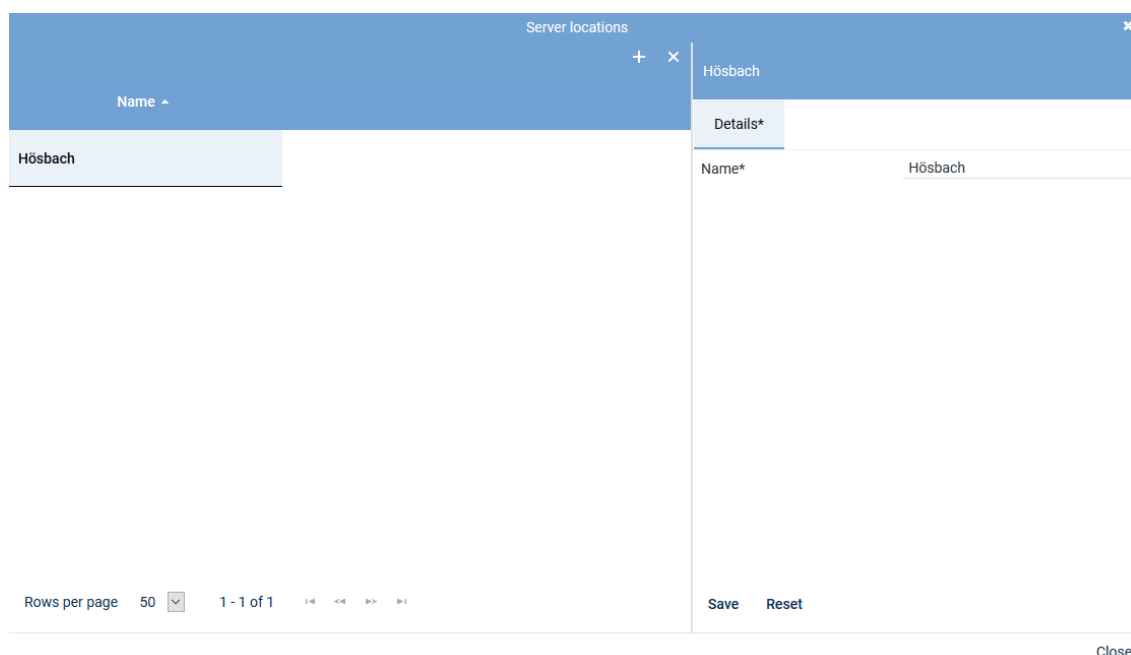



Fig. 18: Add server locations

- 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.

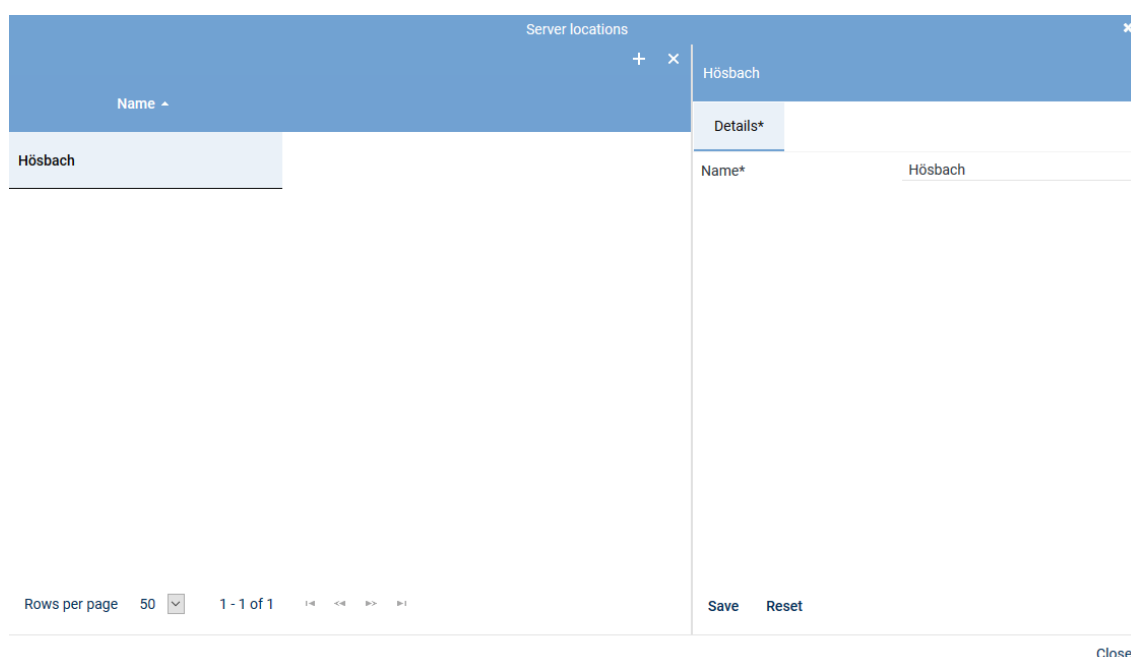



Fig. 19: Delete server location

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*.

7.2.2.2.3 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. 20: 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.

7.2.2.2.4 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. 21: Servers - tab usage

Group field API Server

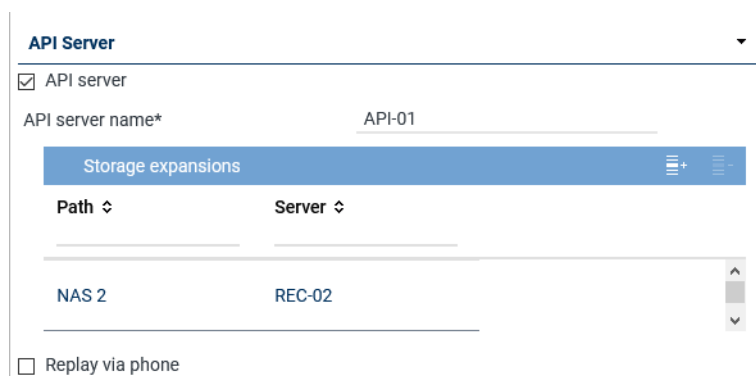




Fig. 22: Group field API Server

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. 35.</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. 26. 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. 33. 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. 23: 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. 24: 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. 4: Configure audio analysis

Emotion Detection ✕

📋

Name ↕

REC-01

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

Add Cancel

Fig. 25: 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. 26: 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. 5: 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. 27: 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. 30. 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. 30. 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. 29: 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. 32.

