

# System Configuration

## User management



## Administration manual

### for tenants

2/24/2021

### Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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

Copyright © 2021 ASC Technologies AG. All rights reserved.

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



## Contents

<b>1</b>	<b>General information .....</b>	<b>6</b>
<b>2</b>	<b>Introduction .....</b>	<b>7</b>
<b>3</b>	<b>LDAP .....</b>	<b>9</b>
3.1	Install certificate .....	9
3.2	Troubleshooting .....	10
<b>4</b>	<b>Tenants module.....</b>	<b>11</b>
4.1	Main view .....	11
4.1.1	Toolbar .....	11
4.2	Detail view.....	11
4.2.1	Tab Details .....	12
4.2.1.1	Add time zone .....	14
4.2.1.2	Group field System Availability.....	15
4.2.1.3	Group field Address .....	16
4.2.1.4	Group field Contact Person.....	16
4.2.2	Tab Passwords .....	17
4.2.2.1	Edit entry .....	21
4.2.3	Tab General Settings .....	22
4.2.3.1	Group field Inactivity.....	22
4.2.3.2	Group field SMTP Account.....	23
4.2.3.3	Group field LDAP Authentication .....	24
4.2.3.4	Group field Miscellaneous Settings.....	25
4.2.3.5	Group field Random Search of Sessions .....	25
4.2.3.6	Group field Terms of Use .....	26
4.2.4	Tab Key Management.....	26
4.2.5	Tab LDAP Connection Data.....	27
4.2.5.1	Edit LDAP connection data .....	28
4.2.6	Tab Web Service.....	28
<b>5</b>	<b>Employees module .....</b>	<b>31</b>
5.1	Main view .....	31
5.1.1	Toolbar .....	32
5.1.1.1	Show summary .....	33
5.1.1.2	Show locked employees .....	34
5.1.1.3	Make employee visible or not visible.....	34
5.1.1.4	Search.....	34
5.2	Detail view.....	35
5.2.1	Tab Details .....	36
5.2.1.1	Group field Employee Information.....	36
5.2.1.2	Group field Address .....	39
5.2.2	Tab Agent Data .....	40

5.2.2.1	Group field Telephony .....	40
5.2.2.2	Group field Chat .....	42
5.2.2.3	Group field Miscellaneous Settings .....	42
5.2.3	Tab Account .....	43
5.2.3.1	Authentication via LDAP .....	45
5.2.3.2	Assign combination user .....	45
5.2.3.3	Delete combination user assignment .....	46
5.2.4	Tab Settings .....	47
5.2.4.1	Group field Permissions .....	47
5.2.4.2	Group field Logging Settings .....	49
5.2.4.3	Group field Settings for Session Release .....	49
5.2.5	Tab Roles .....	51
5.2.5.1	Assign roles .....	52
5.2.5.2	Delete role assignment .....	53
5.2.6	Tab Individual Function Rights .....	53
5.2.7	Tab Conversation Rules .....	56
5.2.7.1	Assign conversation rules .....	57
5.2.7.2	Delete conversation rule assignment .....	58
5.2.8	Tab Organization Units .....	58
5.2.8.1	Assign organization units .....	59
5.2.8.2	Delete organization unit assignment .....	60
5.3	Create new employee .....	60
5.4	Edit employee .....	61
5.5	Delete employee .....	61
5.6	Create new employee with OAuth login .....	61
<b>6</b>	<b>Organization Structure module .....</b>	<b>63</b>
6.1	Main view .....	63
6.1.1	Toolbar .....	63
6.2	Detail view .....	64
6.2.1	Tab Details .....	65
6.2.2	Tab Members .....	65
6.2.2.1	Assign members .....	65
6.2.2.2	Delete member assignment .....	66
6.2.3	Tab Superiors .....	66
6.2.3.1	Assign superiors .....	67
6.2.3.2	Delete superior assignment .....	67
6.2.4	Tab Member Roles .....	67
6.2.5	Tab Superior Roles .....	68
6.3	Create new organization unit .....	68
6.4	Edit organization unit .....	69
6.5	Delete organization unit .....	69
<b>7</b>	<b>Roles module .....</b>	<b>70</b>

7.1	Main view .....	70
7.1.1	Toolbar .....	71
7.2	Detail view .....	72
7.2.1	Tab Details .....	72
7.2.2	Tab Employees .....	73
7.2.2.1	Assign users .....	73
7.2.2.2	Delete user assignment .....	74
7.2.3	Tab Function Rights .....	74
7.2.4	Tab Conversation Rules .....	76
7.2.4.1	Assign conversation rules .....	76
7.2.4.2	Delete conversation rule assignment .....	77
7.3	Create new role .....	77
7.4	Duplicate role .....	78
7.5	Edit role .....	79
7.6	Delete role .....	79
<b>8</b>	<b>Conversation Rules module .....</b>	<b>80</b>
8.1	Main view .....	81
8.1.1	Toolbar .....	81
8.2	Detail view .....	82
8.2.1	Define filter criteria .....	83
8.2.2	Tab Details .....	84
8.2.3	Tab Conversation Criteria .....	84
8.2.4	Tab Participant View Criteria .....	87
8.2.5	Tab Session Criteria .....	89
8.2.6	Tab Mapping .....	91
8.3	Create new conversation rule .....	91
8.4	Edit conversation rule .....	92
8.5	Delete conversation rule .....	93
<b>9</b>	<b>Predefined function packages .....</b>	<b>94</b>
9.1	Create agent .....	94
9.2	Create supervisor .....	95
9.3	Create superior .....	95
9.4	Create Coaching Advisor .....	95
9.5	Create superuser .....	96
	<b>List of figures .....</b>	<b>98</b>
	<b>List of tables .....</b>	<b>102</b>
	<b>Glossary .....</b>	<b>103</b>

## 1 General information

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

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

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

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

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

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

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

## 2 Introduction

The *neo* system has been designed as a potential multi-tenant system. This means several different tenants can be administered within one system. These tenants are created and administered by the system provider. The administrators of the particular tenants have the possibility to create users, define roles, and administrate access rights.

This manual describes how you as tenant can carry out the following configurations:

- Create and administrate own users
- Administrate function rights for your own users
- Edit your own tenant data

The different functions of the user management are executed in the following modules of the application System Configuration:

- Tenants module  
In the Tenants module, you can administrate your own tenant data.  
See [chapter "Tenants module", p. 11.](#)
- Employees module  
In the Employees module, you can create users, administrate their data, and assign function rights.  
See [chapter "Employees module", p. 31.](#)
- Roles module  
In the Roles module, you can define different roles which allow you to assign users function rights by means of a role system.  
See [chapter "Roles module", p. 70.](#)
- Organization Structure module  
In the Organization Structure module, you can create an organization structure where the users of the system have been assigned to the different organization units.  
See [chapter "Organization Structure module", p. 63.](#)
- Conversation Rules module  
In the Conversation Rules module, you can create conversation rules which are used as filters. By means of the conversation rules, you can define which users may see which conversations.  
See [chapter "Conversation Rules module", p. 80.](#)



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



You can either assign roles to a user (in the Employees module) or users to a role (in the Roles module). Both approaches have the effect that users receive the function rights of the role.



In the Employees module, you can add individual function rights to the scope of function rights assigned to users via a role.



---

When changing the users' function rights, their assigned roles or conversation rules while they are logged in, this change only comes into effect after the users have logged off and in again. Users are not notified when their function rights, roles or conversation rules have been changed.

---



---

Your system provider creates an account for you as administrator of a tenant which has to be used to log in to the application System Configuration. You will receive your login data from your system provider.

---



The product line *neo* supports the authentication of users via **LDAP** (Lightweight Directory Access Protocol).

To be able to use the feature **LDAP**, at least 1 configured **LDAP** server (e. g. an active directory) has to be available where the users have been created who are supposed to be able to use the *neo* recording system. All those who are supposed to use the recording system have to have a *user* profile. They may exist in any combination of directories within the **LDAP** server.

To use the authentication via **LDAP**, you first have to configure all connections to possible **LDAP** servers in the Tenants module and activate the basic **LDAP** authentication. When configuring individual users, you can then decide whether the user is supposed to log in via **LDAP**.

- Configure **LDAP** connection data.  
See chapter "Tab LDAP Connection Data", p. 27.
- Always activate **LDAP** authentication.  
See chapter "Group field LDAP Authentication", p. 24.
- Activate **LDAP** authentication for individual users.  
See chapter "Authentication via LDAP", p. 45.



To be able to successfully log in on the **LDAP** server, the authentication method *Simple Authentication* must have been configured on the **LDAP** server.



If authentication via **LDAP** is active for a user and if this authentication is not successful (e. g. since the **LDAP** server cannot be reached or the combination of login name and password is not correct), a local authentication will take place on the basis of the information saved in the database of the recording system. For this reason, users have to enter a local password in the Employees module, although the **LDAP** authentication has been activated.




To connect to the **LDAP** server, you can use the encryption protocol Secure Sockets Layer (**SSL**).

### 3.1

#### Install certificate

To be able to use an encrypted connection, you have to install the respective certificate on the recording server. To do so, use ASC's *Certificate Import Tool*.

1. Open the Windows Explorer.
2. Change to the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts\*.
3. Execute the file *certimporter.exe* as administrator.
4. Select the menu item *HTTPS Trust* in the navigation bar.
5. Select the tab *Import Trusted Certificate*.
6. Click on the button  behind the field *Certificate X.509*.
7. Select the respective certificate from the Explorer dialog and click on the button *Open*.
8. Click on the button *Import* to install the certificate.
9. A success message appears once the certificate have been imported successfully.
10. Restart the *Glassfish server (Enterprise Core)* so that the certificate will be applied.

## 3.2

## Troubleshooting

**LDAP SSL connection does not work**

The certificate that you install on the recording server must be the same certificate as on the LDAP server. When using different certificates, a connection cannot be established. As a result, you will not be able to use LDAP SSL.

## 4 Tenants module

In the Tenants module, you can administrate the following information and settings:

- Contact data for the system provider
- Password rules for the user of the system in your environment
- General settings for the usage of the system in your environment

Open the Tenants module by clicking on the menu item *Tenants* in the navigation bar of the application System Configuration.

### 4.1 Main view

In the main view, your contact data is displayed in the same way they are displayed for your system provider.

If you change the contact data, the information is automatically updated for your system provider.

Tenants General ▾					
Name ▴	Customer ID ▾	Type	Country ▾	Creation Date ▾	Updated ▾
1st-Tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM

Fig. 1: Tenants module - main view

<i>Name</i>	Name which is displayed for the tenant in the system.
<i>Customer ID</i>	Name of the tenant.
<i>Type</i>	Type of tenant. <ul style="list-style-type: none"> <li>• Tenant</li> <li>• Reseller</li> </ul>
<i>Country</i>	Country of the tenant's address.
<i>Creation Date</i>	Date on which the tenant was created.
<i>Updated</i>	Date on which the tenant's information was updated for the last time.

#### 4.1.1 Toolbar

The toolbar offers the following functions.

Tenants	General ▾
---------	-----------

Fig. 2: Tenants module - toolbar

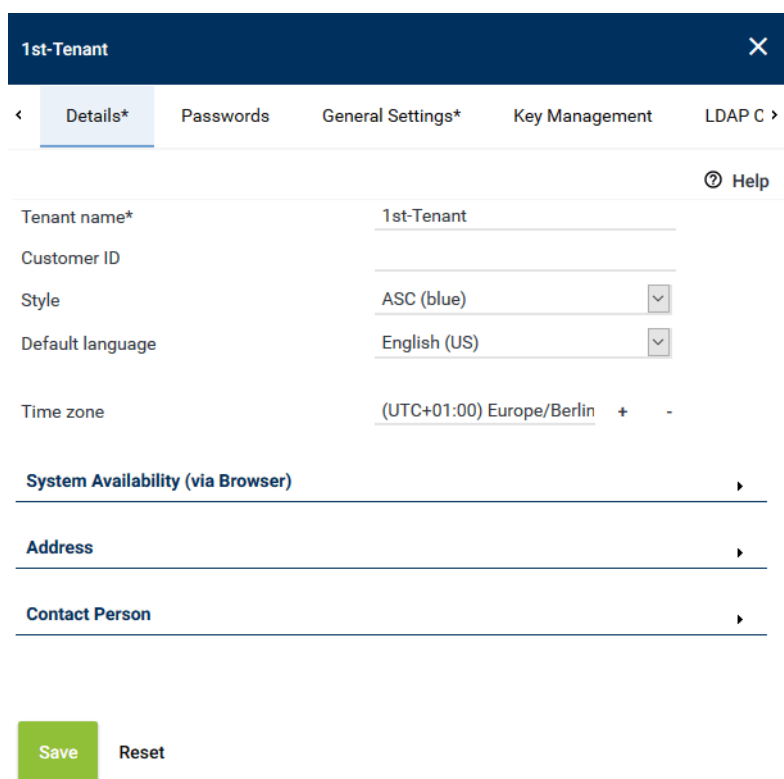
<i>Tenants</i>	This menu is currently not available	
<i>General</i>	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



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

### 4.2 Detail view

The detail view contains additional information about and functions of your tenant account.



The screenshot shows the '1st-Tenant' detail view. At the top, there's a dark blue header with the tenant name and a close button. Below it, a horizontal tab bar contains 'Details\*' (selected), 'Passwords', 'General Settings\*', 'Key Management', and 'LDAP C'. The main content area has a 'Help' icon. The form fields are as follows:

Tenant name*	1st-Tenant
Customer ID	
Style	ASC (blue) [dropdown arrow]
Default language	English (US) [dropdown arrow]
Time zone	(UTC+01:00) Europe/Berlin + -

Below the form, there are three expandable sections: 'System Availability (via Browser)', 'Address', and 'Contact Person', each with a right-pointing arrow. At the bottom left, there are two buttons: a green 'Save' button and a grey 'Reset' button.

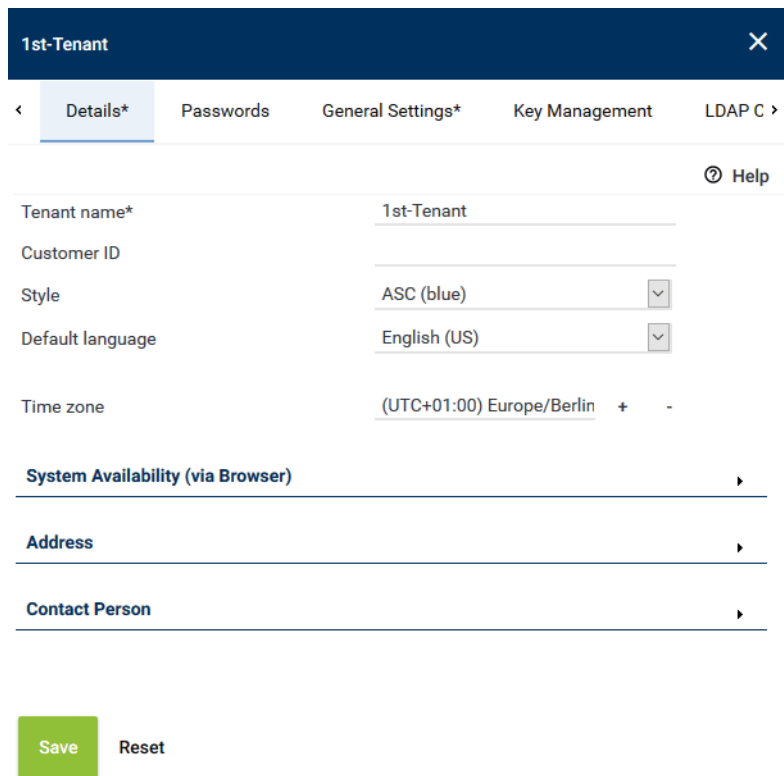
Fig. 3: Tenants module - detail view

The detail view consists of the following tabs:

- *Details*  
Here, you can display and edit your contact data for the system provider.  
See [chapter "Tab Details", p. 12.](#)
- *Passwords*  
Here, you can define the password rules which have to be observed by the users when creating a password.  
See [chapter "Tab Passwords", p. 17.](#)
- *General Settings*  
Here, you can configure the general settings (inactivity, notification settings, [LDAP](#) login).  
See [chapter "Tab General Settings", p. 22.](#)
- *Key management*  
Here, you can define the method which is supposed to be used to encrypt the conversations.  
See [chapter "Tab Key Management", p. 26.](#)
- *LDAP Connection Data*  
Here, you can configure [LDAP](#) connections.  
See [chapter "Tab LDAP Connection Data", p. 27.](#)
- *Web Service*  
Here, you can configure the usage of the Web Service.  
See [chapter "Tab Web Service", p. 28.](#)

#### 4.2.1 Tab Details



Here, you can display and edit your contact data for the system provider.



The screenshot shows the '1st-Tenant' configuration window. It has a dark blue header with a close button (X). Below the header is a tab bar with 'Details\*' (selected), 'Passwords', 'General Settings\*', 'Key Management', and 'LDAP C >'. The main area contains several input fields: 'Tenant name\*' (filled with '1st-Tenant'), 'Customer ID' (empty), 'Style' (dropdown menu showing 'ASC (blue)'), 'Default language' (dropdown menu showing 'English (US)'), and 'Time zone' (text field showing '(UTC+01:00) Europe/Berlin' with '+' and '-' buttons). Below these fields are three expandable sections: 'System Availability (via Browser)', 'Address', and 'Contact Person', each with a right-pointing arrow. At the bottom left are two buttons: a green 'Save' button and a grey 'Reset' button. A 'Help' icon and text are in the top right corner.

Fig. 4: Tenants module - tab Details

1. In the general section, you can adjust the following information:


<i>Tenant name</i>	Your name as tenant.
<i>Customer ID</i>	Enter the customer ID.
<i>Style</i>	Layout in which the tenant sees the user interface of the system. Select one of the available layouts from the drop-down list.
<i>Default language</i>	Language in which the user interface of the system is displayed in your environment. Select the language from the drop-down list.
<i>Time zone</i>	Shows the time zone in which the conversations are supposed to be displayed in the replay applications. This time zone is defined as a pre-setting for all other, newly created employees. If required, you can edit the time zone for each individual employee. The configuration in the Employees module is prioritized.  To select the time zone, click on the button  . See <a href="#">chapter "Add time zone", p. 14</a> .  To delete the selection, click on the button  .

The information in the following group fields is optional:



- *System Availability (via Browser)*
- *Address*
- *Contact Person*



Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.

### 4.2.1.1 Add time zone

1. Click on the button **+** on the right of the entry field.

\_\_\_\_\_ + -

Fig. 5: Add time zone

2. To filter the list of entries in the table, enter the character sequence you would like to filter for in the filter field under the column headline *Continent/Region*.

⇒ The table only displays entries in this column containing the character sequence.

Example:

You would like to display exclusively *continents/regions* containing the character sequence *ber*; to do so, enter the character sequence *ber* in the filter field of the column *Continent/Region*:

Time zone	
Time Difference ↕	Continent/Region ↕
	<input type="text" value="ber"/>
UTC-04:00	Atlantic/Bermuda
UTC+01:00	Europe/Berlin
UTC+10:00	Australia/Canberra
<div> Rows per page 20 ▾ 1 - 3 of 3 1-4 &lt;-4 &gt;4-1 </div>	
<div> Add Cancel </div>	

Fig. 6: The displayed entries in the table are filtered for *ber* (example)

3. Select a time zone from the list.

Time zone	
Time Difference ↕	Continent/Region ↕
	<input type="text" value="ber"/>
UTC-12:00	Etc/GMT+12
UTC-11:00	Pacific/Pago_Pago
UTC-11:00	Pacific/Samoa
UTC-11:00	Pacific/Niue
UTC-11:00	US/Samoa
UTC-11:00	Etc/GMT+11
UTC-11:00	Pacific/Midway
<div> Rows per page 20 ▾ 1 - 20 of 616 1-4 &lt;-4 &gt;4-1 </div>	
<div> Add Cancel </div>	

Fig. 7: Add time zone

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

#### 4.2.1.2 Group field System Availability

1. If you would like to enable access to the system from outside the local network, open the group field *System Availability (via Browser)*.



Fig. 8: System Availability (via Browser)

2. If no separate settings are configured for a reseller or tenant regarding the system availability via the browser, the configuration of the next superordinate reseller or of the system provider is used.  
If superordinate settings are used, they are displayed in the group field. E. g. *Settings from the system applied*.

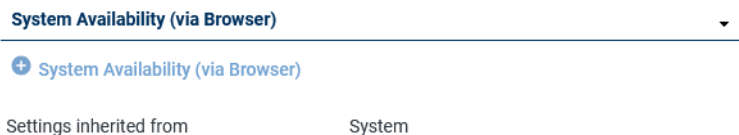



Fig. 9: System Availability (via Browser)

3. If the settings regarding the system availability (via browser) of a superordinate reseller or of the system provider are changed, the changes apply for the subordinate resellers or tenants without configured settings, too.  
If the settings regarding the system availability (via browser) have not been configured for a superordinate reseller or the system provider, no settings can be applied for subordinate instances.
4. To configure system availability (via browser), proceed as follows:
5. In the title bar of the group field, click on the button  *System Availability (via Browser)*.
6. Enter the addresses you would like to use.

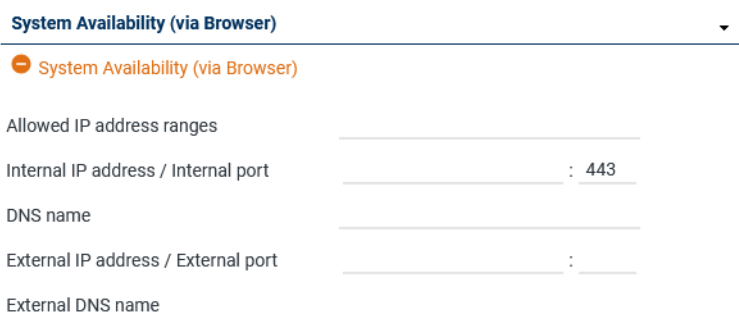


Fig. 10: Configure system availability

<i>Allowed IP address ranges</i>	Enter the <b>IP</b> address ranges under which the Replay module can be reached via the browser.
<i>Internal IP address / Internal port</i>	Enter the target <b>IP</b> address and the port of the replay server under which the Replay module can be reached internally.
<i>DNS name</i>	Enter the DNS name under which the Replay module can be reached internally.


<i>External IP address / External port</i>	Enter the <a href="#">URL</a> or the <a href="#">IP</a> address and the port under which the Replay module can be reached via the browser from outside the local network.
<i>External DNS name</i>	Enter the external DNS name under which the Replay module can be reached via the browser from outside the local network.  <b>NOTICE!</b> If the SSL certificate has been issued for a DNS address, it is mandatory to enter the DNS name, otherwise the certificate check in the replay applications will fail.



To enable the users of the tenant to access the replay server via the browser, an internal IP address and an external IP address must be configured in the Servers module. The address entered here and in the Servers module must be the same.



For information about the configuration of servers refer to the administration manual for system providers *Configuration servers and recording architectures*.


- If you would like to remove all addresses, click on the button  *System Availability (via Browser)* in the title bar of the group field.

#### 4.2.1.3 Group field Address

- If you would like to add a contact address, open the group field *Address*.



Fig. 11: Add address

- In the title bar of the group field, click on the button  *Add Address*.
- Enter the address.