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. 7: 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.

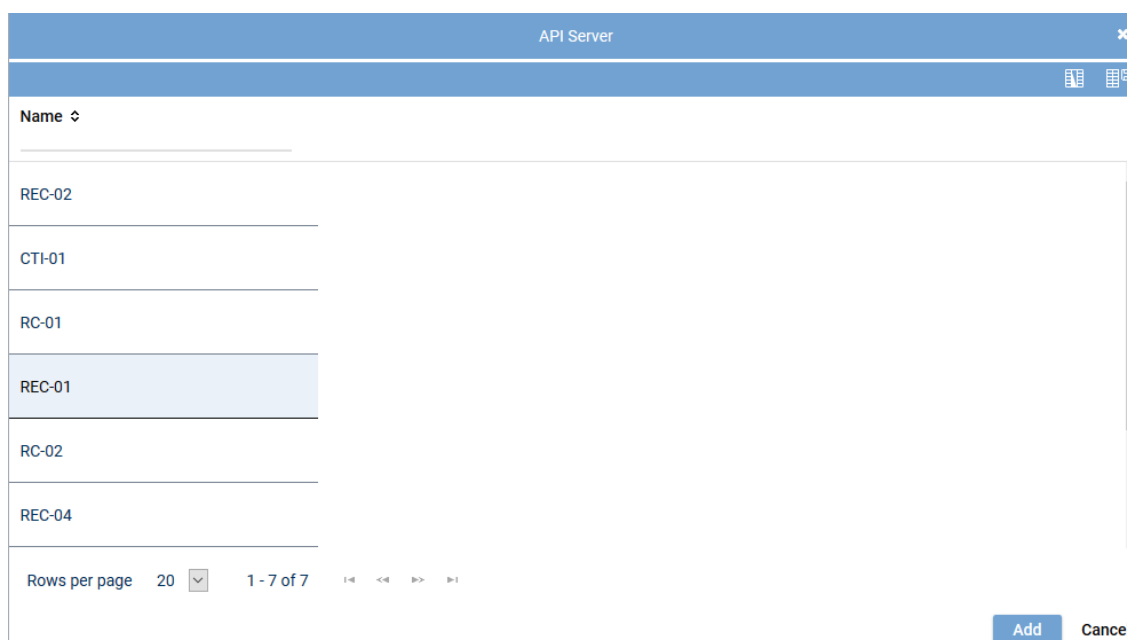


Fig. 30: Select server



Only those servers are available on which the [API](#) service has been installed and activated. See [chapter "Group field API Server", p. 25](#).

- 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. 31: 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. 8: 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.

7.2.2.2.5 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. 32: 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 Registration required.</p>
<i>SIP registration expiration</i>	Enter the time interval after which the registration has to be repeated.

7.2.2.2.6 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. 33: Servers module - tab Replay Server Address Mapping

Group field Replay Server Addresses

1. Enter the following parameters:

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

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



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

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



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



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

7.2.2.2.7 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. 34: 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*.

7.2.2.2.8 Tab Keystore/Virtualization

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

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

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

For key management there are the following options:

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

For licensing, there are the following options:

Without Internet access:

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

- *Trusted Virtualization License*

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

In this case, no separate configuration is required.

With Internet access:

- *ASC License Management System*

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

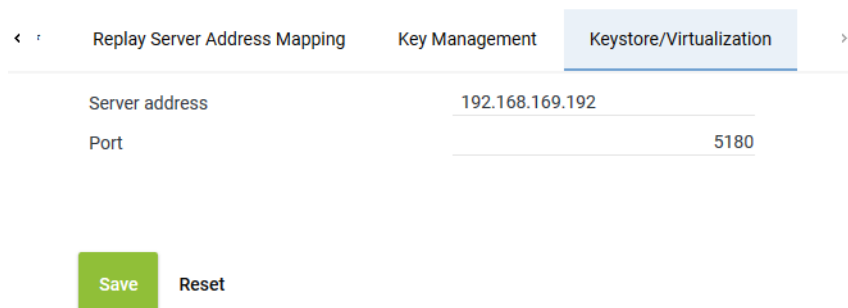


Fig. 35: Servers module - tab Keystore/Virtualization

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*.

7.2.2.3 Create PBX

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

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

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

⇒ The following window appears:

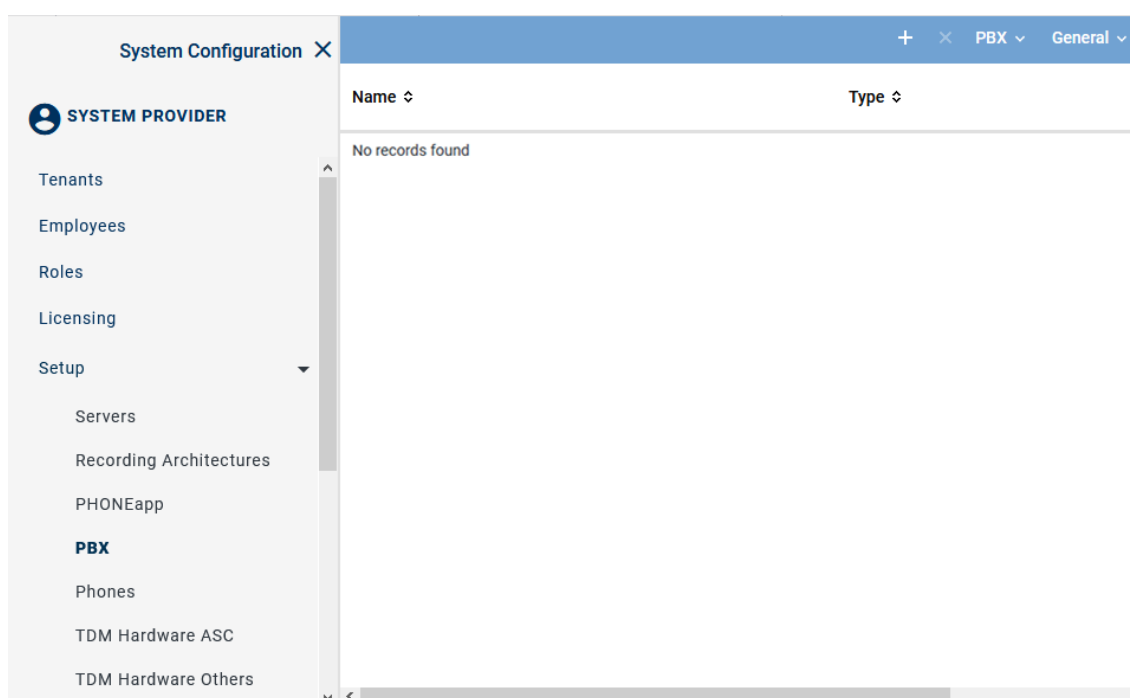


Fig. 36: PBX module - main view

7.2.2.3.1 Toolbar of the PBX module

The toolbar offers the following functions.

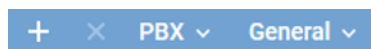





Fig. 37: Toolbar PBX module

	<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*.

7.2.2.3.2 Create new PBX

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

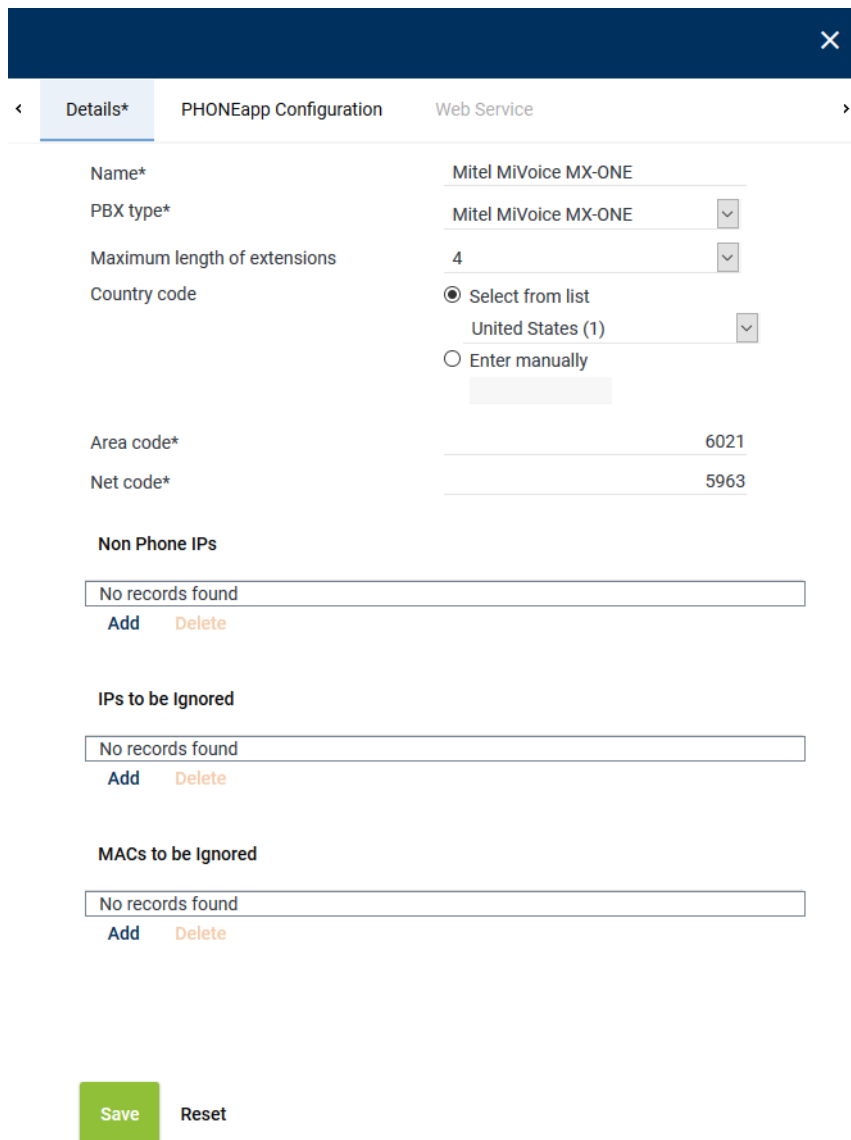


Fig. 38: Create new PBX - tab Details

- 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. 9: Create PBX

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

7.2.2.4 Assign recording resources

Resources for tenants

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

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

Resources for employees

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



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

7.2.2.4.1 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.

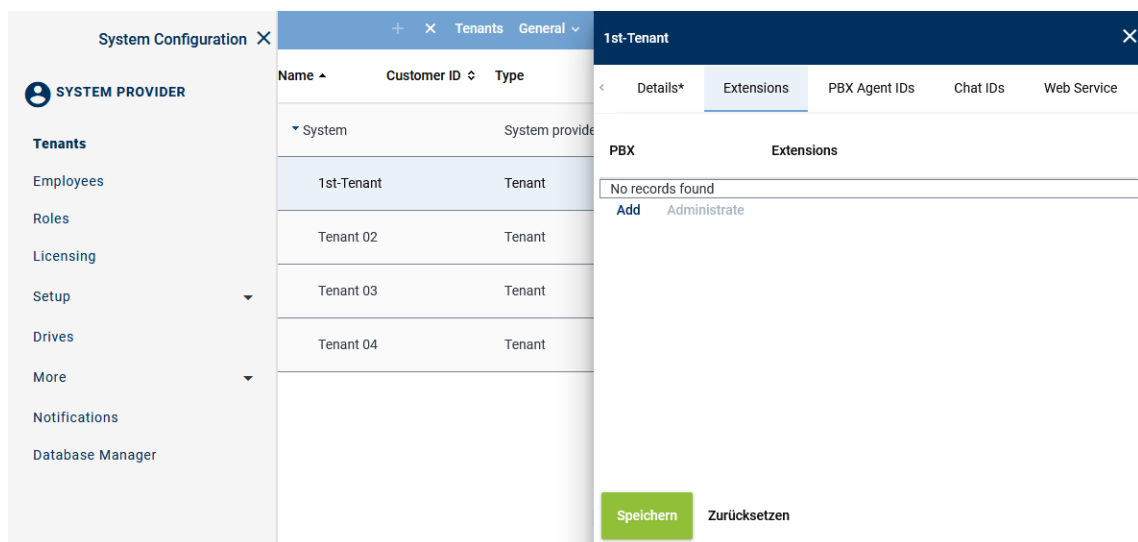


Fig. 39: Tenants - main view - tab Extensions

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. 40: 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} passive for Mitel MiVoice MX-ONE trunk-side recording - Neo 7.x Rev. 3

43 / 68

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.

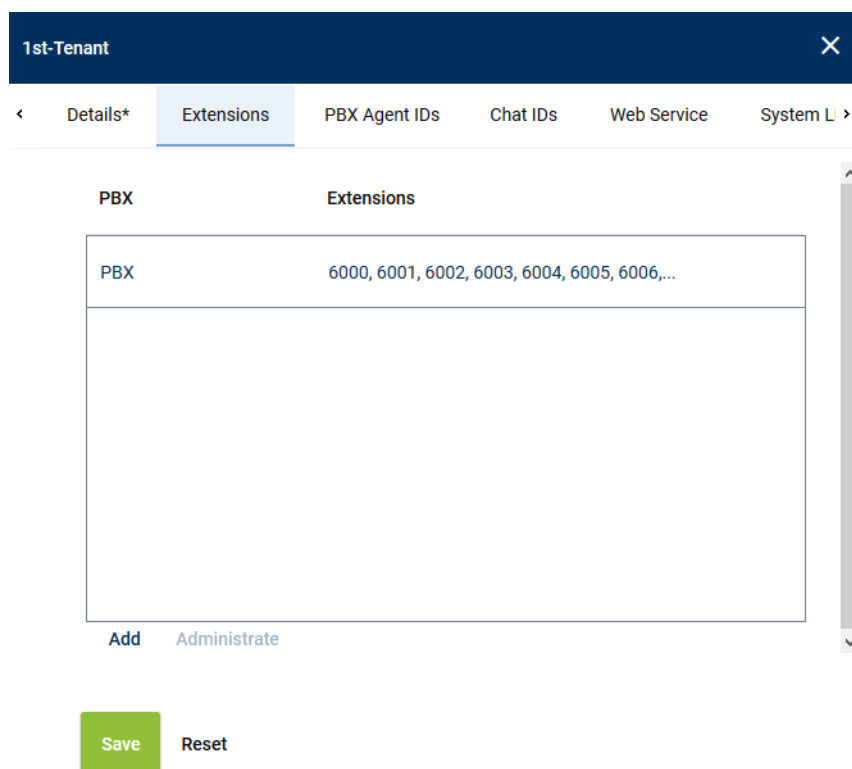


Fig. 41: Remove extensions

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. 42: 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*.

7.2.2.5 Configure additional data

Additional data

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

The recording system differentiates between 2 types of additional data:

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



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

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

The information tagged in CustomCP fields can 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. 43: 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. 44: 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. 45: 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*.

7.2.2.6 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:

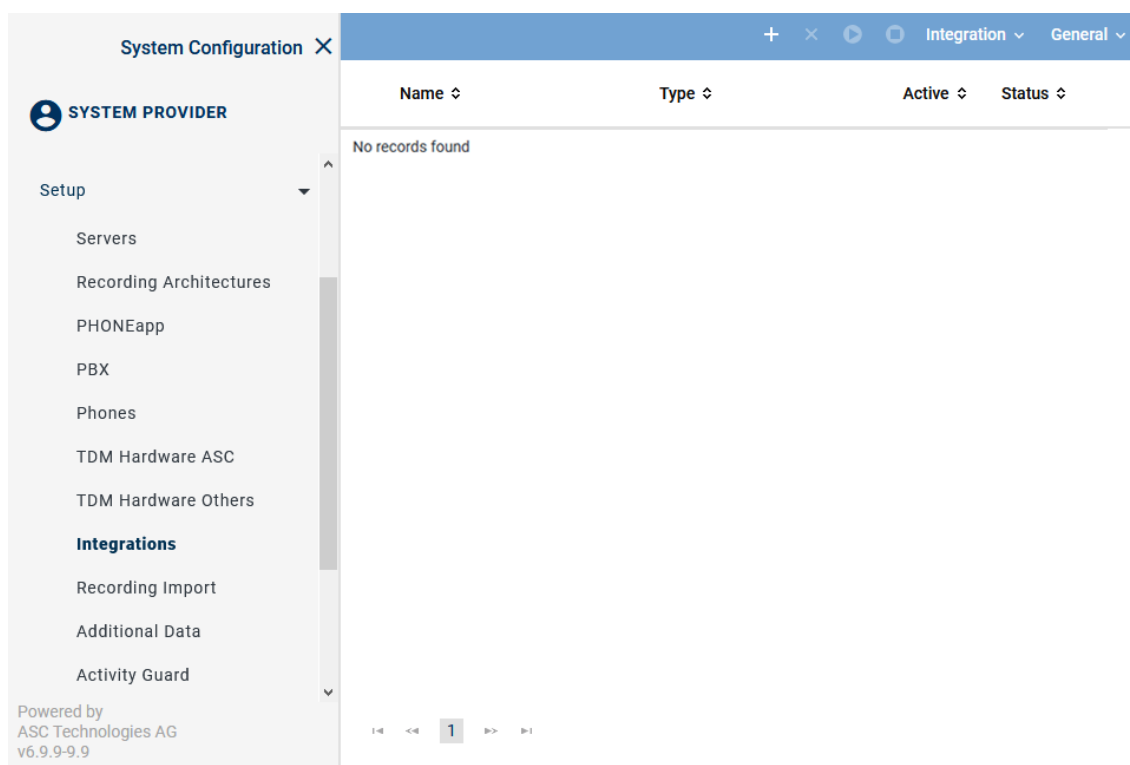




Fig. 46: Integrations - main view

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>

7.2.2.6.1 Toolbar of the Integrations module

The toolbar offers the following functions.