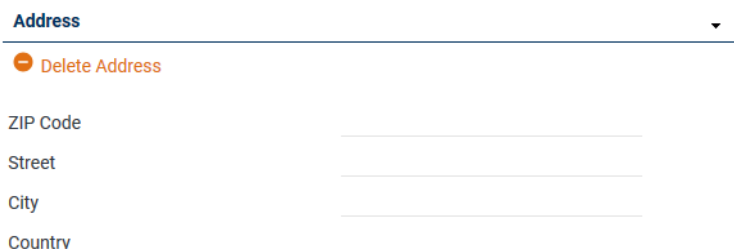



Fig. 12: Add address


- If you would like to remove the address, click on the button  *Remove Address* in the title bar of the group field.

#### 4.2.1.4 Group field Contact Person

- If you would like to add a contact person, open the group field *Contact Person*.



Fig. 13: Add contact person

- In the title bar of the group field, click on the button  *Add Contact Person*.
- Enter the contact data.



**Contact Person** ▼

➔ Remove Contact Person

First name\*

Last name\*

E-mail

Comment

Fig. 14: Add contact person



You can enter anyone as contact person. The contact person does not have to exist as a user in the system.

- If you would like to remove the contact person, click on the button ➔ *Remove Contact Person* in the title bar of the group field.

#### 4.2.2 Tab Passwords

Here, you can define the password rules which have to be observed by the users when creating a password.

◀ Details\* Passwords General Settings\* Key Management LDAP Connectio ▶

**Password Length** ▶

**Mandatory Characters** ▶

**Security** ▶

**Forbidden Passwords** ▶

**Advanced Password Settings** ▶

Fig. 15: Tenants module - tab Passwords

The password rules are applied to all passwords which are newly created or changed. Existing passwords are not checked.

Exceptions:

- Validity*  
All passwords are checked for their current period of validity on a daily basis.
- Possible failed login attempts*  
Upon each login attempt, the number of failed attempts is monitored for all passwords.

The defined password rules do **not** apply in the following cases:


- Authentication takes place via [LDAP](#)
- The user is a superuser
- The following option has been activated for the user account:  
*Does not have to meet the password rules*

Parameters which contain the value 0 or no value at all are ignored.




Defining password rules is optional.



Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.

### Group field Password Length

1. To define the password length, open the group field *Password Length*.
2. In the title bar of the group field, click on the button  *Password Length*.  
The value for all entry fields ranges from 0 to 256 characters.
3. In the field *Minimum length*, enter the minimum number of characters mandatory for the password.




Password Length	
 Remove password length	
Minimum length (max. 3 characters)	<input type="text" value="1"/>
Maximum length (max. 3 characters)	<input type="text" value="256"/>

Fig. 16: Define password length

4. In the field *Maximum length*, enter the maximum number of characters mandatory for the password.  
**NOTICE!** *Maximum length* must be  $\geq$  *minimum length*.
5. If you would like to remove the entries, click on the button  *Remove password length* in the title bar of the group field.

### Group field Mandatory Signs

1. To define the mandatory characters, open the group field *Mandatory Characters*.
2. In the title bar of the group field, click on the button  *Mandatory Characters*.
3. Complete all or only individual fields:  
The value for all entry fields ranges from 0 to 256 characters.




Mandatory Characters	
 Remove mandatory characters	
Max. character repetition (max. 3 characters)	<input type="text" value="256"/>
Min. number of	
Letters (max. 3 characters)	<input type="text" value="2"/>
Digits (max. 3 characters)	<input type="text" value="2"/>
Punctuation characters (max. 3 characters)	<input type="text" value="1"/>
Lower-case letters (max. 3 characters)	<input type="text" value="0"/>
Upper-case letters (max. 3 characters)	<input type="text" value="0"/>

Fig. 17: Define mandatory characters

Max. character repetition	Enter how often a character may be repeated directly one after another.		
	Examples:		
	Max. character repetition	Valid	Invalid
	0	abc	aabc
	1	aabcabc	aaabcabc
	2	aaabc	aaaabcabc
Min. number of letters	Enter how many letters a password must contain at least.		
Min. number of digits	Enter how many numbers a password must contain at least.		
Min. number of punctuation characters	Enter how many punctuation characters a password must contain at least.		
	Valid punctuation characters:		
	Full stop	.	
	Comma	,	
	Semicolon	;	
	Colon	:	
	Question mark	?	
	Exclamation mark	!	
	Quotation marks	""	
	Apostrophe	'	
	Hyphen	-	
	Dash	/	
	Brackets	() [] {}	
		All other punctuation characters are taken as letters.	
Lower-case letters	Enter how many lower-case letters a password must contain at least.		
Upper-case letters	Enter how many upper-case letters a password must contain at least.		

- If you would like to remove the entries, click on the button  *Remove mandatory characters* in the title bar of the group field.

### Group field Security

- To change the settings of the security, open the group field *Security*.
- In the title bar of the group field, click on the button  *Security*.
- Complete all or only individual fields:  
The value for all entry fields ranges from 0 to 999 characters.

**Security** ▼

➔ Remove security

Validity  
(max. 3 characters)  Day(s)

Point in time when information about the imminent expiration of the password is sent  
(max. 3 characters)  Day(s)

Password history

☒ Password history in days  
 Day(s)

☐ Extent of password history

Possible failed login attempts  
(max. 3 characters)


Deny personal data ☐

Fig. 18: Configure password security


<i>Validity</i>	Enter for how long a password is supposed to remain valid. <i>Validity = 0:</i> Passwords never expire
<i>Point in time when information about the imminent expiration of the password is sent</i>	Enter how many days before the expiration of the password users are to be reminded that they will have to change their password soon. <i>Point in time ... = 0:</i> User does not receive any information <b>NOTICE!</b> The value for the point in time to send information must be smaller than the value for the validity of the password.
<i>Password history</i>	Enter for how long the password history is supposed to be saved. Select one of the following options: <ul style="list-style-type: none"> <li>• <i>Password history in days</i> For this option, enter for how long the passwords are supposed to be saved in the password history.</li> <li>• <i>Extent of password history</i> For this option, enter the number of passwords which are supposed to be saved in the password history.</li> </ul> In both cases, the password history is never deleted entirely. If the entered value is reached, only the oldest entries are deleted.
<i>Possible failed login attempts</i>	Enter how often the user may enter an incorrect password before the account is locked. <b>NOTICE!</b> A locked account can be released again by any user with access to the Employees module and to the data of the locked user.
<i>Deny personal data</i>	Define whether users are allowed to use private data from their profiles for the password (e. g. name, user name, date of birth). <input checked="" type="checkbox"/> = Personal data is not allowed. <input type="checkbox"/> = Personal data is allowed.

- If you would like to remove the entries, click on the button ➔ *Remove security* in the title bar of the group field.

### Group field Forbidden Passwords


1. To define forbidden passwords, open the group field *Forbidden Passwords*.
2. In the title bar of the group field, click on the button  *Forbidden Passwords*.
3. In the list *Forbidden Passwords*, compile all words which must not be used as password.  
**NOTICE!** No difference is made between upper or lower case letters.

#### Forbidden Passwords

Server	
System	

**Add** **Delete**


Fig. 19: Define forbidden passwords

<b>Add</b>	Adds a new entry to the list.
<b>Delete</b>	Deletes the selected entry from the list.
	Opens the selected entry for editing (see <a href="#">chapter "Edit entry", p. 21</a> ).

4. If you would like to activate the monitoring of the entered words, activate the check box behind *Use blacklist for passwords*.

*Use blacklist for passwords* ☒ = Monitoring has been activated.

☐ = Monitoring has been deactivated. The entries in the list are ignored.

5. If you would like to remove the entries, click on the button  *Remove forbidden passwords* in the title bar of the group field.

### Group field Advanced Password Settings

1. To define advanced password settings, open the group field *Advance Password Settings*.
2. Select whether the password rules can be ignored.

#### Advanced Password Settings

Password rules can be ignored ☐

Fig. 20: Define advanced password settings


*Password rules can be ignored*




☒ = Password rules can be ignored.

To allow a user to ignore the password rules, additionally activate the option *Does not have to meet the password rules* in the employee's account.

☐ = Password rules cannot be ignored.



#### 4.2.2.1 Edit entry

1. To adjust an entry in the list, click on the icon  (*Edit*) in the corresponding line.  
⇒ The entry is edited in an entry field.

0002150013333	
0602150014444	
<input type="text" value="New value"/>	 

Add Delete

Fig. 21: Edit entry in the list


- Adjust the entry.
- To save the changes, click on the icon  (Save).  
To discard the changes, click on the icon  (Discard).

### 4.2.3 Tab General Settings


Here, you can change several general settings.

[Details\\*](#)
[Passwords](#)
[General Settings\\*](#)
[Key Management](#)
[LDAP Connectio](#)


---

[Inactivity](#) 


---

[SMTP Account](#) 


---

[Login Settings](#) 

---

[Miscellaneous Settings](#) 

---

[Random Search of Sessions](#) 

---



[Terms of Use](#) 

Fig. 22: Tenants module - tab General Settings

#### 4.2.3.1 Group field Inactivity

**Inactivity** 

---

Notify before locking\*  Day(s)  
(max. 3 characters)

User will be deactivated\*  Day(s)  
(max. 3 characters)

Session timeout ☒ Session timeout  Minute(s)  
☐ Session never expires

Fig. 23: Configure user activity

<i>Notify before locking</i>	Select how many days before the locking of the account the user is supposed to be notified that the account will be locked due to inactivity. The account is locked if the user has been inactive for the number of days entered in the field <i>User will be deactivated</i> .  The notification is sent to the e-mail address of the user.
<i>User will be deactivated</i>	Select after how many days of inactivity the account of the user is locked.

### Session timeout

Select after how many minutes of inactivity the session of the user is supposed to be ended automatically by timeout. Select one of the following options:

- **Session timeout**


This option activates the session timeout. Enter a value between 5 and 1440.

- **Session never expires**

This option deactivates the session timeout and enables endless sessions.

#### NOTICE!

Before activating this option, consider the following:

The started session is never ended if the user just closes the browser instead of logging off from the application properly by using the logoff function (menu item  (Logged in as) > Logoff). Each endless session consumes storage space. This may result in the necessity to reboot the server. Upon rebooting the server, all sessions are ended.



Changes in these settings come into effect only after the user has logged in to the system once again.

#### 4.2.3.2

### Group field SMTP Account

To be able to use the function of sending system notifications via e-mail, you have to configure the **SMTP** account of the system user in the application System Configuration.

1. To add an **SMTP** account, open the group field *SMTP Account*.



Fig. 24: SMTP account

2. If no separate settings are configured for the **SMTP** account of a reseller or tenant, the configuration of the next superordinate reseller or of the system provider is used. If superordinate settings are used, they are displayed in the group field. E. g. *Settings from the system applied*.

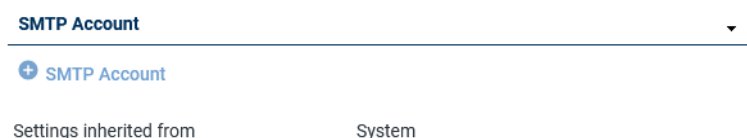



Fig. 25: SMTP account

3. If the **SMTP** account of a superordinate reseller or of the system provider is changed, the changes apply for the subordinate resellers or tenants without configured settings, too. If the **SMTP** account of a superordinate reseller or of the system provider has not been configured, no settings can be applied for subordinate instances.
4. To configure the **SMTP** account, proceed as follows:
5. In the title bar of the group field, click on the button  *SMTP Account*.

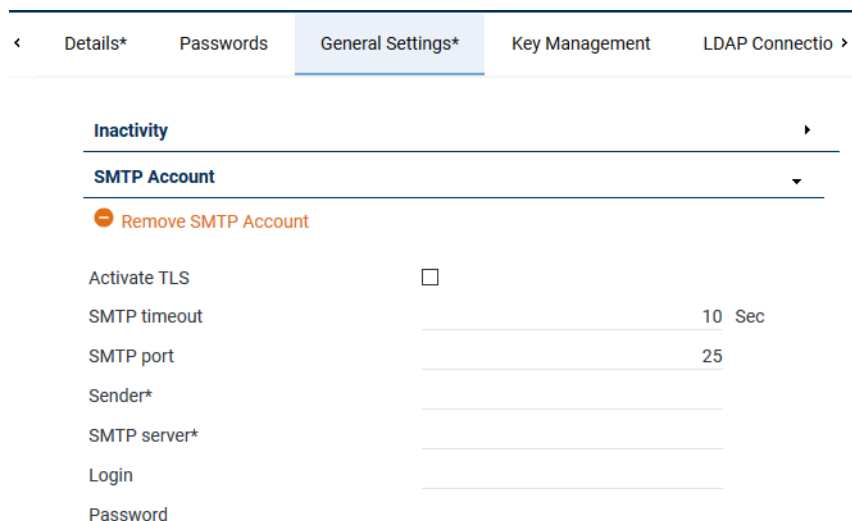




Fig. 26: Add SMTP account



Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.

6. Complete the following fields:

<i>Activate TLS</i>	Select whether you would like to activate the encryption protocol <a href="#">TLS</a> . <input checked="" type="checkbox"/> = <a href="#">TLS</a> has been activated. <input type="checkbox"/> = <a href="#">TLS</a> has been deactivated.
<i>SMTP timeout</i>	Enter after how many seconds a timeout notification is supposed to be sent if no connection to the SMTP server can be established.
<i>SMTP port</i>	Enter the port via which you would like to log in. Default value: 25 (TLS: 587)
<i>Sender</i>	Enter the e-mail address which is supposed to be used as sender address in sent e-mails.
<i>SMTP server</i>	Enter the <a href="#">IP</a> address or the name of the <a href="#">SMTP</a> server on which the account has been created.
<i>Login</i>	Enter the login name for the authentication on the <a href="#">SMTP</a> server.
<i>Password</i>	Enter the password for the authentication on the <a href="#">SMTP</a> server.

7. If you would like to remove the SMTP account, click on the button  *Remove SMTP Account* in the title bar of the group field.

#### 4.2.3.3 Group field LDAP Authentication

Here, you can activate or deactivate the authentication via [LDAP](#) for the users of your environment as a rule.



Fig. 27: Activate LDAP

*Activate LDAP login*    Activate or deactivate the authentication via [LDAP](#).



- ☒ = [LDAP](#) login has been activated.  
☐ = [LDAP](#) login has not been activated.



If you activate [SSO](#) login as well as [LDAP](#) login, the LDAP data are ignored if users log in with their Windows accounts.



[LDAP](#) login cannot be activated before you have configured at least 1 [LDAP](#) connection (see chapter "[Tab LDAP Connection Data](#)", p. 27).

#### 4.2.3.4 Group field Miscellaneous Settings

##### Miscellaneous Settings

- ☐ Display last login date  
☒ Display logout warning  
☒ Resource string view  
☐ Failed login

Fig. 28: Configure miscellaneous settings

<i>Display last login date</i>	Select whether you would like to have the date of the last login displayed in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
<i>Display logout warning</i>	Select whether you would like to issue a logout warning in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
<i>Resource string view</i>	Select whether you would like to display the button to activate the resource string view in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
<i>Failed login</i>	Select whether you would like to display the information about a failed login in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.

#### 4.2.3.5 Group field Random Search of Sessions

##### Random Search of Sessions

Maximum number of search results\* 20

Fig. 29: Configure session search results

<i>Maximum number of search results</i>	Enter how many search results yielded by the random search are supposed to be displayed in the Sessions module at the maximum. Range of values: 0 to 50
---	--

## 4.2.3.6 Group field Terms of Use

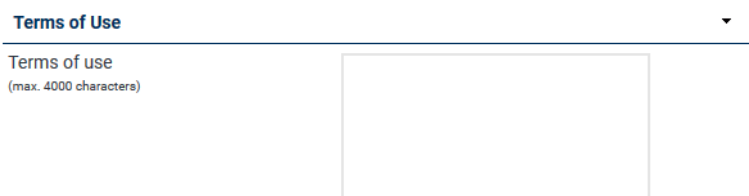


Fig. 30: Configure terms of use

<b>Terms of use</b>	<p>Here, you can enter terms of use.</p> <p>The terms of use are displayed in the browser upon logging in to the application <i>neo</i> and must be confirmed by clicking on <i>OK</i>.</p>
---------------------	---

## 4.2.4 Tab Key Management

The conversations are recorded with encryption to make sure that no unauthorized third parties can replay them. Here, you can define the method which is supposed to be used to encrypt the recordings. You can select 2 different methods:

- Encryption mode *Simple*:  
A default key which never expires is used for the encryption. This method has been preset. It only offers minimum security.
- Encryption mode *neo*:  
neo key management is used for the encryption. This method offers high security.  
You receive an individual key which serves to encrypt your recordings. By means of a password that you define yourself, this key is encrypted as well for additional protection upon saving it in the database. On top of that, you can limit the validity time of the key and generate a new key in regular intervals automatically.

**NOTICE!** Your system provider makes the settings for the validity of the key. Your system provider finds information about this topic in the installation manual *Configuration of servers and recording architectures*.

Preconditions for the usage of the neo key management

- The application has been installed and started.
- The license Key Management is available in the system.
- Key management has been activated and configured by your system provider.

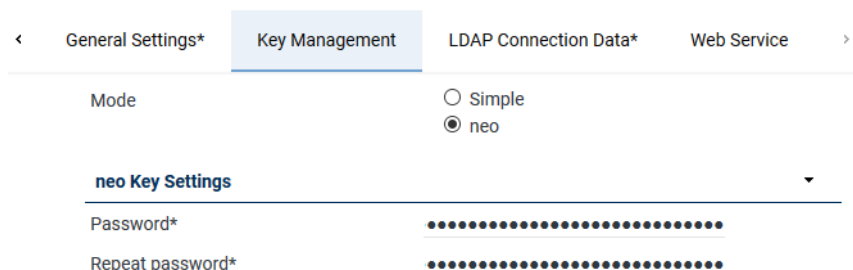


Fig. 31: Tenants module - tab Key Management

**Configure key management**

1. Select the encryption mode.
  - When selecting the encryption mode *Simple*, no further adjustments are necessary. The default key is used to encrypt the recordings.

- When selecting the encryption mode *neo*, proceed as described in the following steps.
- 2. Open the group field *neo Key Settings*.
- 3. In the field *Password*, enter the password which is supposed to be used to protect your key.
- 4. Enter the password again in the field *Repeat password*.
- ⇒ Your password is saved in an encrypted database.
- ⇒ The password-protected key is generated. This key protects all your recordings against unauthorized access.
- ⇒ If a new key is created automatically in regular intervals (settings of the system provider), each new key is protected by this password as well. The current, password-protected key is used to encrypt the recordings.



When changing your password, all your keys currently stored in the database are exported, decrypted with the old password, and encrypted once again with the new password.

5. Click on the button *Save*.
6. To create a key manually, click on the button *Generate Key*.  
This option is only available if configured correspondingly by the system provider. The password must be saved successfully in the application Dongle Manager.

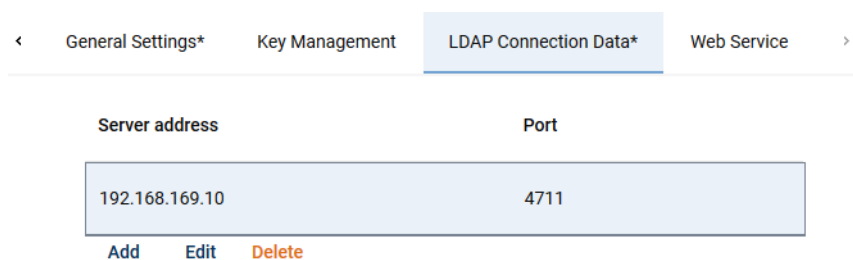


For more information about key management refer to the administration manual for system providers *Encryption of recordings*.

#### 4.2.5 Tab LDAP Connection Data

Here, you can administrate the [LDAP](#) connection data. If you create several [LDAP](#) connections, the system browses all connection configurations upon a login attempt via [LDAP](#) until one of the connections is successful.

You can activate the usage of [LDAP](#) authentication in the tab *General Settings* (see [chapter "Group field LDAP Authentication", p. 24](#)).



Server address	Port
192.168.169.10	4711

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

Fig. 32: Tenants module - tab LDAP Connection Data

<a href="#">Add</a>	Opens a window in which you can add a new <a href="#">LDAP</a> connection (see <a href="#">chapter "Edit LDAP connection data", p. 28</a> ).
<a href="#">Edit</a>	Opens the selected entry for editing (see <a href="#">chapter "Edit LDAP connection data", p. 28</a> ).
<a href="#">Delete</a>	Deletes the selected entry from the list.

## 4.2.5.1 Edit LDAP connection data

Server address	Port
159.159.159.159	46611
123.123.123.123	4711

Add Edit Delete

Fig. 33: LDAP Connection Data

- To configure a new **LDAP** connection, click on the button *Add*.  
To edit an existing **LDAP** connection, click on the button *Edit*.

Edit Connection Data

Server address\*  
Port\*  
Use SSL  
User DN  
Password

123.123.123.123  
4711  
☐  
CN=Johnson Jim:OU=  
•••••

Check LDAP Connection
OK
Cancel

Fig. 34: Edit LDAP connection data (example)

<b>Server address</b>	IP address of the <b>LDAP</b> server.
<b>Port</b>	Port on the <b>LDAP</b> server which is used to establish a connection. By default, the following port is used: 389 = <b>LDAP</b> connection, unencrypted 636 = <b>LDAP</b> connection, encrypted
<b>Use SSL</b>	Activate or deactivate the usage of the <b>SSL</b> protocol. <input checked="" type="checkbox"/> = <b>SSL</b> is used. <input type="checkbox"/> = <b>SSL</b> is not used. <b>NOTICE!</b> <b>SSL</b> can only be used if the <b>LDAP</b> server supports <b>SSL</b> .
<b>User DN</b>	Distinguished name (DN) of the user required for the authentication to the <b>LDAP</b> server.
<b>Password</b>	Password required for the authentication to the <b>LDAP</b> server.

- Complete all fields or only the mandatory ones.
- To check whether a connection to the **LDAP** server can be established with the entered data, click on the button *Check LDAP Connection*.  
⇒ The result of the check is displayed in the window *Edit Connection Data*.
- To save the entries and apply them in the list, click on the button *OK*.  
To discard entries, click on the button *Cancel*.

## 4.2.6 Tab Web Service

The *neo* software provides an interface for web service methods. Via the Web Service providers can automatically create tenants, create the tenant's employees as well as assign extensions.

In this tab, you can see whether the functions for the Web Service have been activated



The functions can only be activated or deactivated by the system provider.