Fig. 47: 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.

7.2.2.6.2 Assign integration type


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




Fig. 48: Create integration type

- Enter the following parameters:

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

Tab. 10: Create integration type

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

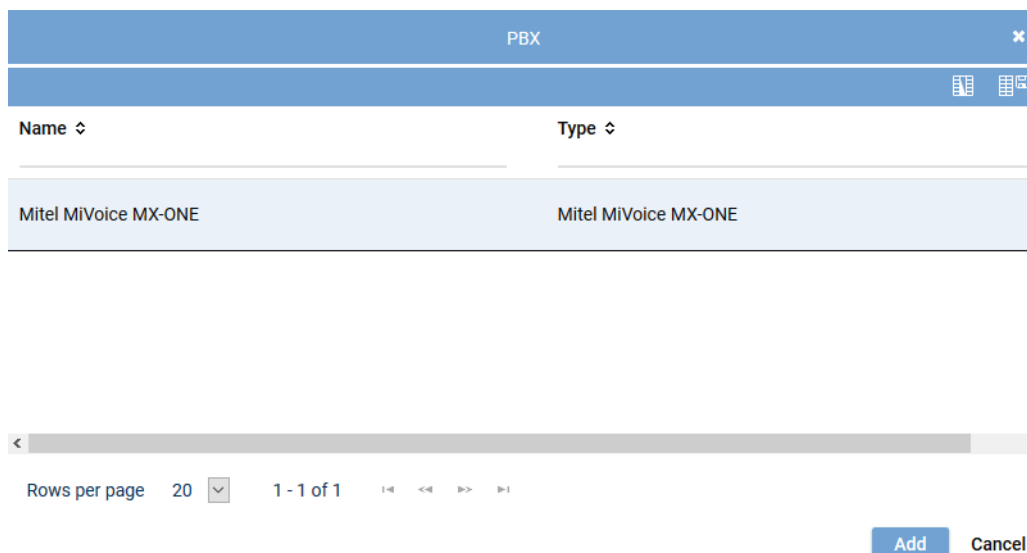


Fig. 49: Integrations - select PBX

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

7.2.2.6.3 Assign recording architecture for All-in-one Basic

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



Fig. 50: 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.

7.2.2.6.4 Configuration steps

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









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

Fig. 51: Configuration steps of the integration

7.2.2.6.5 Configure recording architecture

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

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

Step: Configure Recording Architecture
✕

Details *

Recording architecture*
All-in-one Basic


▼

Save Cancel

Fig. 52: 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.

7.2.2.6.6 Configure CTI connection data

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

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



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



Following an update, you must configure this section again.

Tab MiVoice MX-ONE (CSTA)

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

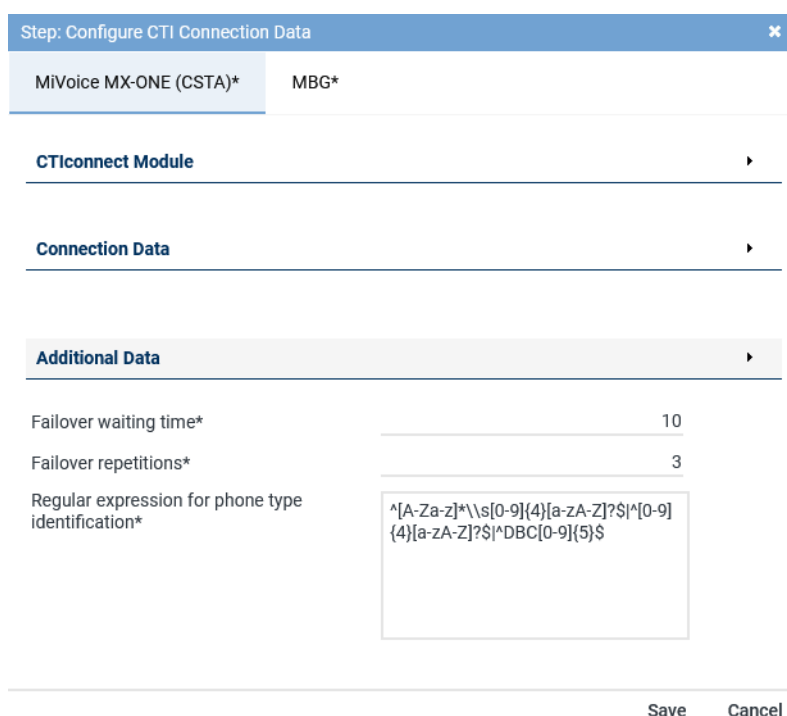


Fig. 53: CTI connection data - tab MiVoice MX-ONE (CSTA)

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

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



Following an update, you must configure this section again.

Group field CTIconnect Module

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

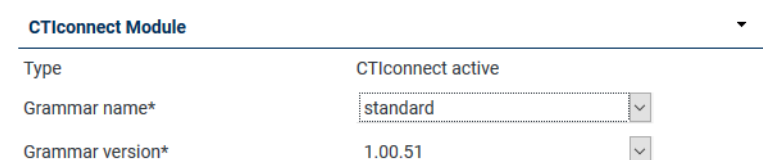


Fig. 54: Configure CTIconnect module

1. Enter the following parameters for the grammar:

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

Tab. 11: Configure CTIconnect module



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

Group field Connection Data MiVoice MX-ONE (CSTA)

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

Connection Data ▼

PBX IP address

No records found

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

Fig. 55: Configure connection data

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

Configure Connection
✕

PBX IP address* 192.168.170.219

PBX CSTA port* 8882

Transport Layer Security (TLS) ☐

☒ Activate authentication

Application ID* 1234

Password* ●●●●●●●●●●●●●●●●

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

Fig. 56: Configure connection data

- Enter the following parameters:

Parameter	Value/Description
PBX IP address	Enter the IP address of the PBX.
PBX CSTA port	Enter the port via which the CSTA connection is supposed to run. Default is <i>TCP 8882</i> , optional for <i>TLS 8883</i> .

Parameter	Value/Description
Transport Layer Security	Activate this check box to use the connection with TLS .

Tab. 12: Configure connection data

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

Group field Additional Data

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

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



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



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



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

Arbitrary assignment

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

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

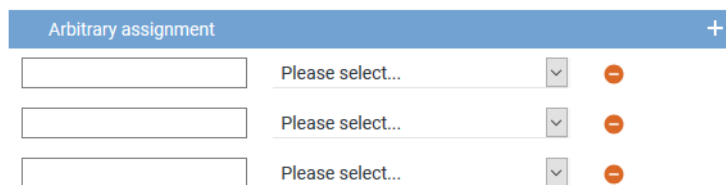



Fig. 57: Group field Additional Data - free assignment of additional data

- Enter the name of the additional data type in the entry field on the left. Observe the exact spelling like it is used in the log file.
- 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.

Tab MBG



Configuring the **MBG** is not required in this recording solution.

7.2.2.6.7

Configure monitor points for MX-ONE CSTA trunk-side recording

In this configuration step, the monitor points of 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.

NOTICE! For trunk-side recording, there is no need to configure extension monitor points. In this case, only the **SIP** trunks are configured.

Tab SIP Trunks

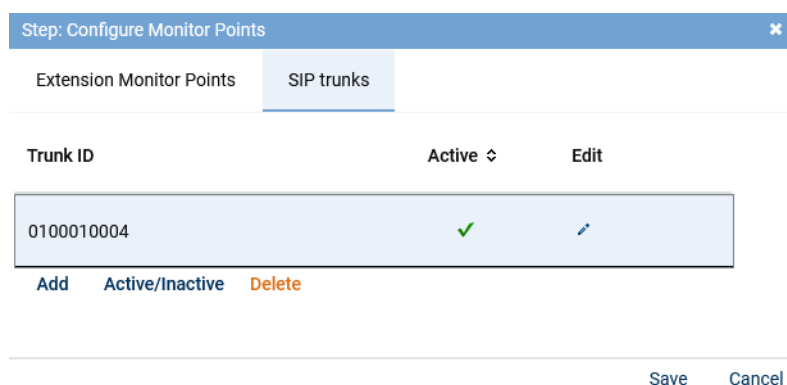
In this tab, you can add, activate, deactivate or remove **SIP** trunks.




As different **SIP** trunks (trunk IDs) may be used, it is advisable to configure all **SIP** trunk IDs configured in the PBX in the recording system so that no information is lost when changing.

1. Click on the button *Add* to add a **SIP** trunk.

⇒ A new row appears.



Trunk ID	Active	Edit
0100010004	✓	

Add Active/Inactive Delete

Save Cancel

Fig. 58: Add SIP trunks

The **SIP** trunk IDs consist of Trunk Line Numbers configured in the **PBX** and are composed as follows:

Layout of a Trunk Line Number

R route number fill with leading zeros, route number 1	RRR = 001
L LIM number fill with leading zeros, LIM 1	LLL = 001
X trunk individual, fill with leading zeros, trunk id 9	XXXX = 0009

Example (Route Number 63)

```
MDSH> roedp:tru=all,rou=63;
ROUTE EQUIPMENT DATA
ROU TRU EQU IP ADDRESS INDDAT CNTRL
```

```
63 001-1 H'000000000000
63 001-2 H'000000000000
63 001-3 H'000000000000
63 001-4 H'000000000000
```

Example (Route Number 63)

```

63 001-5 H'000000000000
63 001-6 H'000000000000
63 001-7 H'000000000000
63 001-8 H'000000000000
63 001-9 H'000000000000
63 001-10 H'000000000000



```

Result:

```

0630010001
0630010002
0630010003
0630010004
0630010005
0630010006
0630010007
0630010008
0630010009
0630010010


```

1. At the end of the row in the column *Edit*, click on the icon .
⇒ The entry mode opens.
2. In the column *Trunk ID*, enter the name of the trunk.
3. Once you have finished editing, click on the icon  at the end of the row to apply the entries.
4. Repeat the process to add further [SIP](#) trunk IDs.
5. To save the entries, click on the button *Save*.
To discard entries, click on the button *Cancel*.

7.2.2.6.8 Global recording settings

Configuring global recording settings such as transport protocol, authentication or registration on the [PBX](#) is not required for trunk-side recording.

7.2.2.6.9 Configure recording servers

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

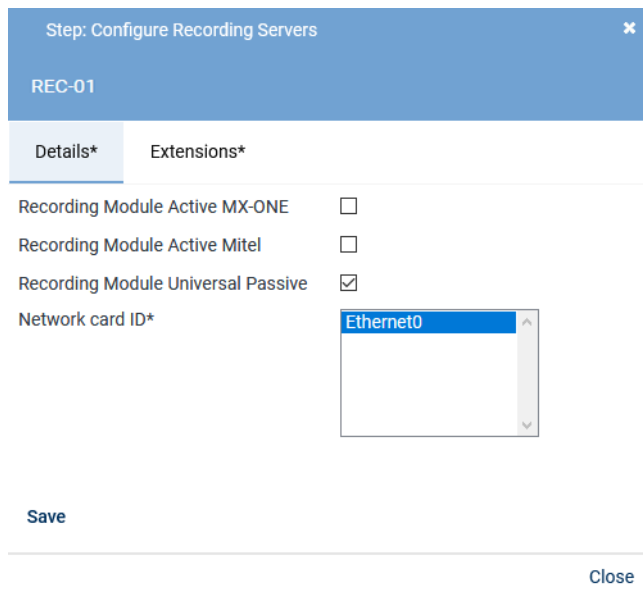


Fig. 59: Configuration step - Configure recording servers

2. *Recording Module Active MX-ONE* is not relevant for this recording solution.
3. *Recording Module Active Mitel* is not relevant for this recording solution.
4. Activate the function *Recording Module Universal Passive* for this recording variant.