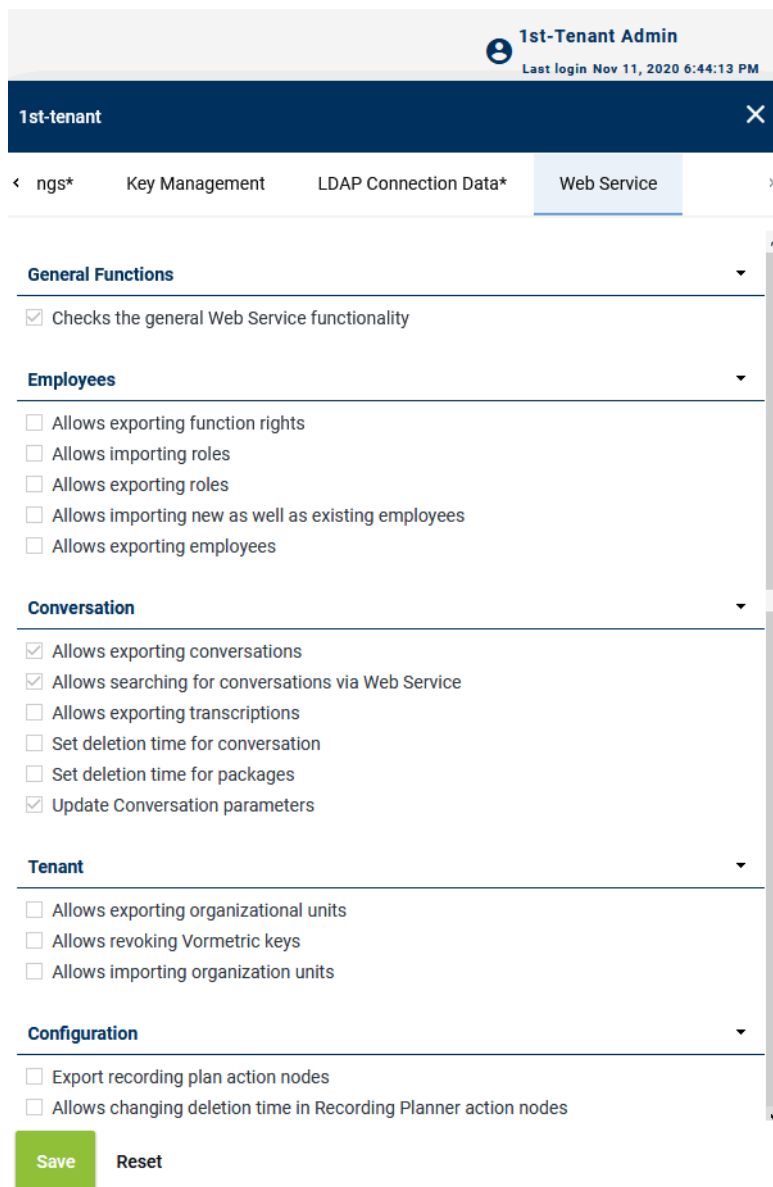


Fig. 35: Display web service functions

☒ = Function has been activated.

☐ = Function has been deactivated.

### Group field General Functions

<i>Checks the general web service functionality</i>	Shows whether you can check the functionality of the Web Service.
---	---

### Group field Employees

<i>Allows exporting function rights</i>	Shows whether function rights can be exported via the Web Service.
<i>Allows importing new as well as existing employees</i>	Shows whether employee data can be administrated via the Web Service.
<i>Allows importing roles</i>	Shows whether roles can be imported via the Web Service.
<i>Allows exporting roles</i>	Shows whether roles can be exported via the Web Service.

*Allows exporting employees* Shows whether employees can be exported via the Web Service.

#### Group field Conversation

*Allows exporting conversations* Shows whether conversations can be exported via the Web Service. The exported conversations are saved as WAVE files.

*Allows searching for conversations via Web Service* Shows whether conversations can be searched via the Web Service.

*Allows exporting transcriptions* Shows whether transcriptions can be exported via the Web Service.

*Set deletion time for conversation* Shows whether a deletion time can be set for the conversations.

*Set deletion time for packages* Shows whether a deletion time can be set for packages via the Web Service.

#### Group field Tenant

*Allows exporting organization units* Shows whether organization units can be exported via the Web Service.

*Allows revoking Vormetric keys* Shows whether a Vormetric keys can be revoked via the Web Service.

*Allows importing organization units* Shows whether organization units can be imported via the Web Service.

## 5 Employees module

In the Employees module, you can create and administrate data about the users:

- Personal data
- Account data
- Function rights for the different applications

You have the possibility to assign a user role rights, individual function rights, and organization units.



Some function rights are linked to certain licenses. These function right can only be assigned if the corresponding (free) license is available in the system.



Upon assigning a user an agent or a supervisor function right, the corresponding license is reserved for this user.



You can import user data from existing [LDAP](#) structures, too. The import is configured via the Configuration Import module. For more information refer to the administration manual *Import of user data*.



You can import configuration data from existing [LDAP](#) structures, too. The import is configured in the Configuration Import module. For further information refer to the administration manual *Import of configuration data*.

Open the Employees module by clicking on the menu item *Employees* in the navigation bar of the application System Configuration.

### 5.1 Main view

All saved employees are displayed in the main view.

+ × Employees General						
Employee Number	First Name	Last Name	E-mail	Date of Entry	Date of Birth	Address
	111	Agent				
800	8.	Agent				
1100	11.	Agent-Superior				
1000	10.	Agent				
900	9.	Agent				
8000	80.	Agent				
700	7.	Agent				
600	6.	Agent				
500	5.	Agent				
400	4.	Agent				
300	3.	Agent				
200	2.	Agent				

Rows per page 50 1 - 14 of 14 < > << >>

Fig. 36: Employees module - main view

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






<i>Employee Number</i>	ID of the employee.
<i>First Name</i>	First name of the employee.
<i>Last Name</i>	Last name of the employee.
<i>E-mail</i>	E-mail address of the employee.
<i>Date of Entry</i>	Date on which the employee was hired.
<i>Date of Birth</i>	Date of birth of the employee.
<i>Address</i>	Private address of the employee.
<i>Is Superuser</i>	Shows whether the employee has superuser rights. ✓ = superuser rights ✗ = no superuser rights
<i>Agent Data</i>	Shows whether agent data has been assigned to the employee. ✓ = Agent data has been assigned. ✗ = No agent data has been assigned.
<i>Visible</i>	Shows whether the employee is visible for other users. 👁 = Employee is visible. 🔒 = Employee is not visible.
<i>Comment</i>	Comment added to the employee's information.
<i>Creation Date</i>	Date on which the employee's information was created.
<i>Updated</i>	Date on which the employee's information was updated for the last time.

### 5.1.1 Toolbar

The toolbar offers the following functions.



Fig. 37: Employees module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria (see <a href="#">chapter "Search", p. 34</a> ). The icon  (Search) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Add</i>	Creates a new employee (see <a href="#">chapter "Create new employee", p. 60</a> ).
	<i>Delete</i>	Deletes the selected employee.
<i>Employees</i>	<i>Summary</i>	Lists all function rights of the selected employee (see <a href="#">chapter "Show summary", p. 33</a> ).
	<i>Show locked employees/Show all employees</i>	Lists only the locked employees in the main view (see <a href="#">chapter "Show locked employees", p. 34</a> ).
	<i>Make employee visible or not visible</i>	Function which makes the selected employee visible or not visible for others (see <a href="#">chapter "Make employee visible or not visible", p. 34</a> ).



	<i>Display agent's shift schedule</i>	Opens a window in which you can see the shift schedule of the selected agent. <b>NOTICE!</b> The icon is only displayed if the connection to the Teleopti server has been activated. <b>NOTICE!</b> The function is only available for employees defined as agents whose user data has been imported. For manually created agents the function is not available.
	<i>Export User Data</i>	Exports the user data of the employee of the current tenant in <a href="#">XML</a> format.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



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

#### 5.1.1.1 Show summary

This function allows displaying the function rights of the employee.

1. Select the respective employee from the list in the main view.
2. Click on the menu item *Employees > Summary* in the toolbar.  
⇒ The window *Summary* appears.

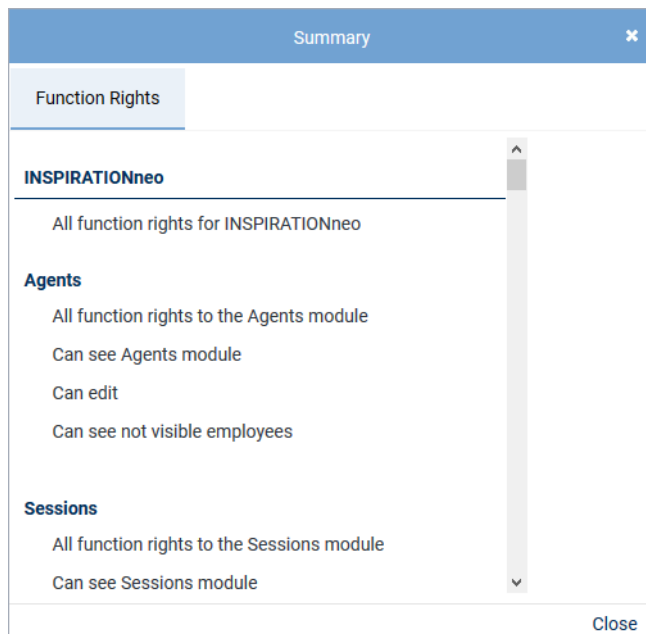


Fig. 38: Summary of the function rights



Function right has been assigned individually.



Function right has been assigned via a role.

**NOTICE!** Let the cursor hover above the icon to display via which role the function right has been assigned.

#### 5.1.1.2 Show locked employees

This function allows filtering for all employees whose account has been locked.

1. Click on the menu item *Employees > Show Locked Employees* in the toolbar.  
⇒ In the main view, only those employees whose account has been locked are displayed.
2. To cancel the filtering, click on the menu item *Show All Employees*.





Information about how to lock an account can be found in the Tab Account.

#### 5.1.1.3 Make employee visible or not visible

You can make an employee visible or invisible for other users of the system.



If employees have been marked as invisible, they can only be seen by superusers or by other users with the function right *Can see invisible employees*. The setting whether an employee is visible has an impact in all *neo* applications.

It can be useful to make an employee invisible for other users e. g. if the employee is absent for a longer period of time (e. g. parental leave) and no tasks are supposed to be assigned to him.

1. Select the respective employee in the main view.
2. Click on the menu item *Employees > Make Employee Visible or Not Visible* in the toolbar.  
⇒ The status of the employee is changed.  
⇒ In the column *Visible* in the main view, the icon changes:  
 = Employee is visible.  
 = Employee is not visible.

#### 5.1.1.4 Search

The search function allows searching systematically for sets of data which meet certain criteria.

1. In the toolbar, click on the icon  or  (*Search*).  
⇒ The window *Search Criteria* appears.

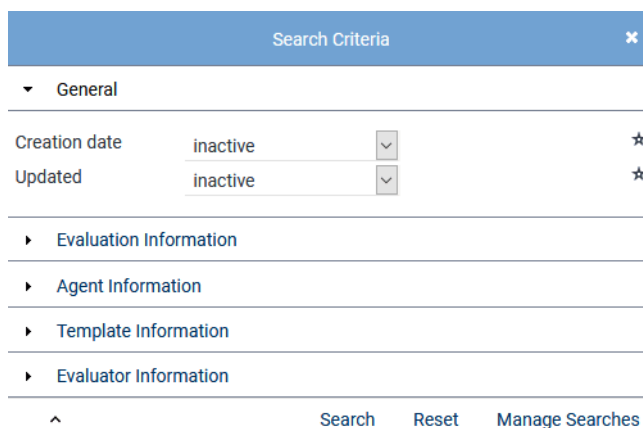





Fig. 39: Window Search Criteria (example)

2. Set the respective search criteria.  
**NOTICE!** It depends on the respective module which search criteria are available.
3. To start the search, click on the button *Search*.  
To reset all manually entered search criteria, click on the button *Reset*.

⇒ After running the search, only those sets of data are displayed in the main view which meet the set search criteria.

4. To display all original sets of data in the main view again, i. e. to reset the manually entered search criteria, click on the icon  (*Reset search*) in the toolbar.

By clicking on the button *Manage Searches*, you can save the defined search criteria under an unambiguous name, load saved search criteria or delete them.

By clicking on the icon , you can tag the search criterion as favorite. Criteria tagged as favorite are displayed additionally in the upper area of the window *Search Criteria* and marked with the icon .



A detailed description of the search function can be found in the user manual *System Configuration - General information*.

## 5.2

### Detail view

The detail view contains information about the data and rights of the selected employee.

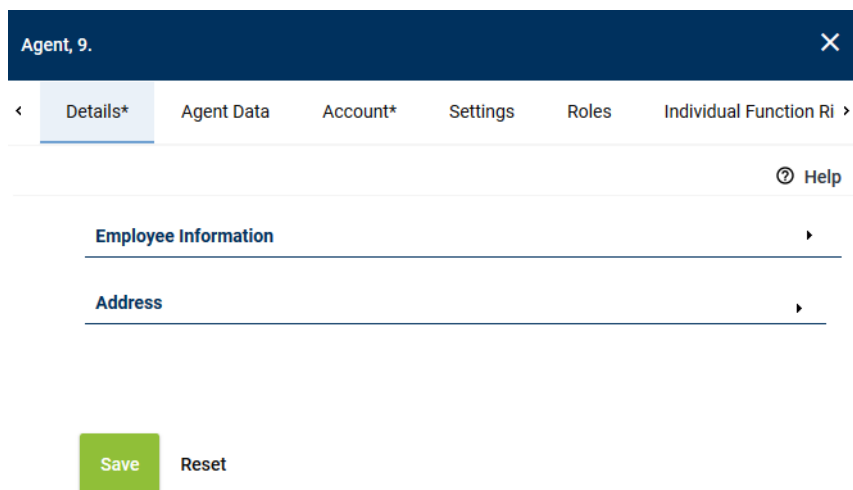


Fig. 40: Employees module - detail view

The detail view consists of the following tabs:

- *Details*  
Here, you can display and edit the employee's personal data.  
See [chapter "Tab Details", p. 36](#).
- *Agent Data*  
Here, you can select whether an employee is supposed to have the function of an agent. In addition, you can display and edit the agent properties of the employee.  
See [chapter "Tab Agent Data", p. 40](#).
- *Account*  
Here, you can display and edit the employee's login data.  
See [chapter "Tab Account", p. 43](#).
- *Settings*  
Here, you can display and edit the employee's rights and logging settings.  
See [chapter "Tab Settings", p. 47](#).
- *Roles*

Here, you can display the roles which have been assigned to the employee and edit the role assignment.

See [chapter "Tab Roles", p. 51](#).

- *Individual Function Rights*

Here, you can display and assign the employee's individual function rights.

See [chapter "Tab Individual Function Rights", p. 53](#).

- *Conversation Rules*

Here, you can display the conversation rules which have been assigned to the employee and edit the assignment of the conversation rules.

See [chapter "Tab Conversation Rules", p. 56](#).

- *Organization Units*

Here, you can display the organization units which have been assigned to the employee and edit the assignment of the organization units.

See [chapter "Tab Organization Units", p. 58](#).



As long as no user account (tab *Account*) exists for the employee, only the following tabs are available for this employee:

- *Details*
- *Agent Data*
- *Account*

### 5.2.1 Tab Details

Here, you can display and edit the employee's personal data.

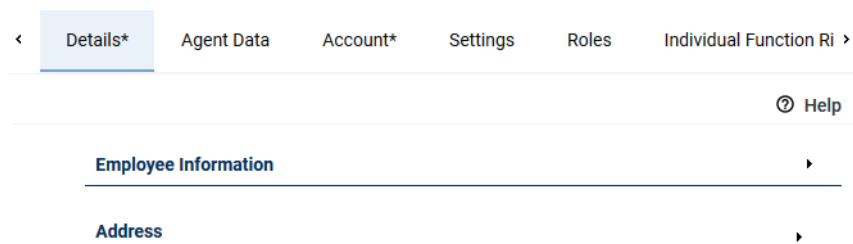



Fig. 41: Employees module - tab Details



Entering an address is optional.

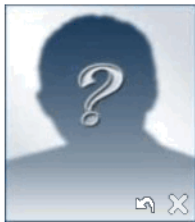


Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.

#### 5.2.1.1 Group field Employee Information

1. To edit personal data of the employee, open the group field *Employee Information*.


## Employee Information




Employee number

First name\*

Last name\*

Date of birth  



E-mail

Date of entry  

Comment

Address for replay via phone

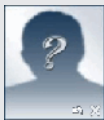
Import key



Time zone   

Release for keyword spotting ☐

Release for transcription ☐

Fig. 42: Edit employee information

	Placeholder for the employee's photo. See <a href="#">chapter "Upload or delete image", p. 38.</a>
<b>Employee Number</b>	ID of the employee.
<b>First Name</b>	First name of the employee.
<b>Last Name</b>	Last name of the employee.
<b>Date of birth</b>	Date of birth of the employee. You can enter the date directly via the keyboard or via the icon.
<b>E-mail</b>	E-mail address of the employee.
<b>Date of Entry</b>	Day on which the employee was hired. You can enter the date directly via the keyboard or via the icon.
<b>Comment</b>	Comment on the employee information.
<b>Address for replay via phone</b>	Enter the address of the phone which is supposed to replay the calls. Depending on which agent logs in on this phone, the audio data that the participant is allowed to replay is provided. You can use the following additional data as address: <ul style="list-style-type: none"> <li>• Extension if it has been configured in the PBX for replay via phone.</li> <li>• Complete phone number, e. g. 06021 5001 1015 if the PBX is connected to the public telephone network.</li> <li>• IP address if it has been configured.</li> <li>• MAC address if it has been configured.</li> </ul>

	<ul style="list-style-type: none"> <li>SIP address, e. g. <i>Extension@IP-Address</i>.</li> </ul>
<i>Import key</i>	<p>Key to unambiguously identify an employee imported from an external source.</p> <p>When importing the employee information for the first time, the import key is entered here automatically. Upon each new import, this import key is checked to determine whether the employee has already been imported before.</p> <p>In addition, the import key is used when transferring (export/import) recordings from a <i>neo</i> system to another <i>neo</i> system to map the recordings to the agents. If the employee does not have an automatically created import key, you can enter an import key manually for this mapping.</p> <p><b>NOTICE!</b> If you change an import key manually, the employee will not be recognized as an already imported employee upon the next import of employee data. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordings.</p>
<i>Time zone</i>	<p>Shows the time zone in which the conversations are supposed to be displayed in the replay applications. The settings which have been configured for the respective employee prevail over the default settings in the Tenants module</p> <p>To select the time zone, click on the button . See <a href="#">chapter "Add time zone", p. 14</a>.</p> <p>To delete the selection, click on the button .</p>
<i>Release for keyword spotting</i>	<p>Select whether the employee's conversations are supposed to be considered for the speech analysis method <i>keyword spotting</i>.</p> <p><input checked="" type="checkbox"/> = Consider for keyword spotting</p> <p><input type="checkbox"/> = Do not consider for keyword spotting</p>
<i>Release for transcription</i>	<p>Select whether the employee's conversations are supposed to be considered for the speech analysis method <i>Transcription</i>.</p> <p><input checked="" type="checkbox"/> = Consider for transcription</p> <p><input type="checkbox"/> = Do not consider for transcription</p>

#### 5.2.1.1.1 Upload or delete image

- Click on the icon  (*Upload image*) on the placeholder for the image.

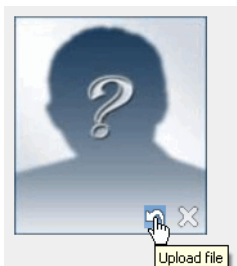


Fig. 43: Upload image

⇒ The window *Upload File* appears.

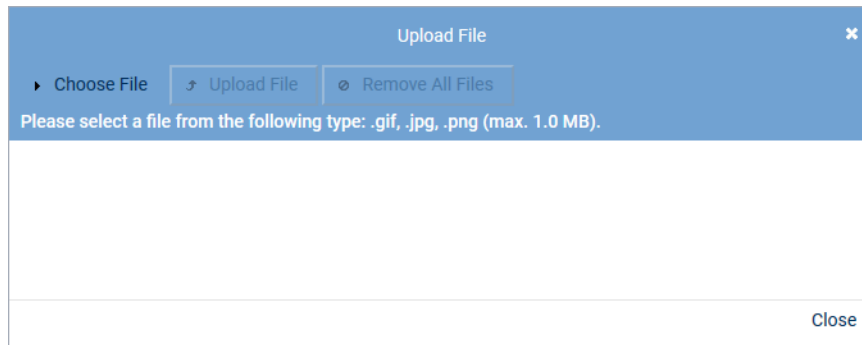


Fig. 44: Upload File


2. Click on the button *Choose File*.
3. Select the file via the Explorer and click on the button *Open*.



You can save several image files in the clipboard.

To empty the clipboard, click the button *Remove All Files*.

To remove only one file from the clipboard, click on the button  next to the file.

4. To apply an image in the detail view, click on the button *Upload file*.  
⇒ The image is displayed in the detail view.
5. If you would like to remove the image again, click on the icon  (*Delete image*) in the bottom right corner of the image.

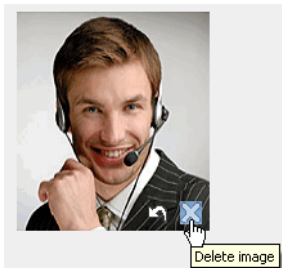


Fig. 45: Delete image (example)

⇒ The image is deleted from the detail view.


### 5.2.1.2

#### Group field Address

1. If you would like to add a contact address, open the group field *Address*.



Fig. 46: Add address

2. In the title bar of the group field, click on the button  *Add Address*.
3. Enter the address.

**Address** ▾

✖ Delete Address

ZIP Code

Street

City

Country

Fig. 47: Add address

- If you would like to remove the address, click on the button ✖ *Remove Address* in the title bar of the group field.

### 5.2.2 Tab Agent Data

Here, you can select whether an employee is supposed to have the function of an agent. In addition, you can display and edit the agent properties of the employee.

To configure the function *Monitoring* for the conversations of the agent, see [chapter "Configure monitoring", p. 41](#).

To configure screen recording for agents, see [chapter "Configure screen recording", p. 43](#).

To configure the recording of the agent's chats, see [chapter "Configure chat recording", p. 42](#).

Entering agent data is optional.

Upon activating the option *Agent*, the employee is recognized as agent by the system; however, he does neither receive any role-specific function rights yet nor access to the system. For the employee to receive the required function rights, you must either assign him the default role *Agent* or an agent role you have defined yourself, see [chapter "Assign roles", p. 52](#).

Upon deactivating the option *Agent*, the system does not consider the employee as an agent anymore. The assignment of the role *Agent* is not removed automatically when deactivating the option. If the employee is supposed to lose the function rights of an agent, too, you have to remove the assignment of the role manually, see [chapter "Delete role assignment", p. 53](#).



◀ Details\* **Agent Data** Account\* Settings Roles Individual Function Ri ▶

☒ Agent

**Telephony** ▶

**Chat** ▶

**Miscellaneous Settings** ▶

Fig. 48: Employees module - tab Agent Data

**Agent** Select whether the system is supposed to recognize the employee as agent.

☒ = Employee is an agent.

☐ = Employee is no agent.

Upon activating the option *Agent*, all other entry fields are displayed.

#### 5.2.2.1 Group field Telephony

To edit the telephony data of the agent, open the group field *Telephony*.



**Telephony** ▼

---

PBX SIP ▼

Extension  
(max. 2500 characters)

427

PBX Agent ID  
(max. 255 characters)

427agent1

Fig. 49: Agent Data - Telephony

<b>PBX</b>	<p>PBX via which the agent's conversations are made.</p> <p>Select the PBX from the drop-down list.</p>
<b>Extension</b>	<p>Extensions which are supposed to be assigned to the agent.</p> <p>Enter the extensions in the entry field.</p> <p><b>NOTICE!</b> Use commas to separate the different extensions.</p>
<b>PBX Agent ID</b>	<p>IDs which have been saved in the <b>PBX</b> for the agent, too. By means of these IDs the recording system can identify an agent and his participation in a conversation.</p> <p>Enter the agent's IDs in the entry field.</p> <p><b>NOTICE!</b> Use commas to separate the different IDs.</p>

#### 5.2.2.1.1 Configure monitoring



Precondition for this function:

The system provider has activated the function *Monitoring* in the Servers module of the system configuration.

The function *Monitoring* allows users with the respective rights to listen in on a conversation which is currently recorded. If you would like to enable the function *Monitoring* for the conversations of the agent, use one of the following options to configure that the conversations are mapped to the agent correctly.

- **Mapping via the PBX Agent IDs**

Use this option if no determined extension has been assigned to the agent.

In this case, enter at least 1 PBX Agent ID in the entry field *PBX Agent ID*. All conversations which correspond to one of these PBX Agent IDs are mapped to the agent.

- **Mapping via extensions**

Use this option if one or several determined extension has been assigned to the agent.

In this case, enter at least 1 extension in the entry field *Extension*. All conversations which are made via one of these extensions are mapped to the agent.

- **Mapping extensions or PBX Agent IDs to a workplace**

Use this option of the function *Monitoring* is supposed to be available in combination with the feature *Free Seating*.

For information about the configuration of the feature *Free Seating* refer to the administration manual *Configuration Free Seating*.

### 5.2.2.2 Group field Chat

To edit the chat system data of the agent, open the group field *Chat*.

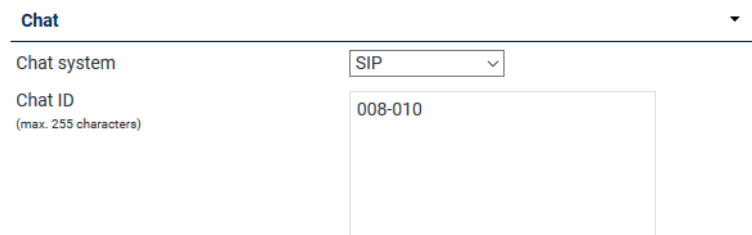


Fig. 50: Agent Data - Chat

<b>Chat system</b>	Chat server via which the agent's chats run. Select the chat server from the drop-down list.
<b>Chat ID</b>	IDs which have been saved in the chat system for the agent. By means of these IDs the recording system can identify an agent and his participation in a conversation. Enter the agent's IDs in the entry field. <b>NOTICE!</b> Use commas to separate the different IDs.

Inform your system provider that the following actions have to be carried out in the System Configuration so that chat recording is started:



- Integrations module - deactivate integration
- Recording Architectures module - deactivate recording architecture
- Recording Architectures module - activate recording architecture
- Integrations module - activate integration

#### 5.2.2.2.1 Configure chat recording

To configure the recording of the agent's chats, proceed as follows:

1. Activate the check box *Agent* in the tab *Agent Data*, see [chapter "Tab Agent Data", p. 40](#).
2. Open the group field *Chat* in the tab *Agent Data*, see [chapter "Group field Chat", p. 42](#).
3. Select the chat system from the drop-down list.
4. Enter the agent's chat ID in the entry field.

### 5.2.2.3 Group field Miscellaneous Settings

To edit the user data of the agent, open the group field *Miscellaneous Settings*.




Fig. 51: Agent Data - Miscellaneous Settings

<b>Login name</b>	Windows login name of the agent. Enter the Windows login name in the entry field.
-------------------	--

	<b>NOTICE!</b> The Windows login name is used for the following features: <ul style="list-style-type: none"> <li>• <i>Screen recording</i> (application <i>SCREENrec</i>)</li> </ul>
<i>Computer name</i>	Name of the computer that the agent uses. Enter the computer name in the entry field.  <b>NOTICE!</b> The computer name is used for the following features: <ul style="list-style-type: none"> <li>• <i>Screen recording</i> (application <i>SCREENrec</i>)</li> <li>• <i>Replay via phone</i></li> </ul>
<i>Dispatcher</i>	This function is not available yet.
<i>Video recording</i>	Select whether video recordings of the employee are supposed to be saved.  <input checked="" type="checkbox"/> = Video recordings are saved. <input type="checkbox"/> = Video recordings are not saved.  This option is only displayed if there is a video recording license in the system.

#### 5.2.2.3.1 Configure screen recording

If you would like to record the screen activities of the agent, the application *SCREENrec* has to be installed on the computer the screen of which is supposed to be recorded.

To be able to map the recorded screen activity to the agent, the application *SCREENrec* either uses the agent's *login name* or the *computer name*, see [chapter "Group field Miscellaneous Settings", p. 42](#). If both values (*login name* AND *computer name*) have been entered for the agent, the application assesses both information. The following mapping order is used: first, the system checks whether there is an agent with the indicated user name. If this is not the case, the system checks whether there is an agent with the indicated computer name.



The values for *login name* and *computer name* must be unambiguous throughout the recording system. Do neither use identical login names nor identical computer names for different agents.

**If the agent works on a remote computer and is supposed to authenticate by means of the computer name**, observe the following:

Depending on the remote desktop configuration of the remote computer, you either have to enter the name of the local computer (the agent's workplace) or the name of the remote computer (computer that the agent is working on and that the recording takes place on) as the computer name. Match the used computer name with the remote desktop configuration of the remote computer.



For information about the installation of the application *SCREENrec* and about the remote desktop configuration refer to the installation manual *Installation SCREENrec*.

#### 5.2.3 Tab Account

Here, you can display and edit the employee's login data. Upon creating an account for the employee, the other tabs are made available.

< Details\* Agent Data **Account\*** Settings Roles Individual Fu >

---

**Account** ▼

➖ Remove Account

Login name\* 8

Password\* .....

Confirm password\* .....

Change password upon the next log in ☐

Does never expire ☒

Lock account ☐

Token-Login-ID Generate

POWERplay Web for Xpert login ID Generate

**LDAP** ▶

**Combination Login** ▶

Fig. 52: Employees module - tab Account



Entering account data is optional.



Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon ➖ in the respective title bar.

1. To create a new account, open the group field *Account*.

**Account** ▼


➕ Add Account

Fig. 53: Add account

2. In the title bar of the group field, click on the button ➕ *Add Account*.
3. Enter all necessary data.

<i>User name</i>	<p>Enter the login name which is required for the employee to log in to the system.</p> <p><b>NOTICE!</b> If you use the function <i>Last Call Repeat</i>, you may use numbers only here.</p> <p><b>NOTICE!</b> If the function SSO login is used, the login name has to consist of the Windows login name and the domain. Format: <i>Domain\Windows_login_name</i></p>
<i>Password</i>	<p>Enter the password which is required for the employee to log in to the system.</p> <p><b>NOTICE!</b> If you use the function <i>Last Call Repeat</i>, you may use numbers only here.</p>
<i>Confirm password</i>	Enter the password for the employee again.
<i>Change password upon the next login</i>	Activate this option if the employee is supposed to change the password upon logging in the next time.
<i>Does never expire</i>	<p>Activate this option if the password is never supposed to expire.</p> <p><b>NOTICE!</b> This option is not available for superusers.</p>

<i>Does not have to meet the password rules</i>	<p>Activate this option if the password does not necessarily have to be consistent with the password rules.</p> <p><b>NOTICE!</b> Password rules can be defined in the Tenants module in the tab <i>Passwords</i>.</p> <p><b>NOTICE!</b> This option is not available for superusers.</p>
<i>Lock account</i>	<p>This option allows locking the employee's account.</p> <p>In the main view, you can filter for this criterion, see <a href="#">chapter "Show locked employees"</a>, p. 34.</p> <p><b>NOTICE!</b> This option is not available for superusers.</p>
<i>Token login ID</i>	<p>This function must only be configured for the replay application POWERplay Go. To generate a token login ID for employees of the tenant for replay, click on the button <i>Generate</i>. This login ID is configured to automate login for this employee.</p> <p><b>NOTICE!</b> This option is only available for tenants.</p>
<i>POWERplay Web for Xpert login ID</i>	<p>This function is only relevant for the replay application POWERplay Web for Xpert. To generate a login ID for the employees of the tenant for the replay in the Xpert client, click on the button <i>Generate</i>. This login ID is configured by the system manager of OpenScope Xpert to automate login for this employee.</p> <p><b>NOTICE!</b> This option is only available for tenants.</p>

- If you would like to remove the account, click on the button  *Remove account* in the title bar of the group field.
- To activate the authentication via LDAP for the employee, see [chapter "Authentication via LDAP"](#), p. 45.
- To assign the employee a combination user, see [chapter "Assign combination user"](#), p. 45.

### 5.2.3.1 Authentication via LDAP

- To activate the authentication via LDAP, open the group field *LDAP*.
- Activate the check box *LDAP authentication*.



Fig. 54: Activate authentication via LDAP

- Enter the complete Distinguished Name (DN) of the user in the field *LDAP DN*.
- If you would like to deactivate the authentication via LDAP again, deactivate the check box *LDAP authentication*.

- ☒ = Authentication via LDAP has been activated.  
☐ = Authentication via LDAP has not been activated.

### 5.2.3.2 Assign combination user

For safety reasons it may be sensible in some cases to assign combination users.



When assigning 1 combination user to a user, this user can only log in to the system together with the combination user.

When assigning several combination users to a user, this user can only log in to the system together with at least 1 of the combination users.

1. Open the group field *Combination Login*.
2. Click on the icon  (*Add*).

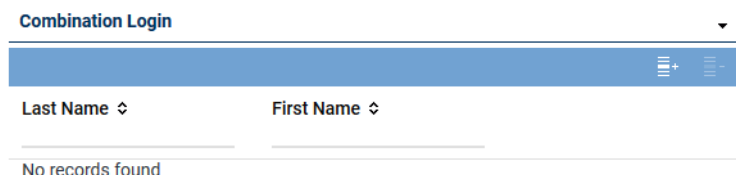
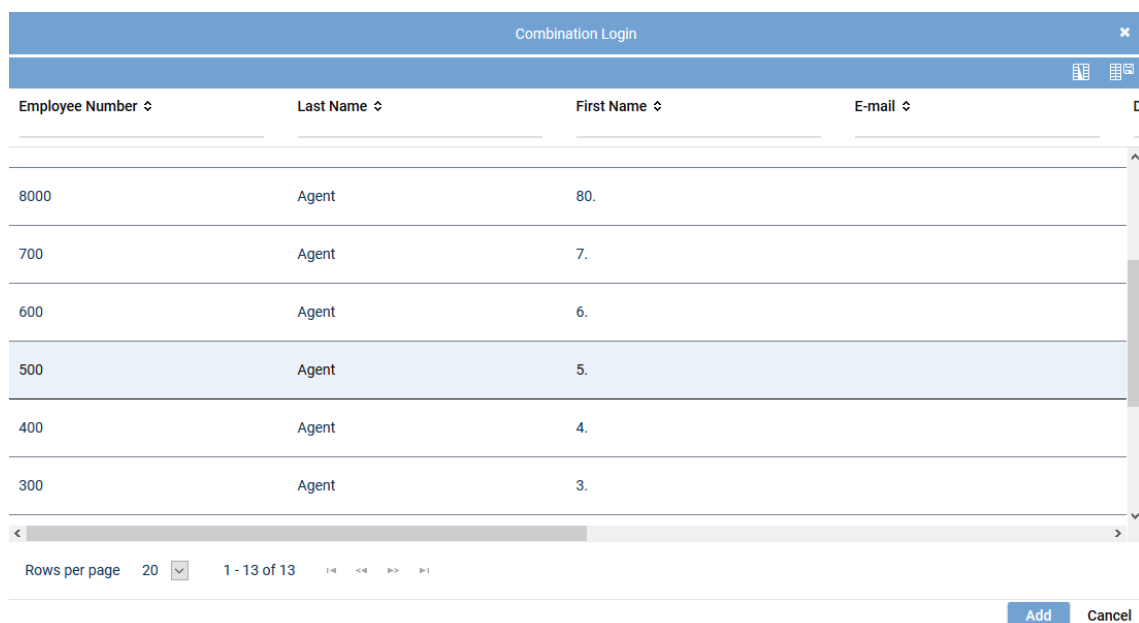


Fig. 55: Assign combination user

3. Select one or several combination users from the list.  
To select several combination users or to revoke the selection, click on the respective line while holding the [Ctrl] key down.




Employee Number	Last Name	First Name	E-mail	
8000	Agent	80.		
700	Agent	7.		
600	Agent	6.		
500	Agent	5.		<input checked="" type="checkbox"/>
400	Agent	4.		
300	Agent	3.		

Fig. 56: Add combination user

4. To add the selected combination users, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.

### 5.2.3.3 Delete combination user assignment

1. Open the group field *Combination Login*.
2. To delete the assignment of a combination user, select the respective combination user in the list and click on the icon  (*Remove*).

Combination Login

Last Name ↕	First Name ↕
Agent	5.

Fig. 57: Delete combination user assignment

### 5.2.4 Tab Settings

Here, you can display and edit the employee's rights and logging settings.

When assigning the rights, you can only select from the rights that are also available to you.

< Details\* Agent Data Account\* **Settings** Roles Individual Function Ri >

---

**Permissions** ▶

---

**Logging Settings** ▶

---

**Settings for Session Release** ▶

Fig. 58: Employees module - tab Settings

#### 5.2.4.1 Group field Permissions

**Permissions** ▼

- ☐ Superuser
- ☐ Has access to employees and their data
- ☐ INSPIRATIONneo user
- ☒ Can replay conversations
- ☐ Can delete conversations
- ☐ Activate voice disguising
- ☐ Cutoff of the calls (beginning)
 

0 Milliseconds
- ☐ Cutoff of the calls (end)
 

0 Milliseconds
- ☐ Coaching Advisor
- ☐ Deactivate employee
- ☐ Can change table configuration of the tenant

Fig. 59: Configure permissions

☒ = Right has been activated.

☐ = Right has been deactivated.

<b>Superuser</b>	This right assigns all function rights in the system to the user if their licenses are available.
------------------	---

<i>Has access to employees and their data</i>	<p>This right gives the user access to the employees' data. It depends on the individual function rights to which extent the user can edit this data.</p> <p>Without this right, the user can only see the data of other employees if he is the superior of the organization unit (see <a href="#">chapter "Tab Organization Units", p. 58</a>). In this case, he can exclusively see the data of the members of these organization units and his own data.</p>
<i>INSPIRATIONneo user</i>	<p>This right enables the user to log in to the application INSPIRATIONneo.</p> <p><b>NOTICE!</b> If this right has been deactivated, it is not possible to log in to the application INSPIRATIONneo.</p>
<i>Can replay conversations</i>	<p>This right does not only allow the user to see conversations but to replay them as well if he has the necessary rights for replaying in a replay application.</p>
<i>Can delete conversations</i>	<p>This right allows the user to delete a conversation in the application POWERplay Web.</p> <p>This option is license-dependent.</p>
<i>Activate voice disguising</i>	<p>If this check box is activated, the voices of the call participants are distorted during replay in order to render them unrecognizable while the content continues to be intelligible. Voice disguising only affects the replay, not the source data.</p>
<i>Cutoff of the calls (beginning)</i>	<p>If this check box is activated, the beginning of the call is cut off so that e. g. the welcome and the introduction are not replayed. In the entry field, enter how many milliseconds are supposed to be cut off at the beginning of the call. Cutoff only affects the replay, not the source data.</p>
<i>Cutoff of the calls (end)</i>	<p>If this check box is activated, the end of the call is cut off so that e. g. the goodbye is not replayed. In the entry field, enter how many milliseconds are supposed to be cut off at the end of the call. Cutoff only affects the replay, not the source data.</p>
<i>Coaching Advisor</i>	<p>This right allows the user to record coaching advisor sessions by means of the application CLIENTcommand.</p> <p>Coaching advisor session are simulated sessions which are recorded for training purposes. These sessions are displayed in the Coaching Advisor module of the application INSPIRATIONneo.</p> <p>For a user to be able to access the Coaching Advisor module, you have to assign the respective right in the tab <i>Individual Function Rights</i> to the user. See <a href="#">chapter "Tab Individual Function Rights", p. 53</a>.</p>
<i>Deactivate employee</i>	<p>This right allows deactivating an employee.</p> <p><input checked="" type="checkbox"/> = Employee has been deactivated.</p> <p><input type="checkbox"/> = Employee has been activated.</p> <p>A deactivated employee will not be recorded anymore.</p> <p>A deactivated employee can no longer log in to the <u>neo</u> applications.</p> <p>Changing the status of a deactivated employee is not possible before 30 days have passed.</p>
<i>Can change table configuration of the tenant</i>	<p>This right allows the user to change the default table configuration for the employees of the tenant.</p> <p>This applies to the main view of the respective modules as well as to dialog windows.</p>



Upon assigning a user superuser rights, only the following tabs are active:



- *Details*
- *Agent Data*
- *Account*
- *Settings*

In this case, no further adjustments are have to be made in any of the other tabs.

#### 5.2.4.2 Group field Logging Settings

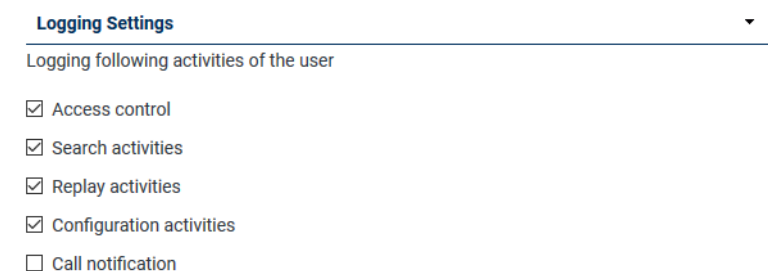


Fig. 60: Configure logging

The options of this group field allow you to log the selected activities of the user.

☒ = Logging has been activated.

☐ = Logging has been deactivated.

<i>Access control</i>	If this option has been activated, the system logs when the user has signed in to and off from the system.
<i>Search activities</i>	If this option has been activated, all search procedures of the user are logged to be able to track which conversations have been searched for.
<i>Replay activities</i>	If this option has been activated, the replay activities of the user are logged to be able to see which conversations have been replayed.
<i>Configuration activities</i>	If this option has been activated, all adjustments of the configuration on behalf of the user are logged.
<i>Call notification</i>	<p>If this option has been activated, the employee receives a notification containing the following conversation data once the conversation is over.</p> <p>Call ID, date, time from, time until, phone numbers of the participants</p> <p>The audit notification <i>EMPLOYEE_CONV_MAIL</i> must have been activated and configured. See administration manual <i>ASC System Configuration - Notifications module (for tenants)</i>.</p>

#### 5.2.4.3 Group field Settings for Session Release



This group field is only available for employees who have been defined as agents.

The subordinated group fields are not displayed before the option *Release sessions* is activated.

The options of this group field allow you to define the conditions under which agents can release sessions as well as how released sessions are supposed to be treated. Depending on these settings, the agent is prompted in the application INSPIRATION<sub>neo</sub> to release sessions for evaluation.

<b>Settings for Session Release</b>	▼
<input checked="" type="checkbox"/> Release sessions	
<b>General Settings</b>	▶
<b>Settings for the Superior</b>	▶
<b>Notification of the Agent</b>	▶

Fig. 61: Set session release for agents

<b>Release sessions</b>	<input checked="" type="checkbox"/> = Agents have to release their sessions so that they can be evaluated. The settings from the subordinated group fields are applied. <input type="checkbox"/> = Agents do not have to release sessions. The superior can see and evaluate all of the agent's sessions.
-------------------------	--

### Group field General Settings

Define the conditions under which agents release sessions

<b>General Settings</b>		▼
Minimum number of sessions of the agent*	10	
Minimum number of sessions to be released*	3	
Maximum number of sessions to be released*	5	
Period of time	Quarterly	▼

Fig. 62: Session release - General Settings

<b>Minimum number of sessions of the agent</b>	Select how many sessions of the agent have to be recorded within the defined period time at least so that the agent is prompted to release sessions for evaluation. If this minimum number has not been reached yet, no sessions of this agent are evaluated.
<b>Minimum number of sessions to be released</b>	<p>Select how many sessions the agent has to release within the defined period time at least. If the agent has released fewer sessions at the end of the period than defined here, then the missing number of sessions is transferred to the following period of time.</p> <p>Example: An agent has to release at least 3 sessions per quarter. However, at the end of the quarter he has only released 2 sessions. As a consequence, he has to release at least 4 sessions until the end of the following quarter.</p>
<b>Maximum number of sessions to be released</b>	Select how many sessions the agent can release within the defined period time at the maximum.
<b>Period of time</b>	<p>Select the period of time that the settings of the session release are supposed to refer to.</p> <p>Select the period from the drop-down list.</p>

### Group field Settings for the Superior

Select which sessions the superior can see and evaluate.

**Settings for the Superior** ▼

Access to sessions

☐ only released ones  
☒ all but only released ones can be evaluated

Fig. 63: Session release - Settings for the Superior

**Access to sessions**

Select one of the following options:

- *only released ones*  
The superior can only see the sessions that the agent has released. All other sessions are not visible for the superior.
- *all, only released ones can be evaluated*  
The superior can see all of the agent's sessions. However, he can only evaluate the sessions that the agent has released. The superior can see and replay the sessions which have not been released by the agent but he cannot evaluate them.

### Group field Notification of the Agent

Select the way and how often the agent is supposed to be informed that he has to release sessions.

**Notification of the Agent** ▼

☒ via e-mail  
☐ via CLIENTcommand

Reminder Weekly ▼

Fig. 64: Session release - Notification of the Agent

<i>via e-mail</i>	<input checked="" type="checkbox"/> = The agent is informed via e-mail. <input type="checkbox"/> = The agent is not informed via e-mail.
<i>via CLIENTcommand</i>	<input checked="" type="checkbox"/> = The agent is informed in the application CLIENT <u>command</u> . <input type="checkbox"/> = The agent is not informed in the application CLIENT <u>command</u> .
<i>Reminder</i>	Select how often the agent is supposed to be informed. Select the interval from the drop-down list.

### 5.2.5

#### Tab Roles

Here, you can assign defined roles to the employee (user).



You can define roles in the Roles module.

[Details\\*](#)
[Agent Data](#)
[Account\\*](#)
[Settings](#)
[Roles](#)
[Individual Fu >](#)

---

**Directly Assigned Roles** ▼

Name ↕	Description ↕
No records found	

**Roles By Orgaunits** ▼

Role Name
No records found


Fig. 65: Employees module - tab Roles

The assignment of a role makes the user a member of this role and gives him all the rights which have been assigned for this role.



In the Employees module, you can add individual function rights to the scope of function rights assigned to users via a role.