Parameter	Value/Description
Network card ID	From the list field, select the network card which is supposed to be used for sniffing RTP audio data.

Tab. 13: Configure recording servers



To avoid that other network traffic interferes with sniffing audio data, a separate network card must have been configured for sniffing which receives only a copy of the audio data of the calls from the **SPAN** port of a network switch that reach the PBX via the trunk. If additional network traffic is sent to the recording server via the **SPAN** port, the system's performance may be severely compromised.

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



If you use several passive integrations in one recording architecture, you must assign a different network card to each recording server in the configuration step *Configure recording servers*.



If a network card for passive VoIP recording is added in a system in a virtualized environment and does not appear in the selection of available network card IDs, then you have to reboot the server.



Following an update, you must configure this section again.

7.2.2.6.10 Configure add-on



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



Add-ons are not supported in this recording solution.


7.2.2.6.11 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.

7.2.2.6.12 Activate integration

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

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

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

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




















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

Fig. 60: Activate integration

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






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

Fig. 61: Activated integration



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



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



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




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



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

7.2.2.6.13 Deactivate/Delete integration

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

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






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

Fig. 62: Deactivate integration

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

7.2.2.7 Adjust Neo configuration file

Some parameters cannot be configured via the graphic interface but have to be adjusted in the configuration files.

7.2.2.7.1 Adjust recording control

Configure trim function

When participant phone numbers can be signaled via different sources with a different number of zeros or a plus sign at the beginning, you can activate the trim function of the Recording Control Service to remove preceding zeros and the plus sign to standardize the format of the phone numbers.

To activate this function, the file *ASC.RecordingControl.ini* must be adjusted.



Deactivate the Recording Control Service before making changes.

- Open the Windows Explorer.
- Change to the installation directory of the recordings software
 \Program Files (x86)\ASC\ASC Product Suite\data\RecordingControl.
- Open the configuration file *ASC.RecordingControl.ini* with the Editor.
- Set the following parameters to 1 to remove an arbitrary number of zeros or a plus sign displayed in front of mobile phone numbers.

Section [RC]

- trimLeadingZeros=1
 - trimLeadingPlus=1
5. Save the changes in the configuration file.
 6. Start the service *ASC RecordingControl* to apply the changes.



For further information about how to adjust the configuration files contact your local ASC support or call ASC support at +49 700 27278776.

7.2.3 Configure Recording Content Validation

Recording Content Validation is an easy and quick possibility to check the functionality of the recording system whenever required. The information is displayed in the Notifications module. Reports can be used to visualize the results.

Preconditions for validation:

- *The license Recording Content Validation must have been installed.*
- *Emotion detection must have been activated in the Servers module.*
- *The server for emotion detection must have been selected.*

Configuration in the Servers module

1. Go to the *Servers module*.
2. In the main view, select the server that you would like to configure.
3. Select the tab *Usage*.
4. Open the group field *Audio Analysis*.

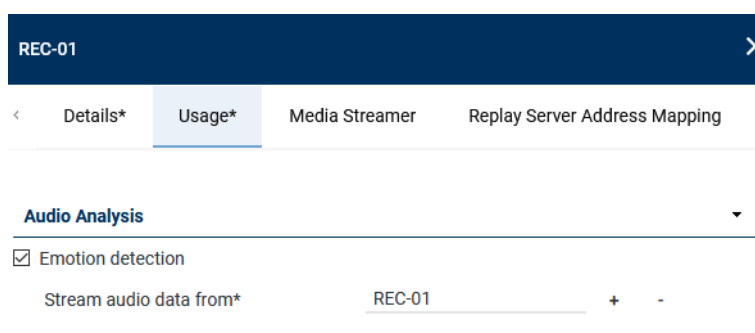


Fig. 63: Servers module - Activate emotion detection

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 the correct functionality of the recording system and the validity of recording content:

- *Packet loss detection*
- *Silence detection*

✕

< Details*
Recording Content Validation
>

Activate packet loss detection ☒

Activate decryption error detection ☐

☒ Activate silence detection

Minimum duration* ms

Threshold value* dB

Silence percentage* %

Weighting*

Emotion detection*

Save

Reset

Fig. 64: Create integration - tab Recording Content Validation

Activate packet loss detection	<input checked="" type="checkbox"/> Activate the check box to check whether packets of a recording have been lost. NOTICE! Packet loss compromises audio quality. If a high percentage of packets is lost, this may result in the total loss of the recording.
Activate decryption error detection	NOTICE! This check is not required in this recording solution.
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! A high percentage of silence sections can indicate a technical problem such as a connection interruption.
<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 extent to which the audio curve (samples) is supposed to be smoothed out. The higher the value, the more signal peaks are smoothed out. Default value is 10. Values of 1-10000 can be recommended.
<i>Emotion detection server</i>	By clicking on the icon <input checked="" type="text" value="+"/> , select the server that emotion detection runs on. The speech analysis software recognizes whether there are silence sections in the recording.