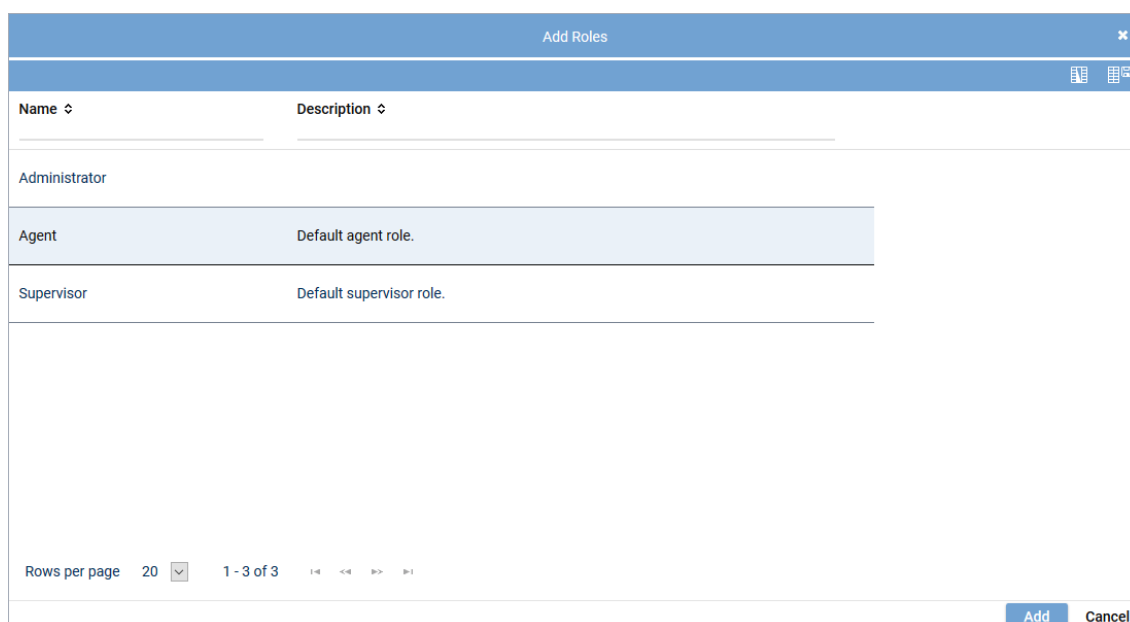
### 5.2.5.1 Assign roles

1. Click on the icon  (Add).

Name ↕	Description ↕
No records found	

Fig. 66: Assign roles

2. Select one or several roles from the list.  
To select several roles or to revoke the selection, click on the respective line while holding the [Ctrl] key down.



Name	Description
Administrator	
Agent	Default agent role.
Supervisor	Default supervisor role.

Rows per page 20 1 - 3 of 3

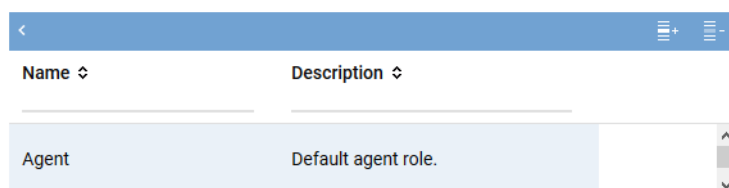
Add Cancel

Fig. 67: Add role

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

### 5.2.5.2 Delete role assignment

- Select the role you would like to remove from the list and click on the icon  (*Remove*).



Name	Description
Agent	Default agent role.

Remove

Fig. 68: Delete role assignment



A change in the role assignment only comes into effect after the user has logged off from and in to the system again.

### 5.2.6 Tab Individual Function Rights

Here, you can display and assign the employee's individual function rights.

< Roles	Individual Function Rights	Conversation Rules	Organization Units
INSPIRATIONneo			▸
REPORTneo			▸
System Configuration			▸
POWERplay Web			▸
POWERplay Pro			▸
POWERplay Instant			▸
INSIGHTneo			▸
Additional data			▸
Player function rights			▸
System Monitoring			▸

Fig. 69: Employees module - tab Individual Function Rights (example)

You can assign the function rights for the different *neo* applications individually.

- To adjust the function rights to an application, open the group field with the respective application name.
  - ⇒ All sections of the application are listed.

System Configuration	▼
<input type="checkbox"/> All function rights for System Configuration	
User Configuration	+
Tenants	+

Fig. 70: Function rights - display sections (example)

- If you would like to assign a user all function rights to an application at once, activate the check box *All function rights for ....* This right is superior and applies to all modules of this application.




The option to assign all function rights at once is not available for all applications.

- If you would like to assign the function rights selectively, open the details of a sub-section (e. g. a module) by clicking on the icon “+” in the line with the respective text.
  - ⇒ All function rights of this sub-section are displayed.

System Configuration ▾




☐ All function rights for System Configuration

User Configuration -

Name	Type	Role
<input type="checkbox"/> Can configure users		

Tenants +

Fig. 71: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. <input checked="" type="checkbox"/> = individual function right <input type="checkbox"/> = no individual function right
Name	Description of the function right.
Type	Shows which license is required for this right.  = agent license  = supervisor license  = basic license (without agent or supervisors rights)
Role	Shows whether the function right has been assigned to the user via a role (role right). no mark = no role right <input checked="" type="checkbox"/> = role right <b>NOTICE!</b> In the window <i>Summary</i> , you can see via which role the function right has been assigned, see <a href="#">chapter "Show summary", p. 33</a> .

Tab. 1: Function rights

- To assign all function rights for a sub-section, activate the respective check box *All function rights for ....*  
To assign merely single function rights, only activate the check box of the function rights you would like to assign.
- If you would like to hide the details in a sub-section, click on the icon “-” in the line with the respective text.

The individual function rights are largely self-explanatory. In the following you will find the description of the non-self-explanatory function rights.

**Group field INSPIRATIONneo > Evaluation templates**  
**Group field INSPIRATIONneo > Training package templates**  
**Group field INSPIRATIONneo > Quiz templates**

Can remove editing locks	<p>This function right allows removing edit locks.</p> <p>When a user edits a template, an editing lock is set for this template so that the locked template cannot be edited by other users at the same time. In case the editing lock remains in place for any reason even if no user is editing the template (e. g. when the browser is closed), this function right allows you to remove the editing lock.</p>
--------------------------	--

Tab. 2: Function rights INSPIRATIONneo &gt; Evaluation templates





By assigning conversation rules, you can define which conversations the employee may see. Conversation rules take effect in the following applications and modules:

Application	Module
POWER <del>play</del> Web	<ul style="list-style-type: none"> <li>• Conversation module</li> <li>• Participant View module</li> </ul>
POWER <del>play</del> Pro	<ul style="list-style-type: none"> <li>• Conversation module</li> <li>• Participant View module</li> </ul>
INSPIRATION <del>neo</del>	<ul style="list-style-type: none"> <li>• Sessions module</li> <li>• Calibrations module</li> <li>• Audio Analysis module</li> </ul>

### Group field Directly Mapped Rules

Here, you see all conversation rules which have been mapped to the employee individually. You can change the mapping of individually mapped conversation rules arbitrarily. See [chapter "Assign conversation rules", p. 57](#) and [chapter "Delete conversation rule assignment", p. 58](#).

### Group field Rules Mapped via a Role

Here, you see all conversation rules which have been mapped to the employee on basis of his roles. All conversation rules of a role are automatically applied to the employee if he has been mapped a role.

Conversation rules are mapped to the roles in the Roles module.

#### 5.2.7.1 Assign conversation rules

1. In the group field *Directly Mapped Rules* click on the icon  (Add).

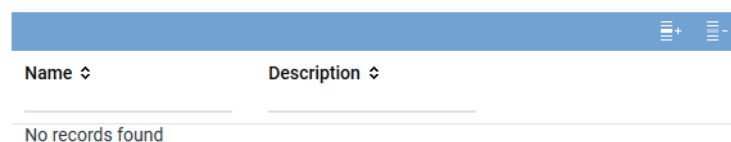


Fig. 73: Assign conversation rule


2. Select one or several conversation rules from the list.  
To select several conversation rules or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Assigned Conversation Rules		
Name ↕	Description ↕	Creator ↕
1w 10 min	Conversations last week > 10 min	Admin, 1st-Tenant
Agent Group 1	Agents 4 and 9	Admin, 1st-Tenant
Agent 9 internal	Agent 9 - internal conversations	Admin, 1st-Tenant
<div> Rows per page 20 ▾ 1 - 3 of 3 </div>		
		Add Cancel

Fig. 74: Add conversation rules

- To add the selected conversation rules, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.

### 5.2.7.2 Delete conversation rule assignment

- Select the conversation rule you would like to remove from the list and click on the icon  (*Remove*).

Name ↕	Description ↕
Agent 9 internal	Agent 9 - internal conversations
Agent Group 1	Agents 4 and 9

Fig. 75: Delete conversation rule assignment

### 5.2.8 Tab Organization Units

Here, you can assign predefined organization units to the employee (user).



You can define organization units in the Organization Structure module.

If a user has the right *Has access to employees and their data* (see [chapter "Tab Settings", p. 47](#)) and has been assigned to an organization unit as a superior, he can see the data of the employees who are members of this organization unit. He cannot see employees or data of other organization units.

[Roles](#)
[Individual Function Rights](#)
[Conversation Rules](#)
[Organization Units](#)

---

**Access To** ▼

Name ↕	Description ↕
Sales Europe	

**Member Of** ▼

Name ↕	Description ↕
Sales	
Sales America	

Fig. 76: Employees module - tab Organization Units


### Group field Access To

Here, you see the organization units that the employee has been mapped to as superior. You can change the mapping arbitrarily. See [chapter "Assign organization units", p. 59](#) and [chapter "Delete organization unit assignment", p. 60](#).

### Group field Member Of

Here, you see the organization units that the employee has been mapped to as member. You can change the mapping arbitrarily. See [chapter "Assign organization units", p. 59](#) and [chapter "Delete organization unit assignment", p. 60](#).

#### 5.2.8.1 Assign organization units

1. Click on the icon  (Add).

Name ↕	Description ↕
No records found	

Fig. 77: Assign organization units

2. Select one or several organization units from the list.  
To select several organization units or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

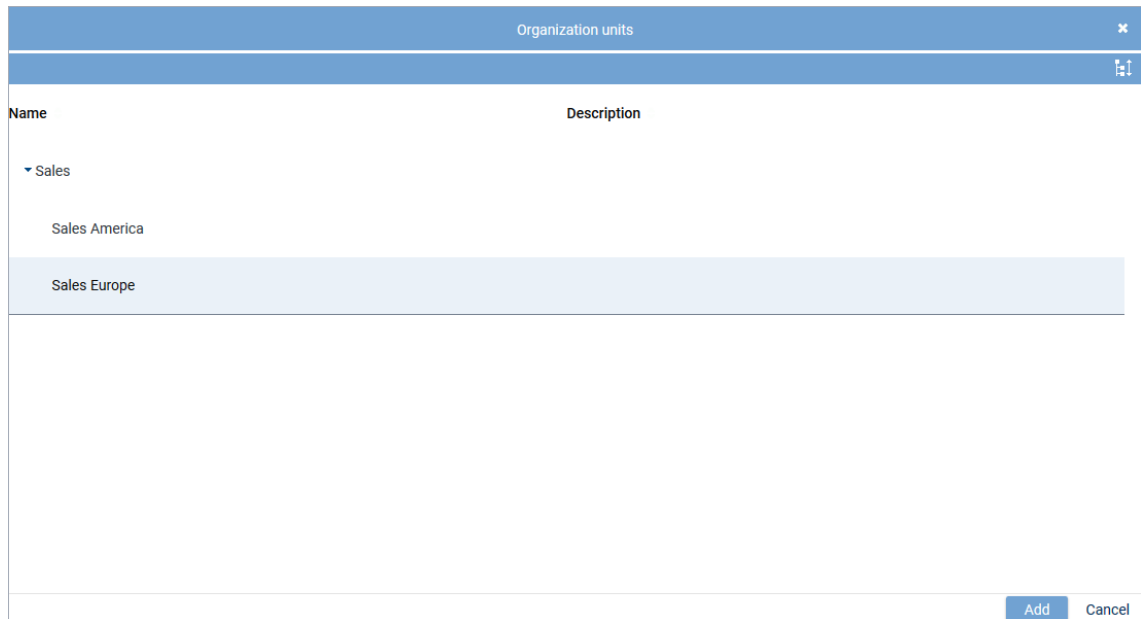





Fig. 78: Add organization units




If you click on the icon  in the window *Organization Units*, you can expand the display of the organization structure so that all organizational levels are visible or you can reduce them so that only the 1st organizational level is visible.

By clicking on the icon  or  in front of an organization unit, you can show or hide the sub-units of this organization unit.

- To add the selected organization units, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.

### 5.2.8.2 Delete organization unit assignment

- Select the organization unit you would like to remove from the list and click on the icon  (*Remove*).

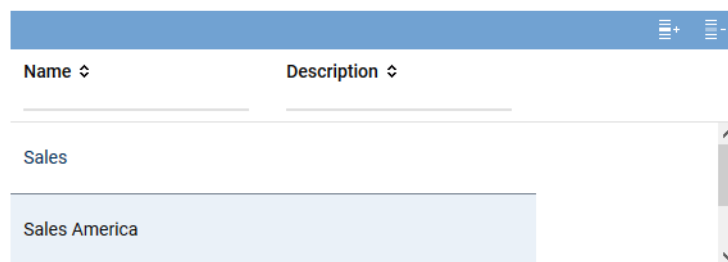



Fig. 79: Delete organization unit assignment

## 5.3 Create new employee

- Click on the icon  (*Add*) in the toolbar.
- Adjust all settings in the tabs of the detail view as described in the respective chapters.  
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button *Save* to save the settings.  
To discard the entries, click on the button *Reset*.

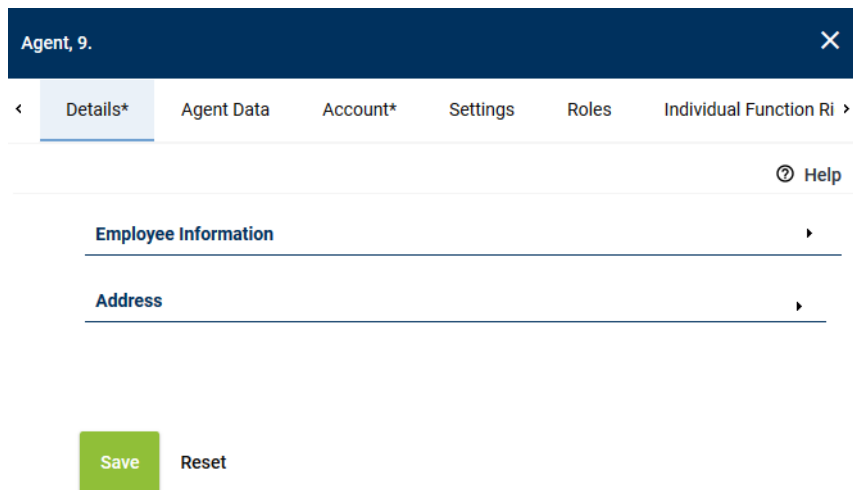


Fig. 80: Save employee

As long as no user account (tab *Account*) exists for the employee, only the following tabs are available for this employee:



- *Details*
- *Agent Data*
- *Account*


#### 5.4

##### Edit employee

1. In the main view, select the employee for whom you would like to edit the data.
2. Make all necessary changes in the tabs of the detail view.  
You can change tabs without buffering without risking the loss of your settings.
3. Once you have finished adjusting the settings, click on the button *Save* to save the settings.  
To discard the entries, click on the button *Reset*.

#### 5.5

##### Delete employee

1. In the main view, select the employee you would like to delete.
2. Click on the icon  (*Delete*) in the toolbar.
3. To really delete the selected employee, confirm the security prompt.



If the deleted employee had been assigned as combination user, you receive a corresponding warning.



If you delete employees while they are logged in as user in the system, the deletion of the profile will come into effect after they have logged off from the system.

#### 5.6

##### Create new employee with OAuth login

*neo* supports the login procedure OAuth2 OpenID Connect. If OAuth has been configured for *neo*, *neo* opens the OAuth authorization website configured in the application System Configuration in the default browser upon starting where users can then log in. Upon successful authentication, the user is logged in to the application *neo*.


Before this configuration, the OAuth login for the system must be activated by the administrator of the system provider in the Tenants module of the application System Configuration.



---

For information about the configuration refer to the administration manual *System Configuration - User management for system providers*.

---

1. Click on the icon  (*Add*) in the toolbar.
2. Adjust the required settings in the tabs of the detail view as described in the corresponding chapters..  
You can change tabs without buffering without risking to lose already entered data.
3. Assign the employee the same user name (login name) that is also used on the corresponding OAuth website. **WARNING!** The password should **NOT** be the same as on the OAuth website.
4. Click on the button *Save* to save the entries.  
Click on the button *Cancel* to discard the entries.

---

As long as no user account (tab *Account*) exists for the employee, only the following tabs are available for this employee:



- *Details*
- *Agent Data*
- *Account*



---

Once this configuration has been completed, neo can exclusively be used with a valid OAuth login.

---

## 6 Organization Structure module

In the Organization Structure module, you can display the organization units of your company in any structure. You can assign members and superiors to the individual organization units. This will clearly show which employee works for which organization units and which position he has there.



You can add agents as members (*member of*) of organization units only.

Users who are no agents can only be added as superiors (*access to*) of organization units.

Users can be member and superior of the same organization unit at the same time.



You can import user data from existing [LDAP](#) structures, too. The import is configured via the Configuration Import module. For more information refer to the administration manual *Import of user data*.

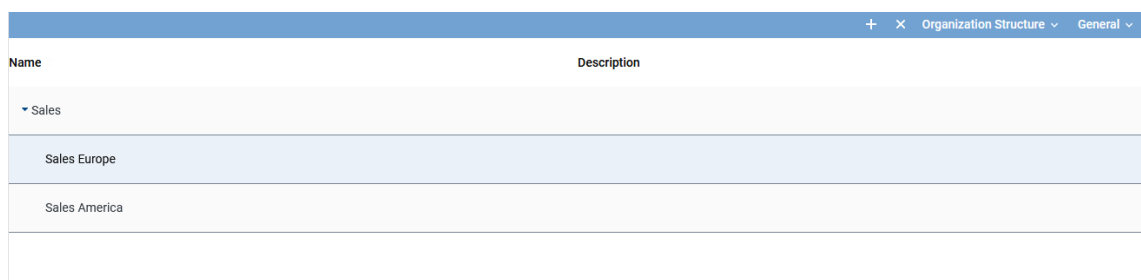


You can import configuration data from existing [LDAP](#) structures, too. The import is configured in the Configuration Import module. For further information refer to the administration manual *Import of configuration data*.

Open the Organization Structure module by clicking on the menu item *Organization Structure* in the navigation bar of the application System Configuration.

### 6.1 Main view

All saved organization units are displayed in the main view.





Name	Description
▼ Sales	
Sales Europe	
Sales America	

Fig. 81: Organization Structure module - main view

The following information is displayed in the main view:

<i>Name</i>	Name of the organization unit.
<i>Description</i>	Description of the organization unit.





By clicking on the icon  or  in front of an organization unit, you can show or hide the sub-units of this organization unit.

#### 6.1.1 Toolbar



Fig. 82: Organization Structure module - toolbar

In the following, you find a description of the icons.

	<i>Create</i>	Creates a new organization unit (see <a href="#">chapter "Create new organization unit", p. 68</a> ).
	<i>Delete</i>	Deletes the selected organization unit (see <a href="#">chapter "Delete organization unit", p. 69</a> ).

<i>Organization Structure</i>	<i>Expand/Collapse all nodes</i>	Opens or closes the entire organization structure including its subordinated organization units.
<i>General</i>	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



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

## 6.2

### Detail view

The detail view contains additional information about the selected organization unit.

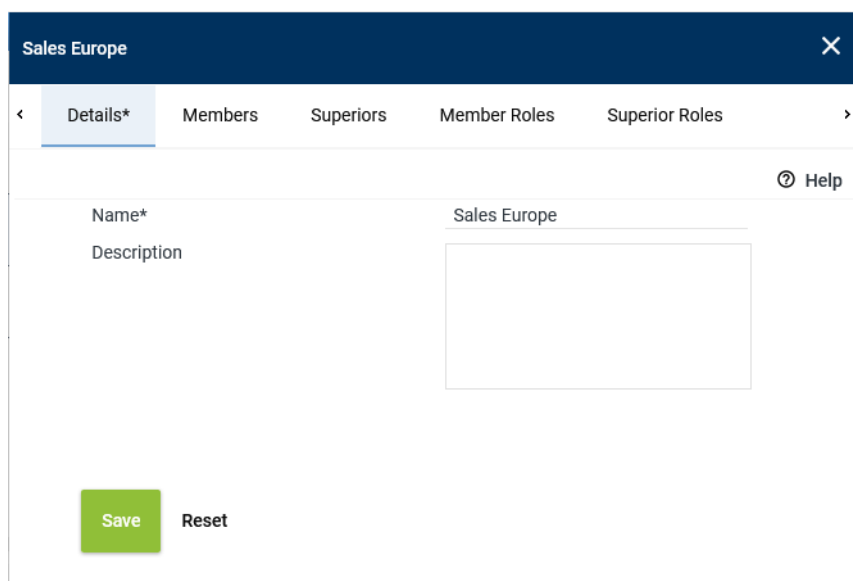


Fig. 83: Organization Structure module - detail view

The detail view consists of the following tabs:

- *Details*  
Here, you can display and edit the name and the description of the organization unit.  
See [chapter "Tab Details", p. 65](#).
- *Members*  
Here, you can display the members of the organization unit and edit the member assignment.  
See [chapter "Tab Members", p. 65](#).
- *Superiors*  
Here, you can display the superiors of the organization unit and edit the superiors' assignment.  
See [chapter "Tab Superiors", p. 66](#).
- *Member Roles*  
Here, you can display the roles for the members of the organization unit and edit the role assignment.  
See [chapter "Tab Member Roles", p. 67](#).
- *Superior Roles*  
Here, you can display the roles for the superiors of the organization unit and edit the role assignment.



See [chapter "Tab Superior Roles"](#), p. 68.

### 6.2.1 Tab Details

Here, you can display and edit the name and the description of the organization unit.

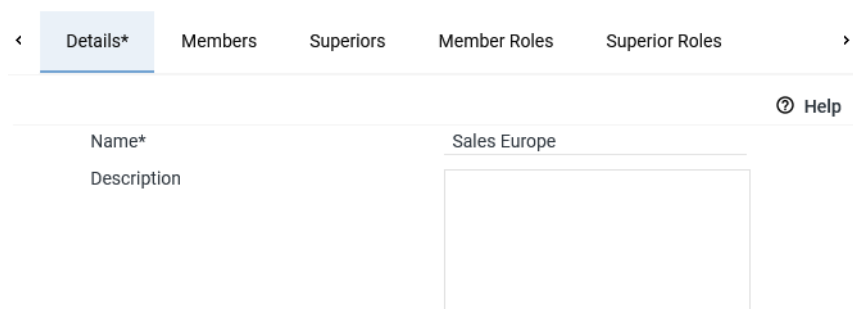
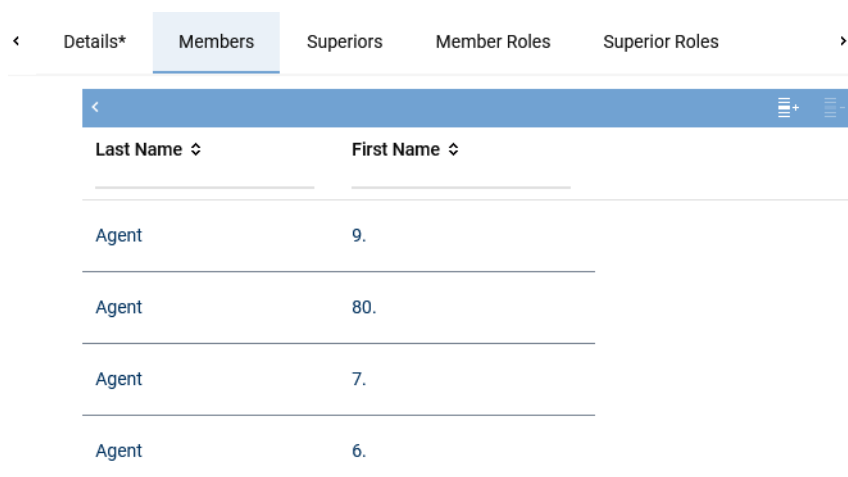


Fig. 84: Organization Structure module - tab Details

<b>Name</b>	Name of the organization unit.
<b>Description</b>	Description of the organization unit.

### 6.2.2 Tab Members


Here, you can display the members of the organization unit and edit the member assignment.

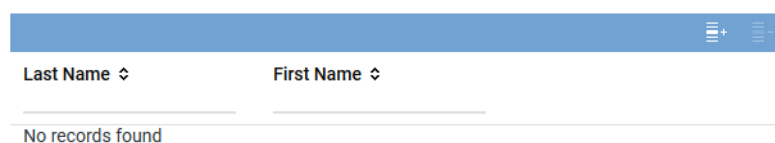


Last Name ↕	First Name ↕
Agent	9.
Agent	80.
Agent	7.
Agent	6.

Fig. 85: Organization Structure module - tab Members

#### 6.2.2.1 Assign members

1. Click on the icon  (Add).



Last Name ↕	First Name ↕
No records found	

Fig. 86: Assign users


- Select one or several users from the list.  
To select several users or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Employee Number ▾					
First Name ▾					
Last Name ▾					
E-mail ▾					
Date of Entry ▾					
Date of Birth ▾					
1100	11.	Agent-Superior			
1000	10.	Agent			
900	9.	Agent			
800	8.	Agent			
700	7.	Agent			
600	6.	Agent			
500	5.	Agent			
Rows per page 20 ▾ 1 - 11 of 11 < << >> >					
Add Cancel					

Fig. 87: Add user

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

### 6.2.2.2 Delete member assignment

- Select the user you would like to remove from the list and click on the icon  (*Remove*).

Last Name ▾	
First Name ▾	
Agent	9.

Fig. 88: Delete user assignment

### 6.2.3 Tab Superiors

Here, you can display the superiors of the organization unit and edit the superiors' assignment.

<	Details*	Members	Superiors	Member Roles	Superior Roles	>
Last Name ▾						
First Name ▾						
Agent	80.					
Agent	9.					

Fig. 89: Organization Structure module - tab Superiors

### 6.2.3.1 Assign superiors

1. Click on the icon  (*Add*).

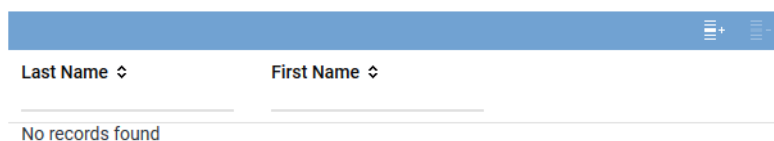
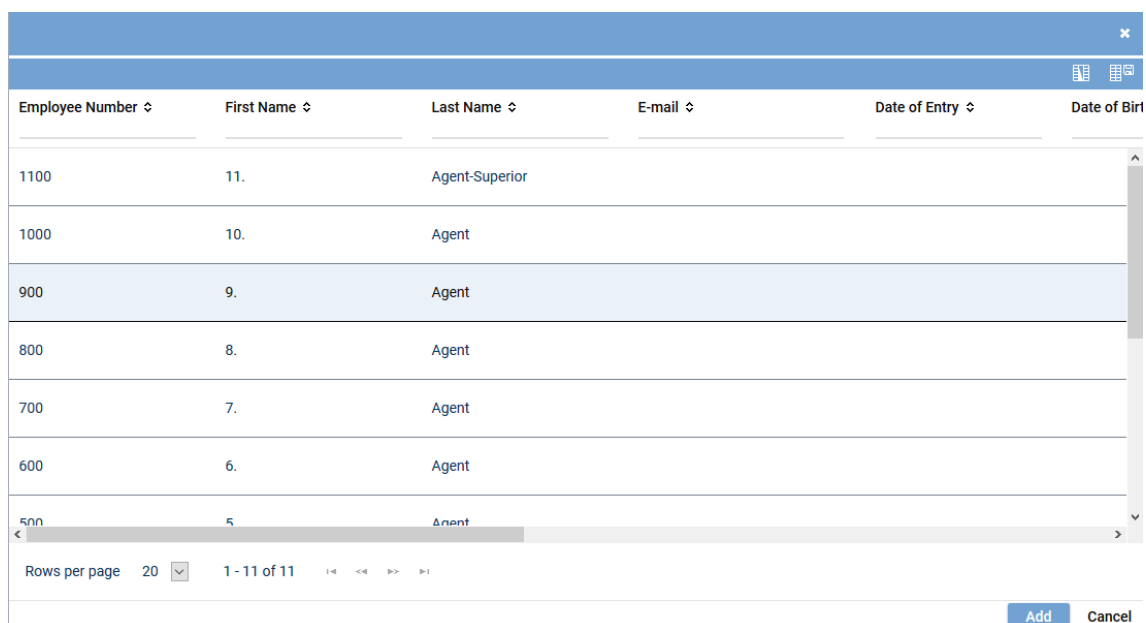


Fig. 90: Assign users

2. Select one or several users from the list.  
To select several users or revoke a selection, click on the respective line while holding the [Ctrl] key down.




Employee Number	First Name	Last Name	E-mail	Date of Entry	Date of Birth
1100	11.	Agent-Superior			
1000	10.	Agent			
900	9.	Agent			
800	8.	Agent			
700	7.	Agent			
600	6.	Agent			
500	5.	Agent			

Fig. 91: Add user

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

### 6.2.3.2 Delete superior assignment

1. Select the user you would like to remove from the list and click on the icon  (*Remove*).

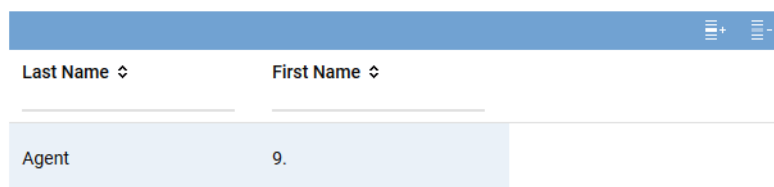


Fig. 92: Delete user assignment

### 6.2.4 Tab Member Roles

Here, you can display the roles for the members of the organization unit and edit the role assignment.

<	Details*	Members	Superiors	Member Roles	Superior Roles	>
---	----------	---------	-----------	--------------	----------------	---

<			+	...
Name ↕	Description ↕			
Agent	Default agent role.			

Fig. 93: Organization Structure module - tab Member Roles

For a description of how to add roles, see [chapter "Assign roles"](#), p. 52.

For a description of how to remove roles, see [chapter "Delete role assignment"](#), p. 53.

### 6.2.5 Tab Superior Roles

Here, you can display the roles for the superiors of the organization unit and edit the role assignment.

<	Details*	Members	Superiors	Member Roles	Superior Roles	>
---	----------	---------	-----------	--------------	----------------	---

<			+	...
Name ↕	Description ↕			
Supervisor	Default supervisor role.			

Fig. 94: Organization Structure module - tab Superior Roles

For a description of how to add roles, see [chapter "Assign roles"](#), p. 52.


For a description of how to remove roles, see [chapter "Delete role assignment"](#), p. 53.

## 6.3 Create new organization unit

1. Select an organization unit for which you would like to create a sub-unit.



If you would like to create an organization unit on the first level, no organization unit may be selected (marked) in the main view. To revoke the selection, if required, click on the respective line while holding the [Ctrl] key.

2. Click on the icon  (Create) in the toolbar.
3. Adjust all settings in the tabs of the detail view as described in the respective chapters (see [chapter "Detail view"](#), p. 64).  
You can change tabs without buffering without risking the loss of your settings.
4. Once you have finished adjusting the settings, click on the button Save to save the settings.  
To discard the entries, click on the button Reset.

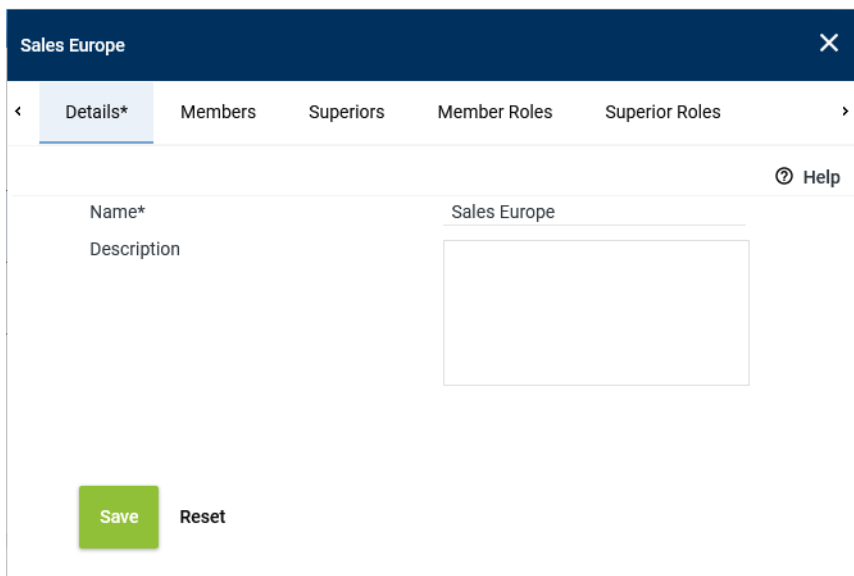


Fig. 95: Save organization unit

#### 6.4 Edit organization unit

1. In the main view, select the organization unit you would like to edit.
2. Make all necessary changes in the tabs of the detail view, see [chapter "Detail view", p. 64](#). You can change tabs without buffering without risking the loss of your settings.
3. Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.

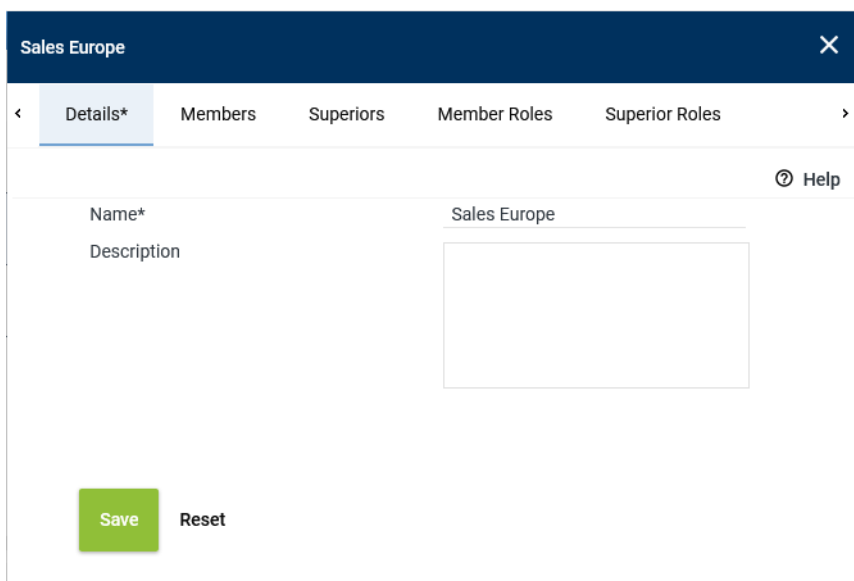



Fig. 96: Save changes

#### 6.5 Delete organization unit

1. In the main view, select the organization unit you would like to delete.
2. Click on the icon  (*Delete*) in the toolbar.
3. To really delete the selected organization unit, confirm the security prompt.



When deleting an organization unit, the subordinate organization units are deleted, too.

In the Roles module, you can create different roles and assign selected function rights for the different applications to these roles.

By assigning users a role, you automatically assign them all function rights of this role. By assigning users several roles, you automatically assign them the sum of all function rights which are included in these roles.

The following roles are set up by default in the *neo* system:

- Role *Agent*

The default role for agents grants users access to their own data only, e. g. their sessions, evaluations, and training packages in the following modules of the application INSPIRATION*neo*:

- Evaluations module
- Sessions module
- E-Learning module

- Role *Supervisor*

The default role for supervisors allows users to access all data and functions in all modules of the application INSPIRATION*neo*.

These roles cannot be changed. However, you can define as many additional roles as necessary.



In the Employees module, you can add individual function rights to the scope of function rights assigned to users via a role.

The default roles *Agent* and *Supervisor* cannot be changed. To deactivate individual function right which are not wanted in a default role, duplicate the role and make the respective changes in the duplicate (see [chapter "Duplicate role", p. 78](#)). Make sure that employees are only assigned the role (default role or duplicate) they are supposed to have.



You can import user data from existing [LDAP](#) structures, too. The import is configured via the Configuration Import module. For more information refer to the administration manual *Import of user data*.



You can import configuration data from existing [LDAP](#) structures, too. The import is configured in the Configuration Import module. For further information refer to the administration manual *Import of configuration data*.

Open the Roles module by clicking on the menu item *Roles* in the navigation bar of the application System Configuration.

In the main view, all saved roles are displayed.

+ X Roles General	
Name	Description
Administrator	
Agent	Default agent role.
Supervisor	Default supervisor role.
Rows per page 50 1 - 3 of 3	

Fig. 97: Roles module - main view

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

<i>Name</i>	Name of the role.
<i>Description</i>	Description of the role.
<i>Creation Date</i>	Date on which the role was created.
<i>Updated</i>	Date on which the role was updated for the last time.






### 7.1.1

#### Toolbar

The toolbar offers the following functions.



Fig. 98: Roles module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see <a href="#">chapter "Search", p. 34</a> . The icon  (Search) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new role (see <a href="#">chapter "Create new role", p. 77</a> ).
	<i>Delete</i>	Deletes the selected role (see <a href="#">chapter "Delete role", p. 79</a> ).
<i>Roles</i>	<i>Duplicate with Employees</i>	Creates a copy of the selected role (see <a href="#">chapter "Duplicate role", p. 78</a> ).
	<i>Duplicate Without Employees</i>	Creates a copy of the selected role (see <a href="#">chapter "Duplicate role", p. 78</a> ).
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.

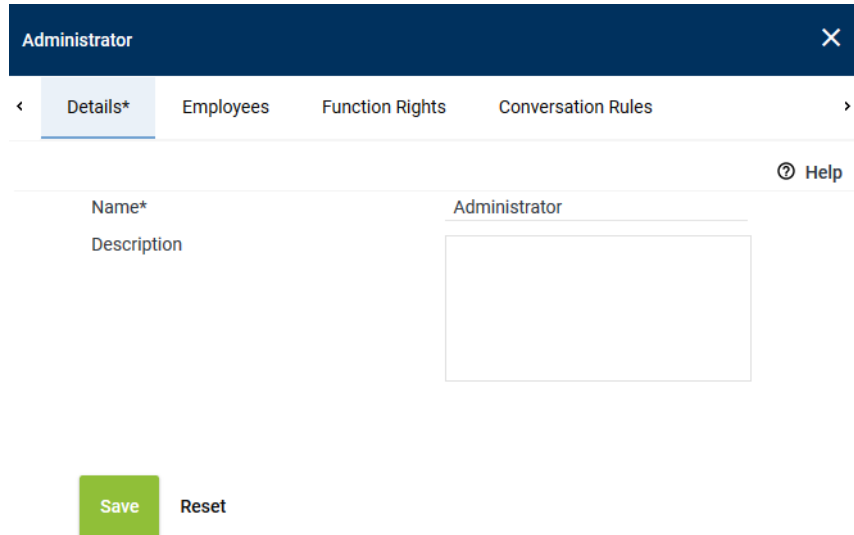


For detailed information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

## 7.2

### Detail view

The detail view contains data and information about the selected role.



The screenshot shows the 'Administrator' role detail view. At the top, there's a dark blue header with the role name 'Administrator' and a close button. Below the header is a tabbed interface with four tabs: 'Details\*' (selected), 'Employees', 'Function Rights', and 'Conversation Rules'. To the right of the tabs is a 'Help' icon. The 'Details\*' tab contains two input fields: 'Name\*' with the value 'Administrator' and 'Description' with an empty text area. At the bottom left, there are two buttons: a green 'Save' button and a 'Reset' button.

Fig. 99: Roles module - detail view

The detail view consists of the following tabs:

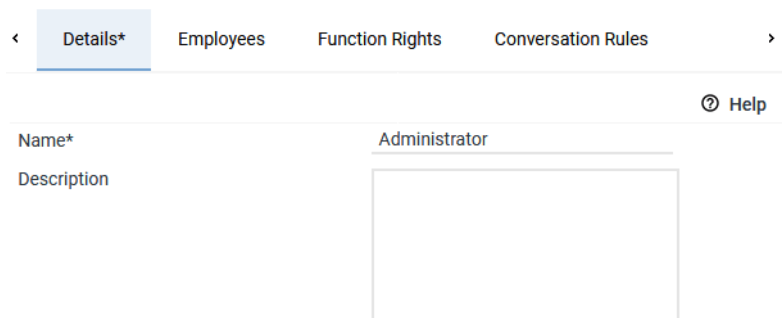
- *Details*  
Here, you can display and edit the name and the description of the role.  
See [chapter "Tab Details", p. 72](#).
- *Employees*  
Here, you can display the users who have been assigned the role and edit the user assignment.  
See [chapter "Tab Employees", p. 73](#).
- *Function Rights*  
Here, you can display and assign the function rights of the role.  
See [chapter "Tab Function Rights", p. 74](#)
- *Conversation Rules*  
Here, you can display and assign the conversation rules of the role.  
See [chapter "Tab Conversation Rules", p. 76](#).

### 7.2.1

#### Tab Details

Here, you can display and edit the name and the description of the role.





The screenshot shows the 'Details\*' tab in the Roles module. It features a 'Name\*' field with the value 'Administrator' and a 'Description' field which is currently empty. A 'Help' icon is visible in the top right corner of the form area.

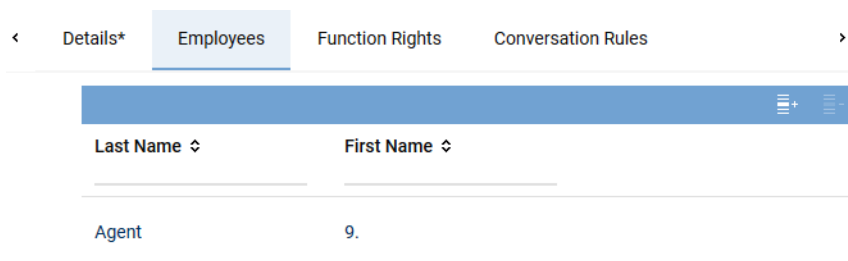
Fig. 100: Roles module - tab Details

<b>Name</b>	Name of the role.
<b>Description</b>	Description of the role.

## 7.2.2 Tab Employees

Here, you can assign selected employees (users) to the role.

The assignment of a role makes the user a member of this role and gives him all the rights which have been assigned for this role.



The screenshot shows the 'Employees' tab in the Roles module. It displays a table with two columns: 'Last Name' and 'First Name'. The first row shows 'Agent' and '9.'. There is a blue header bar at the top of the table area with a '+' icon and a list icon.

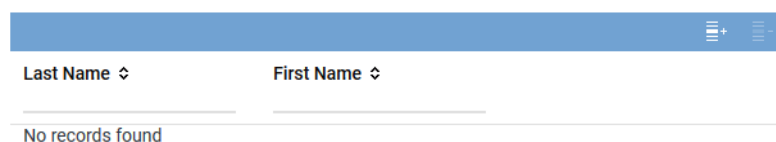
Fig. 101: Roles module - tab Employees



In the Employees module, you can add individual function rights to the scope of function rights assigned to users via a role.

### 7.2.2.1 Assign users

1. Click on the icon  (Add).



The screenshot shows the 'Employees' tab in the Roles module. It displays a table with two columns: 'Last Name' and 'First Name'. Below the table, it says 'No records found'. There is a blue header bar at the top of the table area with a '+' icon and a list icon.

Fig. 102: Assign users


2. Select one or several users from the list.  
To select several users or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Employee Number ↕	First Name ↕	Last Name ↕	E-mail ↕	Date of Entry ↕	Date of Birth ↕
1100	11.	Agent-Superior			
1000	10.	Agent			
900	9.	Agent			
800	8.	Agent			
700	7.	Agent			
600	6.	Agent			
500	5.	Agent			
Rows per page 20 1 - 11 of 11					
					Add Cancel

Fig. 103: Add user

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

### 7.2.2.2 Delete user assignment

- Select the user you would like to remove from the list and click on the icon  (*Remove*).

Last Name ↕		First Name ↕	
Agent		9.	

Fig. 104: Delete user assignment

### 7.2.3 Tab Function Rights

Here, you can display and assign the function rights of the role.

<	Details*	Employees	Function Rights	Conversation Rules	>
			INSPIRATIONneo		▸
			System Configuration		▸
			POWERplay Web		▸
			POWERplay Pro		▸
			POWERplay Instant		▸
			INSIGHTneo		▸
			Additional data		▸
			Player function rights		▸
			System Monitoring		▸

Fig. 105: Roles module - tab Function Rights (example)

- To adjust the function rights to an application, open the group field with the respective application name.  
⇒ All sections of the application are listed.

System Configuration	▼
<input type="checkbox"/> All function rights for System Configuration	
User Configuration	+
Tenants	+

Fig. 106: Function rights - display sections (example)

- If you would like to assign a user all function rights to an application at once, activate the check box *All function rights for ....* This right is superior and applies to all modules of this application.



The option to assign all function rights at once is not available for all applications.

- If you would like to assign the function rights selectively, open the details of a sub-section (e. g. a module) by clicking on the icon “+” in the line with the respective text.  
⇒ All function rights of this sub-section are displayed.

<b>System Configuration</b> ▼	
<input type="checkbox"/> All function rights for System Configuration	
<b>User Configuration</b> -	
<b>Name</b>	<b>Type</b>
<input type="checkbox"/> Can configure users	👤
<b>Tenants</b> +	

Fig. 107: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. <input checked="" type="checkbox"/> = individual function right <input type="checkbox"/> = no individual function right
<b>Name</b>	Description of the function right.
<b>Type</b>	Shows which license is required for this right. 👤 = agent license 👤👤 = supervisor license 👤👤👤 = basic license (without agent or supervisors rights)

Tab. 4: Function rights

- To assign all function rights for a sub-section, activate the respective check box *All function rights for ....*  
To assign merely single function rights, only activate the check box of the function rights you would like to assign.
- If you would like to hide the details in a sub-section, click on the icon “-” in the line with the respective text.

### 7.2.4 Tab Conversation Rules

Here, you can display and assign the conversation rules of the role.



Conversation rules can be defined in the Conversation Rules module.

<

Details\*

Employees

Function Rights

Conversation Rules

>

<

+

⋮

⋮

Name ⚙

Description ⚙

No records found

Fig. 108: Roles module - tab Conversation Rules Object Rules

By assigning conversation rules, you can define which conversations may be seen by the members of the role.

#### 7.2.4.1 Assign conversation rules

- In the group field *Directly Mapped Rules* click on the icon  (Add).