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

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

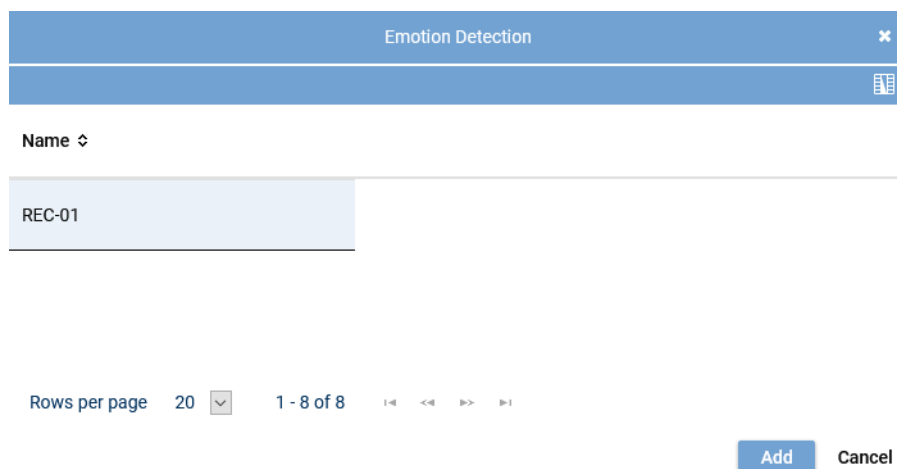


Fig. 65: Select server for emotion detection

4. Click on the button *Add* to apply the selected server.
5. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

Configuration in the Notifications module

To issue notifications in case of an error, the corresponding notifications must be configured in the Notifications module.



For basic information about the Notifications module refer to the administration manual for tenants *Notifications module*.

Configuration in the application INSIGHT_{neo}

To issue a report visualizing the errors occurred, a report must be created in the application INSIGHT_{neo}.



For information about using the Report Templates module and the Report Instances module refer to the respective INSIGHT_{neo} user manuals.

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.

If no recording is possible, check:

- whether the correct network card has been selected in System Configuration, see [chapter "Configure server", p. 20](#).
- the correct installation of the [SPAN](#) port

When opening a ticket, 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, MAC IP address of the affected device
- manufacturer, type, and software version of the PBX
- Wireshark traces of the recording network interface

Log level settings

Module	Log level
RECORDING_CONTROL	DEBUG
RECORDING_MODULE_MANAGER	DEBUG
API_SERVER	DEBUG
FILE_MANAGER	DEBUG

List of figures

Fig. 1	Recording solution EVOIP\$neo\$ passive for Mitel MiVoice MX-ONE trunk-side recording	5
Fig. 2	Configure CSTA server.....	11
Fig. 3	Check license status.....	12
Fig. 4	Check server, path and port	13
Fig. 5	System Configuration - Web interface	14
Fig. 6	System Configuration - main view	15
Fig. 7	Recording architectures - main view.....	15
Fig. 8	Toolbar Recording Architectures module	16
Fig. 9	Create recording architecture - All-in-one Basic Recording.....	17
Fig. 10	Recording architecture - tab Details	18
Fig. 11	Select integration type	18
Fig. 12	Recording architecture - tab Server Assignment	19
Fig. 13	Recording architecture - assign server	19
Fig. 14	Recording architecture - activate recording variant	20
Fig. 15	Recording architecture - activate recording architecture	20
Fig. 16	Servers - main view	21
Fig. 17	Toolbar Servers module	21
Fig. 18	Add server locations	22
Fig. 19	Delete server location	23
Fig. 20	Servers - tab Details	24
Fig. 21	Servers - tab usage	24
Fig. 22	Group field API Server.....	25
Fig. 23	Select storage expansion	26
Fig. 24	Group field Audio Analysis.....	27
Fig. 25	Select server for emotion detection	27
Fig. 26	Group field Recording Control/Key Management.....	27
Fig. 27	Group field Data Processing.....	28
Fig. 28	Select server.....	30
Fig. 29	Group field Replay	31
Fig. 30	Select server.....	32
Fig. 31	Group field Virtualization.....	33
Fig. 32	Servers module - tab Media Streamer.....	34
Fig. 33	Servers module - tab Replay Server Address Mapping.....	35
Fig. 34	Servers module - tab Key Management	37
Fig. 35	Servers module - tab Keystore/Virtualization	39
Fig. 36	PBX module - main view.....	40
Fig. 37	Toolbar PBX module.....	40
Fig. 38	Create new PBX - tab Details	41
Fig. 39	Tenants - main view - tab Extensions.....	42
Fig. 40	Assign extensions to tenants.....	43

Fig. 41	Remove extensions	44
Fig. 42	Select extensions.....	45
Fig. 43	Additional Data module main view.....	46
Fig. 44	Configure additional data.....	46
Fig. 45	Additional data - configure availability	47
Fig. 46	Integrations - main view	48
Fig. 47	Toolbar Integrations module	48
Fig. 48	Create integration type	49
Fig. 49	Integrations - select PBX	49
Fig. 50	Assign recording architecture - All-in-one Basic	50
Fig. 51	Configuration steps of the integration	51
Fig. 52	Configuration step - Configure Recording Architecture	51
Fig. 53	CTI connection data - tab MiVoice MX-ONE (CSTA)	52
Fig. 54	Configure CTIconnect module	52
Fig. 55	Configure connection data	53
Fig. 56	Configure connection data	53
Fig. 57	Group field Additional Data - free assignment of additional data.....	54
Fig. 58	Add SIP trunks.....	55
Fig. 59	Configuration step - Configure recording servers	57
Fig. 60	Activate integration	58
Fig. 61	Activated integration	58
Fig. 62	Deactivate integration	59
Fig. 63	Servers module - Activate emotion detection	60
Fig. 64	Create integration - tab Recording Content Validation	61
Fig. 65	Select server for emotion detection	62

List of tables

Tab. 1	Licenses for recording server	8
Tab. 2	Licenses for recording with Mitel MiVoice MX-ONE	8
Tab. 3	Login data - system provider	14
Tab. 4	Configure audio analysis	27
Tab. 5	Configure recording control/key management.....	28
Tab. 6	Data storage	28
Tab. 7	Configure replay	31
Tab. 8	Configure virtualization	33
Tab. 9	Create PBX.....	41
Tab. 10	Create integration type	49
Tab. 11	Configure CTIconnect module	53
Tab. 12	Configure connection data.....	53
Tab. 13	Configure recording servers	57

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.

CTI

Computer Telephony Integration

DNS

Domain Name System is a worldwide directory service which administrates the name domain of the Internet. It main task is to answer the queries regarding name resolutions. (Source: Wikipedia 5th April 2017)

IP

Internet Protocol, basic protocol for Internet communication

LCR

Last Conversation Repeat

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

SPAN

Switched Port Analyzing

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