Name ↕		Description ↕	
No records found			

Fig. 109: Assign conversation rule

- Select one or several conversation rules from the list.  
To select several conversation rules or revoke a selection, click on the respective line while holding the [Ctrl] key down.

Assigned Conversation Rules

Name	Description	Creator
1w 10 min	Conversations last week > 10 min	Admin, 1st-Tenant
Agent Group 1	Agents 4 and 9	Admin, 1st-Tenant
Agent 9 internal	Agent 9 - internal conversations	Admin, 1st-Tenant

Rows per page

20

1 - 3 of 3


Add

Cancel

Fig. 110: Add conversation rules

- To add the selected conversation rules, click on the button *Add*.  
To discard the selection and close the window, click on the button *Cancel*.


#### 7.2.4.2 Delete conversation rule assignment

- Select the conversation rule you would like to remove from the list and click on the icon  (*Remove*).

Name ↕		Description ↕	
Agent 9 internal	Agent 9 - internal conversations		
Agent Group 1	Agents 4 and 9		

Fig. 111: Delete conversation rule assignment

### 7.3 Create new role

- Click on the icon  (*Create*) in the toolbar.
- Adjust all settings in the tabs of the detail view as described in the respective chapters.  
You can change tabs without buffering without risking the loss of your settings.

- Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.

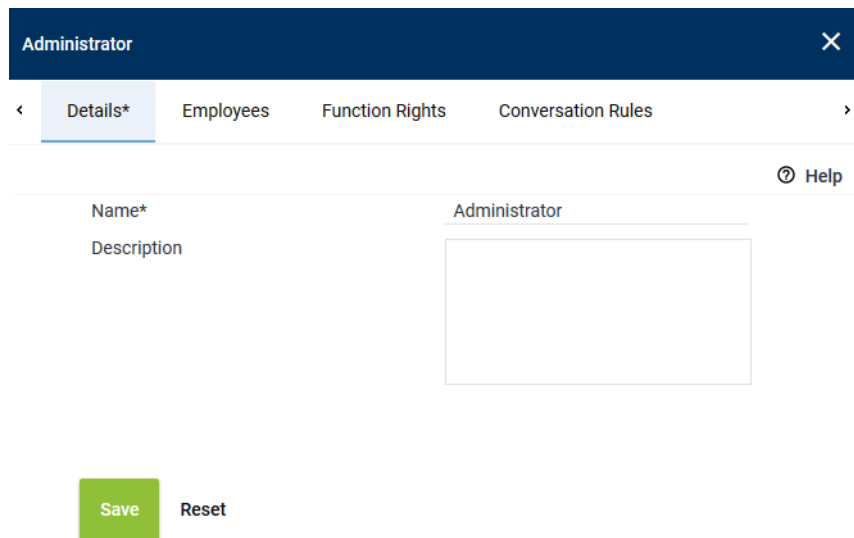


Fig. 112: Save role

#### 7.4

#### Duplicate role

- In the main view, select the role you would like to duplicate.
- Click on the menu *Roles* in the toolbar.
- Select one of the following options:

<i>Duplicate with Employees</i>	Creates a copy of the selected role with the assigned employee.
<i>Duplicate Without Employees</i>	Creates a copy of the selected role without the assigned employee.

- A copy of the role is created in the detail view.
- Enter a new name for the copied role.
- Adjust all settings in the tabs of the detail view as described in the respective chapters (see [chapter "Detail view", p. 72](#)).  
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.

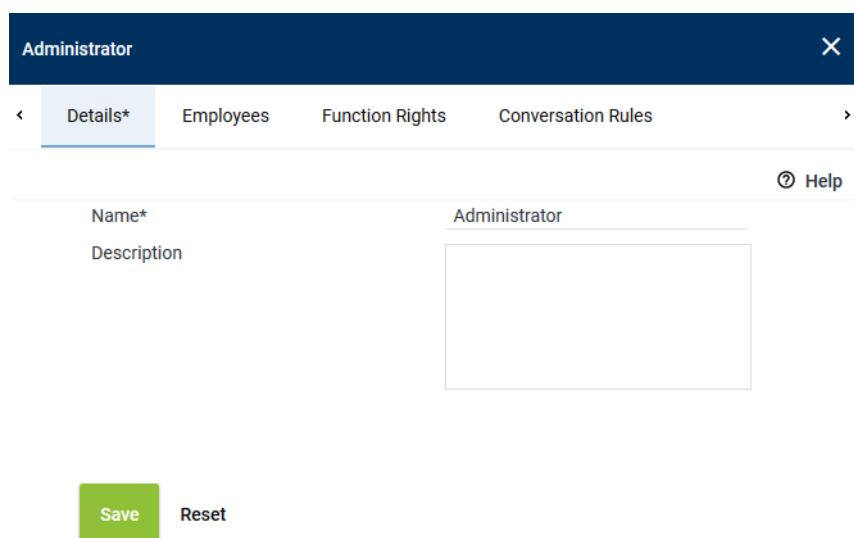


Fig. 113: Save role

## 7.5

### Edit role

1. In the main view, select the role you would like to edit.
2. Make all necessary changes in the tabs of the detail view, see [chapter "Detail view", p. 72](#). You can change tabs without buffering without risking the loss of your settings.
3. Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.

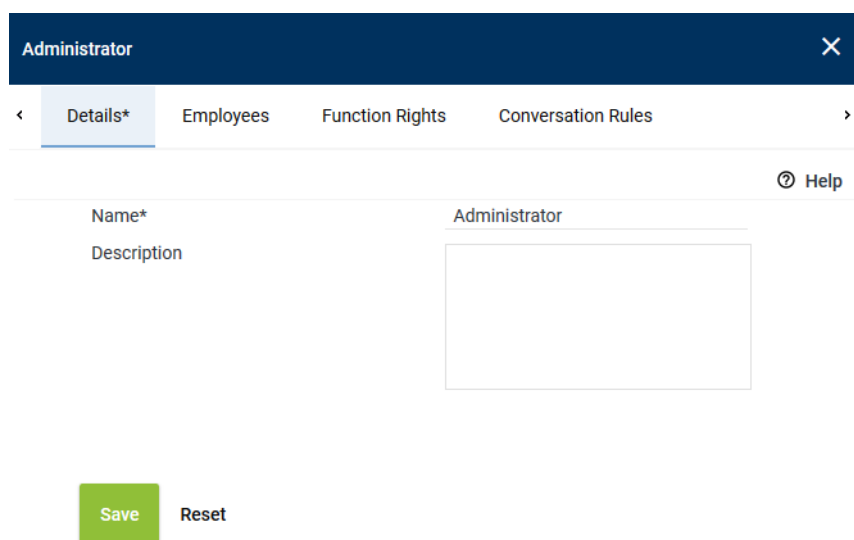



Fig. 114: Save changes

## 7.6

### Delete role

1. In the main view, select the role you would like to delete.
2. Click on the icon  (*Delete*) in the toolbar.
3. To really delete the selected role, confirm the security prompt.



The system does not issue a prompt if the role you are deleting has been assigned to a user. By deleting this role the user loses all function rights he has been assigned via this role. If this user is currently logged in to the system, the deletion of the role will come into effect after he has logged off from the system.

In the Conversation Rules module, you can create conversation rules which are used as filters for displaying conversations and sessions (referred to as conversations in the following) and participant views. By mapping conversation rules to the individual users or to user roles, you can define which conversations are supposed to be visible for a user. You can limit the access to conversations; it is not possible to increase it, though. Under no circumstances can a user receive access to more or to other conversations than defined in his function rights.

If you have not mapped additional function rights, a user can exclusively see his own conversations. A conversation is considered mapped to a user, if he is the initiator (caller), the called party or the 1st-connected participant. The two following settings allow a user to see additional conversations:

- Superior regulation:  
Superiors of an organization unit have access to the conversations of all members of the organization unit. They cannot access the conversations of members of subordinated organization units.
- Superuser:  
Users with the right *Superuser* have access to the conversations of all employees of the tenant to whom they have been assigned to themselves.

You can map the conversation rules defined in the Conversation Rules module to the users in the following locations:

- In the Employees module:  
Here, you can map conversations rules to the individual user directly.
- In the Roles module:  
Here, you can map conversations rules to the different roles. In this case, the conversation rules are mapped to the users via the role, i. e. the user receives the conversations rules that the roles mapped to him contain.

In a conversation rule, you define filter criteria for displaying the conversations. For the filter result, the individual filter criteria are connected by a logical AND connection. Only those conversations which meet all defined filter criteria are displayed.

#### Example 1:

Conversation rule CR1 contains the filter criterion FC1 with the filter value FV1 and the filter criterion FC2 with the filter value FV2

Result: The user only sees those conversations which meet both FC1 (FV1) and FC2 (FV2).

If a user has been mapped several conversation rules, then the sum of all conversation rules takes effect.

#### Example 2:

Conversation rule CR1 contains the filter criterion FC1 with the filter value FV1 and the filter criterion FC2 with the filter value FV2

Conversation rule CR2 contains the filter criterion FC3 with the filter value FV3.

The user has been mapped both conversation rules (CR1 and CR2).

Result: The user only sees those conversations which meet FC1 (FV1) and FC2 (FV2) as well as FC3 (FV3).

Conversation rules take effect in the following applications and modules:



Application	Module
POWER <del>play</del> Web	<ul style="list-style-type: none"> <li>• Conversation module</li> <li>• Participant View module</li> </ul>
POWER <del>play</del> Pro	<ul style="list-style-type: none"> <li>• Conversation module</li> <li>• Participant View module</li> </ul>
INSPIRATION <del>neo</del>	<ul style="list-style-type: none"> <li>• Sessions module</li> <li>• Calibrations module</li> <li>• Audio Analysis module</li> </ul>

In the window of the search function (🔍) of these applications and modules, the user-specific filter settings from the conversation rules are displayed as predefined search settings. Users can restrict these filter settings or search settings but not increase them.

Depending on the tab in which you have configured the conversation rules, the user's view of the conversations may differ in the applications and modules mentioned above.

- The settings in the tab *Session Criteria* affect the view in INSPIRATION~~neo~~;
- the settings in the tab *Participant View Criteria* affect the participant view in POWER~~play~~ Web and in POWER~~play~~ Pro;
- the settings in the tab *Conversation Criteria* affect the conversation view in POWER~~play~~ Web, in POWER~~play~~ Pro as well as in the Sessions module in INSPIRATION~~neo~~.

Open the Conversation Rules module by clicking on the menu item *Conversation Rules* in the navigation bar of the application System Configuration.

## 8.1

### Main view

In the main view, all saved conversation rules are displayed.

+ × Conversation Rules General ▾		
Name ↕	Description ↕	Creator ↕
1w 10 min	Conversations last week > 10 min	Admin, 1st-Tenant
Agent Group 1	Agents 4 and 9	Admin, 1st-Tenant
Agent 9 internal	Agent 9 - internal conversations	Admin, 1st-Tenant
Rows per page 50 ▾ 1 - 3 of 3 < < > >		

Fig. 115: Conversation Rules module - main view

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

<i>Name</i>	Name of the conversation rule.
<i>Description</i>	Description of the conversation rule.
<i>Creator</i>	Name of the user who has created the conversation rule.
<i>Creation Date</i>	Date on which the conversation rule was created.
<i>Updated</i>	Date on which the conversation rule was updated for the last time.






### 8.1.1

#### Toolbar

The toolbar offers the following functions.



Fig. 116: Conversation Rules module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see <a href="#">chapter "Search", p. 34</a> .  The icon  ( <i>Search</i> ) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new conversation rule (see <a href="#">chapter "Create new conversation rule", p. 91</a> ).
	<i>Delete</i>	Deletes the selected conversation rule (see <a href="#">chapter "Delete conversation rule", p. 93</a> ).
<i>Conversation Rules</i>		This menu is currently not available
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



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

## 8.2

### Detail view

The detail view contains data and information about the selected conversation rule.

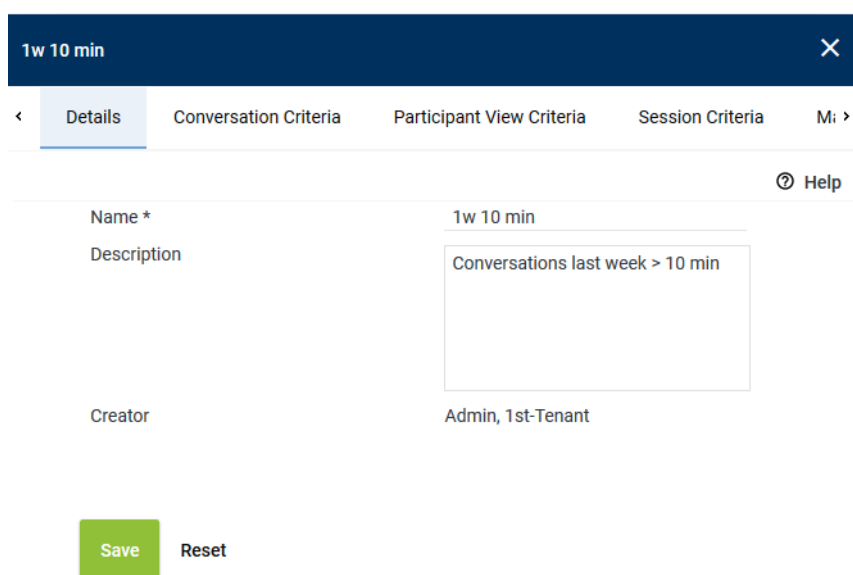


Fig. 117: Conversation Rules module - detail view

The detail view consists of the following tabs:

- **Details**  
Here, you can display and edit a comment and the name of the conversation rule.  
See [chapter "Tab Details", p. 84.](#)
- **Conversation Criteria**  
Here, you can define filter criteria based on the conversation data.  
See [chapter "Tab Conversation Criteria", p. 84.](#)
- **Participant View Criteria**  
Here, you can define filter criteria based on the conversation data from the view of the individual participants.  
See [chapter "Tab Participant View Criteria", p. 87.](#)
- **Session Criteria**  
Here, you can define filter criteria based on the session data.  
See [chapter "Tab Session Criteria", p. 89.](#)
- **Assignment**  
Here, you can see the roles and employees that the conversation rule has been mapped to.  
See [chapter "Tab Mapping", p. 91.](#)

### 8.2.1 Define filter criteria

In the tabs of the detail view, different filter criteria are available which have been divided into different categories (group fields).

For each filter criterion, you can select different comparison parameters from a drop-down list. As soon as a comparison parameter has been selected, the corresponding entry field becomes active.

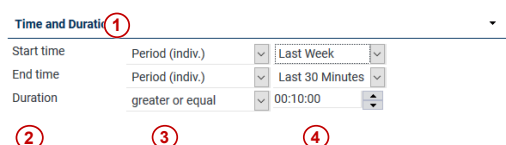



Fig. 118: Filter criteria

1	Category of the filter criteria
2	Filter criterion
3	Comparison parameters
4	Entry field for the filter value

Depending on the respective filter criterion, the following comparison parameters are available:

<i>inactive</i>	The filter criterion is ignored.
<i>equal</i>	All conversations which exactly meet the entered value are displayed as filter result. Enter the value directly into the entry field via the keyboard.
<i>in</i>	You can enter one or several values which are supposed to be filtered for. All conversations which meet at least one of the entered value are displayed as filter result. Enter each individual value directly into the entry field next to the button <b>+</b> via the keyboard. Consequently, click on the button <b>+</b> to apply the value in the list. To remove a value from the list, click on the icon  on the right of the value.
<i>greater or equal</i>	All conversations which meet the entered value or a larger value are displayed as filter result. Enter the value directly into the entry field via the keyboard. Alternatively, use the rotating field by clicking on one of the arrows to increase or reduce the value.
<i>Period of time</i>	All conversations which meet the entered value are displayed as filter result. Select the value from the drop-down list.

### 8.2.2 Tab Details

Here, you can display and edit the name and a description of the conversation rule.

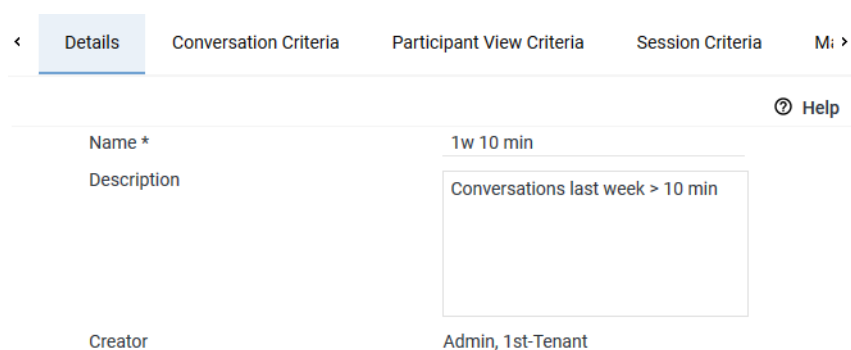


Fig. 119: Conversation Rules module - tab Details

<i>Name</i>	Name of the conversation rule.
<i>Description</i>	Description of the conversation rule.
<i>Creator</i>	Name of the user who has created the conversation rule.

### 8.2.3 Tab Conversation Criteria

Here, you can define filter criteria based on the conversation data.

For information about how to define the different filter criteria see [chapter "Define filter criteria", p. 83](#).

< Details
 

Conversation Criteria
 Participant View Criteria
 Session Criteria
 Mi >

---

Conversation Information
 ▶

---

Statistics of the Conversation
 ▶

---

Calling Party Information
 ▶

---

Called Party Information
 ▶

---

1st-Connected Participant Information
 ▶

---

Additional Data
 ▶

---

General
 ▶

---

Fig. 120: Conversation Rules module - tab Conversation Criteria

### Group field Conversation Information

Conversation Information
 ▼

---

Conversation ID	inactive	▼
Start time	inactive	▼
End time	inactive	▼
Duration	inactive	▼
Subject	inactive	▼

Fig. 121: Conversation Criteria - Conversation Information (example)

<i>Conversation ID</i>	This <a href="#">ID</a> clearly identifies the conversation.
<i>Start time</i>	Period of time when the conversation was started.
<i>End time</i>	Period of time when the conversation was ended.
<i>Duration</i>	Duration of the conversation.
<i>Subject</i>	Subject of the conversation.

### Group field Statistics of the Conversation

Statistics of the Conversation
 ▼

---

Duration of ringing sections	inactive	▼
Duration of hold sections	inactive	▼
Duration of connected sections	inactive	▼
Conversation ID of callback request	inactive	▼

Fig. 122: Conversation criteria - Statistics of the Conversation (example)

<i>Duration of Ringing Sections</i>	Duration of ringing sections
-------------------------------------	------------------------------

<i>Duration of Hold Sections</i>	Duration of hold sections
<i>Duration of Connected Sections</i>	Duration of the connected sections
<i>Conversation ID of Callback Request</i>	Conversation ID of callback request

### Group field Calling Party Information

Calling Party Information			
First name	equal	▼	9.
Last name	equal	▼	Agent
Employee number	equal	▼	900
PBX Agent ID	inactive	▼	
Phone number	inactive	▼	

Fig. 123: Conversation Criteria - Calling Party Information (example)



The filter criteria of this group field can only be applied to internal calls.

<i>First name</i>	First name of the calling party.
<i>Last name</i>	Last name of the calling party.
<i>Employee number</i>	Employee number of the calling party.
<i>PBX Agent ID</i>	ID of the calling agent. This ID has been saved in the <a href="#">PBX</a> and clearly identifies the calling party.
<i>Phone number</i>	Complete phone number of the calling party.

### Group field Called Party Information

Called Party Information			
First name	equal	▼	8.
Last name	equal	▼	Agent
Employee number	equal	▼	800
PBX Agent ID	inactive	▼	
Phone number	inactive	▼	

Fig. 124: Conversation Criteria - Called Party Information (example)

<i>First name</i>	First name of the called party.
<i>Last name</i>	Last name of the called party.
<i>Employee number</i>	Employee number of the called party.
<i>PBX Agent ID</i>	ID of the called agent. This ID has been saved in the <a href="#">PBX</a> and clearly identifies the called party.
<i>Phone number</i>	Complete phone number of the called party.

### Group field 1st-Connected Participant Information

1st-Connected Participant Information			
First name	equal	▼	9.
Last name	equal	▼	Agent
Employee number	equal	▼	900
PBX Agent ID	inactive	▼	
Phone number	inactive	▼	

Fig. 125: Conversation Criteria - 1st-Connected Participant Information (example)

<i>First name</i>	First name of the 1st-connected participant.
<i>Last name</i>	Last name of the 1st-connected participant.
<i>Employee number</i>	Employee number of the 1st-connected participant.
<i>PBX Agent ID</i>	ID of the 1st-connected agent. This ID has been saved in the PBX and clearly identifies the 1st-connected participant.
<i>Phone number</i>	Complete phone number of the 1st-connected participant.

### Group field Additional Data

Additional Data			
Universal Call ID	inactive	▼	
Comment	equal	▼	Information
User name	inactive	▼	

Fig. 126: Conversation Criteria - Additional Data (example)

**NOTICE!** The depicted additional data *VDN Extension* and *Comment* are only exemplary additional data!

In this group field, the system provider displays individually defined and customer-specifically provided additional data. In addition, it depends on your function rights which additional data are displayed here. Your system provider can inform you about the meaning of the additional data which is available in your system.

### Group field General

General			
Creation date	Period (indiv.)	▼	Last Week
Updated	Period (indiv.)	▼	Last 30 Minutes

Fig. 127: Conversation Criteria - General (example)

<i>Creation date</i>	Date on which the conversation was saved in the system.
<i>Updated</i>	Date on which the conversation was updated for the last time. An update takes place whenever the conversation is edited manually, e. g. by adding comments or additional data.

#### 8.2.4 Tab Participant View Criteria

Here, you can define filter criteria based on the conversation data from the view of the individual participants.

For information about how to define the different filter criteria see [chapter "Define filter criteria", p. 83](#).

< Details Conversation Criteria **Participant View Criteria** Session Criteria Mi >

---

**Participant View Information** ▶

---

**Participant Information** ▶

---

**General** ▶

---

Fig. 128: Conversation Rules module - tab Participant View Criteria

### Group field Conversation Information

**Participant View Information** ▼

Conversation ID	equal	▼	c00d123f-fa0f-43f7-t
Participant view ID	equal	▼	5e31e665-70fe-4f23
Start time	Period (indiv.)	▼	Last 24 Hours ▼
End time	Period (indiv.)	▼	Last 24 Hours ▼
Duration	greater or equal	▼	00:15:00 ▲▼
Comment	equal	▼	gut

Fig. 129: Participant View Criteria - Conversation Information

<i>Conversation ID</i>	This ID clearly identifies the conversation that the participant view belongs to.
<i>Participant View ID</i>	This ID clearly identifies the individual participant views of a conversation.
<i>Start time</i>	Period of time when the conversation was started from the participant view.
<i>End time</i>	Period of time when the conversation was ended from the participant view.
<i>Duration</i>	Duration of the conversation in the participant view.
<i>Comment</i>	Comment which has been entered for the participant view of the conversation in the Replay module.

### Group field Participant Information

**Participant Information** ▼

First name	equal	▼	9.
Last name	equal	▼	Agent
Employee number	equal	▼	900
Called party PBX Agent ID	inactive	▼	
Participant phone number	inactive	▼	

Fig. 130: Participant View Criteria - Participant Information (example)

<i>First name</i>	First name of any participant.
<i>Last name</i>	Last name of any participant.
<i>Employee number</i>	Employee number of any participant.



<i>Called party PBX Agent ID</i>	ID of any agent who has participated in the conversation. This ID has been saved in the <b>PBX</b> and clearly identifies every participant.
<i>Participant phone number</i>	Complete phone number of any participant.

### Group field General

**General** ▼

Creation date	Period (indiv.) ▼	Last Week ▼
Updated	Period (indiv.) ▼	Last 30 Minutes ▼

Fig. 131: Participant View Criteria - General (example)

<i>Creation date</i>	Date on which the participant view of the conversation was saved in the system.
<i>Updated</i>	Date on which the participant view of the conversation was updated for the last time.  An update takes place whenever the participant view is edited manually, e. g. by adding comments or additional data.

### 8.2.5

#### Tab Session Criteria

Here, you can define filter criteria based on the session data.

For information about how to define the different filter criteria see [chapter "Define filter criteria", p. 83](#).

< Details Conversation Criteria Participant View Criteria **Session Criteria** Mi >

---

**Agent Information** ▶

---

**Time and Duration** ▶

---

**CTI Information** ▶

---

**Categories** ▶

---

**General** ▶

---

**Organization Units** ▶

---

Fig. 132: Conversation Rules module - tab Session Criteria

### Group field Agent Information

**Agent Information** ▼

First name	equal ▼	9.
Last name	equal ▼	Agent

Fig. 133: Session Criteria - Agent Information (example)

<i>First name</i>	First name of any agent who has participated in the session.
<i>Last name</i>	Last name of any agent who has participated in the session.

### Group field Time and Duration

**Time and Duration** ▼

Start time	Period (indiv.)	▼	Last Week	▼
End time	Period (indiv.)	▼	Last 30 Minutes	▼
Duration	greater or equal	▼	00:10:00	▼

Fig. 134: Session Criteria - Time and Duration (example)

<i>Start time</i>	Period of time when the session was started.
<i>End time</i>	Period of time when the session was ended.
<i>Duration</i>	Session duration.

### Group field CTI Information

**CTI Information** ▼

Session transfers	equal	▼	4
Hold time	greater or equal	▼	00:10:00
Comment	equal	▼	good
Wrap-up time	greater or equal	▼	00:10:00

Fig. 135: Session Criteria - CTI Information (example)

<i>Session transfers</i>	Number of session transfers.
<i>Hold time</i>	Period of time that the session was “on hold”.
<i>Comment</i>	Comment which has been entered for the session in the Replay module or in the Sessions module.
<i>Wrap-up time</i>	Duration of the wrap-up time of the session.

### Group field Categories

**Categories** ▼

Name	equal	▼	Information
------	-------	---	-------------

Fig. 136: Session Criteria - Categories (example)

<i>Name</i>	Name of the category that the session belongs to.
-------------	---

### Group field General

**General** ▼

Creation date	Period (indiv.)	▼	Last Week	▼
Updated	Period (indiv.)	▼	Last 30 Minutes	▼
Session ID	equal	▼	4552b5ba-2a12-43ce	

Fig. 137: Session Criteria - General (example)

<i>Creation date</i>	Date on which the session was saved in the system.
<i>Updated</i>	Date on which the session was updated for the last time.

	An update takes place whenever the session is edited manually, e. g. by adding comments or additional data.
Session ID	This ID clearly identifies the session.

### Group field Organization Units

Organization Units		
Of the agent	inactive	▼
Of the calling party	inactive	▼
Of the called party	inactive	▼
Of the 1st-connected	inactive	▼

Fig. 138: Session Criteria - Organization Units (example)

<i>Of the agent</i>	Organization unit of the agent who has participated in the session.
<i>Of the calling party</i>	Organization unit of the calling party who has participated in the session.
<i>Of the called party</i>	Organization unit of the called party who has participated in the session.
<i>Of the 1st-connected</i>	Organization unit of the first connected who has participated in the session.

### 8.2.6 Tab Mapping

Here, you can see the roles and employees that the conversation rule has been mapped to.

<

Conversation Criteria

Participant View Criteria

Session Criteria

Mapping >

Mapping to Employees

First Name

Last Name

No records found

Mapping to Roles

Name

Description

No records found

Fig. 139: Conversation Rules module - tab Mapping

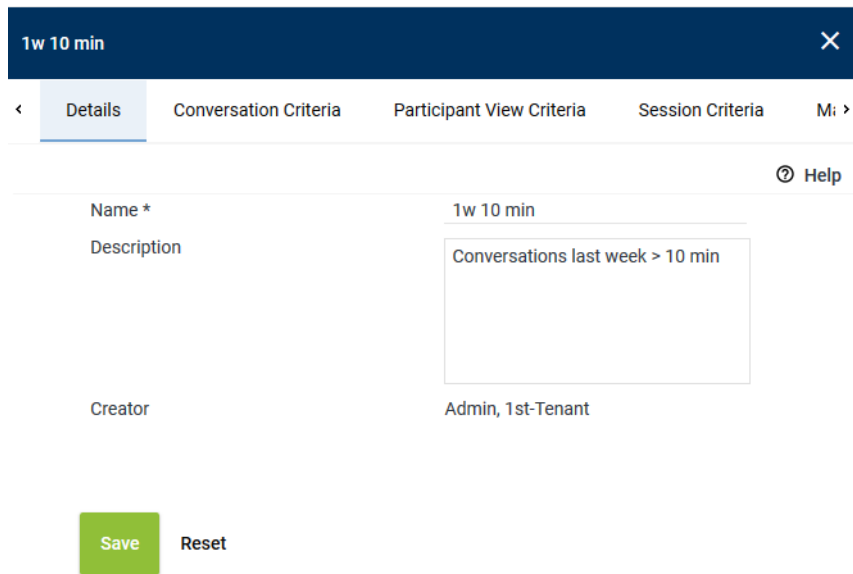
### 8.3 Create new conversation rule

1. Click on the icon  (*Create*) in the toolbar.
2. Select one of the following options:

<i>Create New</i>	A completely new conversation rule is created.
<i>Create Clone</i>	<i>This function is currently unavailable.</i>

3. Adjust the respective settings in the tabs of the detail view (see [chapter "Detail view", p. 82](#)).  
You can change tabs without buffering without risking the loss of your settings.

- Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.



1w 10 min

< Details Conversation Criteria Participant View Criteria Session Criteria Mi >

Help

Name \* 1w 10 min

Description Conversations last week > 10 min

Creator Admin, 1st-Tenant

Save Reset

Fig. 140: Save conversation rule

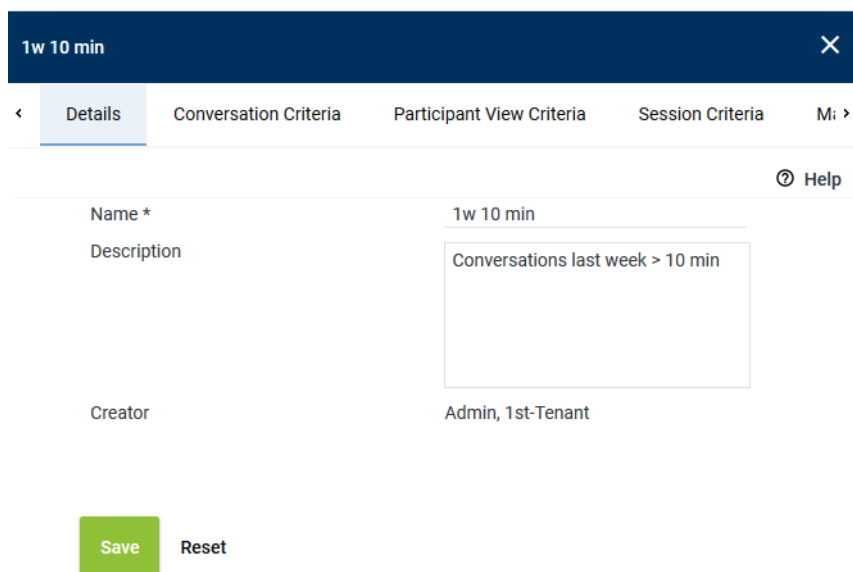
## 8.4

### Edit conversation rule



You can change a conversation rule any time you like, i. e. even if it has already been mapped to users or roles. The change only comes into effect for the user after he has logged off from and in to the system again.

- In the main view, select the conversation rule you would like to edit.
- Adjust the respective settings in the tabs of the detail view (see [chapter "Detail view", p. 82](#)).  
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.



1w 10 min

< Details Conversation Criteria Participant View Criteria Session Criteria Mi >

Help

Name \* 1w 10 min

Description Conversations last week > 10 min


Creator Admin, 1st-Tenant

Save Reset

Fig. 141: Save changes

## 8.5

**Delete conversation rule**

1. In the main view, select the conversation rule you would like to delete.
2. Click on the icon  (*Delete*) in the toolbar.
3. To really delete the selected conversation rule, confirm the security prompt.



---

If you are trying to delete a conversation rule which has already been mapped to a user, then the system issues a respective notification. You can delete the conversation rule anyway.

If the affected user is currently logged in to the system and is using a module in which the conversation rule is relevant, then the deletion of the role will come into effect after he has logged off from the system.

---

## 9

## Predefined function packages

The system offers the following predefined function packages to make selected function rights available to the users:

- **Agent** (only for tenants)

Agents have the following function rights at their disposal:

- Selected modules and functions in the application INSPIRATION<sub>neo</sub>

The individual function rights and additional roles allow you to assign agents further individual rights.

See [chapter "Create agent", p. 94](#).

- **Supervisor** (only for tenants)

Supervisors have the following function rights at their disposal:

- All modules and functions in the application INSPIRATION<sub>neo</sub>

The individual function rights and additional roles allow you to assign supervisor further individual rights.

See [chapter "Create supervisor", p. 95](#).

- **Superior** (superior of an organization unit, only for tenants)

The superior of an organization unit can see the data of the agents who are members of this organization unit. He cannot see agents or data of other organization units. Superiors can at the same time be a member of their organization unit.

See [chapter "Create superior", p. 95](#).

**NOTICE!** To be able to view the data of agents in the application INSPIRATION<sub>neo</sub>, the rights of roles (e. g. agent) or individual function rights are required.

- **Coaching Advisor** (only for tenants)

By means of the application CLIENT<sub>command</sub>, a coaching advisor can record coaching advisor sessions.

Coaching advisor session are simulated sessions which are recorded exclusively for training purposes. These sessions are displayed in the Coaching Advisor module of the application INSPIRATION<sub>neo</sub>.

See [chapter "Create Coaching Advisor", p. 95](#).

- **Superuser**

A superuser has the rights to all functions in the system if the respective licenses are available.

See [chapter "Create superuser", p. 96](#).

## 9.1

## Create agent

- ✓ At least 1 free agent license is available in the system.

1. Open the Employees module.
2. In the main view, select the user you would like to define as agent.
3. Click on the tab *Agent Data* in the detail view.
4. Activate the option *Agent* and enter all required information, see [chapter "Tab Agent Data", p. 40](#).
5. Click on the tab *Roles* in the detail view.
6. Assign the user the default role *Agent* or an agent role you have defined yourself, see [chapter "Assign roles", p. 52](#).  
Only by assigning this role to the user, he receives the required function rights.

7. Click on the button *Save* to save the setting.



Upon deactivating the option *Agent*, the system does not consider the employee as an agent anymore. The assignment of the role *Agent* is not removed automatically when deactivating the option. If the employee is supposed to lose the function rights of an agent, too, you have to remove the assignment of the role manually, see [chapter "Delete role assignment", p. 53](#).



The default role for agents grants users access to their own data only, e. g. their sessions, evaluations, and training packages in the following modules of the application INSPIRATION<sub>neo</sub>:

- Evaluations module
- Sessions module
- E-Learning module

You can add individual function rights to the scope of function rights which have been assigned to a user via the default role, see [chapter "Tab Individual Function Rights", p. 53](#).

## 9.2

### Create supervisor

- ✓ At least 1 free supervisor license is available in the system.
- 1. Open the Employees module.
- 2. In the main view, select the user whom you would like to assign supervisor rights.
- 3. Click on the tab *Roles* in the detail view.
- 4. Assign the user the role *Supervisor*, see [chapter "Assign roles", p. 52](#).
- 5. Click on the button *Save* to save the setting.

## 9.3

### Create superior

- ✓ The user has the right *Has access to agents and their data*, see [chapter "Tab Settings", p. 47](#).
- 1. Open the Organization Structure module.
- 2. In the main view, select the organization unit for which you would like to define a superior.
- 3. Click on the tab *Superiors*.
- 4. Assign the user to the organization unit who is supposed to be the superior, see [chapter "Assign superiors", p. 67](#).
- 5. Click on the button *Save* to save the setting.



Alternatively, you can define a user as superior in the Employees module, see [chapter "Tab Organization Units", p. 58](#).

## 9.4

### Create Coaching Advisor

- ✓ The user has the right *Has access to agents and their data*, see [chapter "Tab Settings", p. 47](#).
- 1. Open the Employees module.
- 2. In the main view, select the agent you would like to assign coaching advisor rights.
- 3. Click on the tab *Settings* in the detail view.
- 4. Open the group field *Permissions*.
- 5. Activate the check box in front of *Coaching Advisor*.

< Details\* Agent Data Account\* Settings Roles Individual Function Ri...

▼ Permissions

☐ Superuser

☒ Has access to employees and their data

☐ Can replay conversations

☐ Can delete conversations

☐ Activate voice disguising

☐ Cutoff of the calls (beginning)

0 Milliseconds

☐ Cutoff of the calls (end)

0 Milliseconds

☒ Coaching Advisor

Fig. 142: Create Coaching Advisor

6. Click on the tab *Individual Function Rights*.
7. Open the group field *INSPIRATION<sub>neo</sub>*.
8. Click on the icon "+" in front of the entry *Coaching Advisor*.
9. Give the user all function rights to the Coaching Advisor module.
10. Click on the button *Save* to save the setting.

## 9.5

### Create superuser

1. Open the Employees module.
2. In the main view, select the user you would like to assign superuser rights.
3. Click on the tab *Settings* in the detail view.
4. Open the group field *Permissions*.
5. Activate the check box in front of *Superuser*.

< Details\* Agent Data Account\* Settings Roles Individual Function Ri...

▼ Permissions

☒ Superuser

☒ Has access to employees and their data

☒ Can replay conversations

☐ Can delete conversations

☐ Activate voice disguising

☐ Cutoff of the calls (beginning)

0 Milliseconds

☐ Cutoff of the calls (end)

0 Milliseconds

☐ Coaching Advisor

Fig. 143: Create superuser

6. Click on the button *Save* to save the setting.



---

Upon assigning a user superuser rights, only the following tabs are active:



- *Details*
- *Agent Data*
- *Account*
- *Settings*

In this case, no further adjustments are have to be made in any of the other tabs.

---

## List of figures

Fig. 1	Tenants module - main view .....	11
Fig. 2	Tenants module - toolbar .....	11
Fig. 3	Tenants module - detail view .....	12
Fig. 4	Tenants module - tab Details .....	13
Fig. 5	Add time zone .....	14
Fig. 6	The displayed entries in the table are filtered for ber (example) .....	14
Fig. 7	Add time zone .....	14
Fig. 8	System Availability (via Browser) .....	15
Fig. 9	System Availability (via Browser) .....	15
Fig. 10	Configure system availability .....	15
Fig. 11	Add address .....	16
Fig. 12	Add address .....	16
Fig. 13	Add contact person .....	16
Fig. 14	Add contact person .....	17
Fig. 15	Tenants module - tab Passwords .....	17
Fig. 16	Define password length .....	18
Fig. 17	Define mandatory characters .....	18
Fig. 18	Configure password security .....	20
Fig. 19	Define forbidden passwords .....	21
Fig. 20	Define advanced password settings .....	21
Fig. 21	Edit entry in the list .....	22
Fig. 22	Tenants module - tab General Settings .....	22
Fig. 23	Configure user activity .....	22
Fig. 24	SMTP account .....	23
Fig. 25	SMTP account .....	23
Fig. 26	Add SMTP account .....	24
Fig. 27	Activate LDAP .....	24
Fig. 28	Configure miscellaneous settings .....	25
Fig. 29	Configure session search results .....	25
Fig. 30	Configure terms of use .....	26
Fig. 31	Tenants module - tab Key Management .....	26
Fig. 32	Tenants module - tab LDAP Connection Data .....	27
Fig. 33	LDAP Connection Data .....	28
Fig. 34	Edit LDAP connection data (example) .....	28
Fig. 35	Display web service functions .....	29
Fig. 36	Employees module - main view .....	31
Fig. 37	Employees module - toolbar .....	32
Fig. 38	Summary of the function rights .....	33
Fig. 39	Window Search Criteria (example) .....	34
Fig. 40	Employees module - detail view .....	35
Fig. 41	Employees module - tab Details .....	36

Fig. 42	Edit employee information.....	37
Fig. 43	Upload image .....	38
Fig. 44	Upload File .....	39
Fig. 45	Delete image (example) .....	39
Fig. 46	Add address .....	39
Fig. 47	Add address .....	40
Fig. 48	Employees module - tab Agent Data .....	40
Fig. 49	Agent Data - Telephony .....	41
Fig. 50	Agent Data - Chat .....	42
Fig. 51	Agent Data - Miscellaneous Settings .....	42
Fig. 52	Employees module - tab Account .....	44
Fig. 53	Add account .....	44
Fig. 54	Activate authentication via LDAP .....	45
Fig. 55	Assign combination user .....	46
Fig. 56	Add combination user .....	46
Fig. 57	Delete combination user assignment .....	47
Fig. 58	Employees module - tab Settings .....	47
Fig. 59	Configure permissions .....	47
Fig. 60	Configure logging .....	49
Fig. 61	Set session release for agents .....	50
Fig. 62	Session release - General Settings.....	50
Fig. 63	Session release - Settings for the Superior.....	51
Fig. 64	Session release - Notification of the Agent .....	51
Fig. 65	Employees module - tab Roles .....	52
Fig. 66	Assign roles.....	52
Fig. 67	Add role.....	53
Fig. 68	Delete role assignment .....	53
Fig. 69	Employees module - tab Individual Function Rights (example) .....	54
Fig. 70	Function rights - display sections (example) .....	54
Fig. 71	Function rights - Display function rights .....	55
Fig. 72	Employees module - tab Conversation Rules .....	56
Fig. 73	Assign conversation rule .....	57
Fig. 74	Add conversation rules.....	58
Fig. 75	Delete conversation rule assignment .....	58
Fig. 76	Employees module - tab Organization Units.....	59
Fig. 77	Assign organization units .....	59
Fig. 78	Add organization units.....	60
Fig. 79	Delete organization unit assignment .....	60
Fig. 80	Save employee .....	61
Fig. 81	Organization Structure module - main view .....	63
Fig. 82	Organization Structure module - toolbar .....	63
Fig. 83	Organization Structure module - detail view .....	64

Fig. 84	Organization Structure module - tab Details .....	65
Fig. 85	Organization Structure module - tab Members .....	65
Fig. 86	Assign users.....	65
Fig. 87	Add user.....	66
Fig. 88	Delete user assignment .....	66
Fig. 89	Organization Structure module - tab Superiors.....	66
Fig. 90	Assign users.....	67
Fig. 91	Add user.....	67
Fig. 92	Delete user assignment .....	67
Fig. 93	Organization Structure module - tab Member Roles.....	68
Fig. 94	Organization Structure module - tab Superior Roles .....	68
Fig. 95	Save organization unit.....	69
Fig. 96	Save changes .....	69
Fig. 97	Roles module - main view .....	71
Fig. 98	Roles module - toolbar .....	71
Fig. 99	Roles module - detail view .....	72
Fig. 100	Roles module - tab Details .....	73
Fig. 101	Roles module - tab Employees .....	73
Fig. 102	Assign users.....	73
Fig. 103	Add user.....	74
Fig. 104	Delete user assignment .....	74
Fig. 105	Roles module - tab Function Rights (example).....	75
Fig. 106	Function rights - display sections (example) .....	75
Fig. 107	Function rights - Display function rights .....	76
Fig. 108	Roles module - tab Conversation Rules Object Rules .....	76
Fig. 109	Assign conversation rule.....	77
Fig. 110	Add conversation rules.....	77
Fig. 111	Delete conversation rule assignment.....	77
Fig. 112	Save role .....	78
Fig. 113	Save role .....	79
Fig. 114	Save changes .....	79
Fig. 115	Conversation Rules module - main view .....	81
Fig. 116	Conversation Rules module - toolbar.....	82
Fig. 117	Conversation Rules module - detail view .....	83
Fig. 118	Filter criteria .....	83
Fig. 119	Conversation Rules module - tab Details.....	84
Fig. 120	Conversation Rules module - tab Conversation Criteria .....	85
Fig. 121	Conversation Criteria - Conversation Information (example).....	85
Fig. 122	Conversation criteria - Statistics of the Conversation (example) .....	85
Fig. 123	Conversation Criteria - Calling Party Information (example).....	86
Fig. 124	Conversation Criteria - Called Party Information (example).....	86
Fig. 125	Conversation Criteria - 1st-Connected Participant Information (example).....	87

Fig. 126 Conversation Criteria - Additional Data (example).....	87
Fig. 127 Conversation Criteria - General (example) .....	87
Fig. 128 Conversation Rules module - tab Participant View Criteria .....	88
Fig. 129 Participant View Criteria - Conversation Information .....	88
Fig. 130 Participant View Criteria - Participant Information (example).....	88
Fig. 131 Participant View Criteria - General (example).....	89
Fig. 132 Conversation Rules module - tab Session Criteria .....	89
Fig. 133 Session Criteria - Agent Information (example) .....	89
Fig. 134 Session Criteria - Time and Duration (example).....	90
Fig. 135 Session Criteria - CTI Information (example).....	90
Fig. 136 Session Criteria - Categories (example) .....	90
Fig. 137 Session Criteria - General (example).....	90
Fig. 138 Session Criteria - Organization Units (example).....	91
Fig. 139 Conversation Rules module - tab Mapping .....	91
Fig. 140 Save conversation rule.....	92
Fig. 141 Save changes .....	92
Fig. 142 Create Coaching Advisor .....	96
Fig. 143 Create superuser .....	96

## List of tables

Tab. 1	Function rights.....	55
Tab. 2	Function rights INSPIRATIONneo > Evaluation templates .....	55
Tab. 3	Function rights player .....	56
Tab. 4	Function rights.....	76

## Glossary

### ID

Identifier, ID

### IP

Internet Protocol, basic protocol for Internet communication

### LDAP

Lightweight Directory Access Protocol

### PBX

Private Branch Exchange

### SMTP

Simple Mail Transfer Protocol is a protocol which serves to send e-mails in computer networks.

### SSL

Secure Socket Layer

### SSO

Single Sign On; Simplified login mode. After a one-off authentication at one workplace users will be able to use all services and applications that they have been authorized for from this workplace. They do not have to authenticate for the individual applications again.

### TLS

Transport Layer Security; previously known as Secure Sockets Layer (SSL), is a hybrid encryption protocol for safe data transmission in the Internet. Since version 3.0, the SSL protocol is developed under the new name TLS.

### 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)

### XML

Extensible Markup Language is a human-readable and machine-readable language which defines a set of rules for encoding documents.