System Configuration

User management

Administration manual

for tenants

10/25/2021

Product line *neo*, version 6.x

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

EVOIP*neo*

EVOLUTION*neo* / XXL / eco

INSPIRATION*neo*

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.

ASC Technologies AG - Seibelstr. 2-4 - 63768 Hösbach - Germany

Contents

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.

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. 32.
- 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. 73.
- 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. 66.
- 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. 83.

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.

3 LDAP

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

To be able to use the feature LDAP authentication, at least 1 configured LDAP server (e. g. an Active Directory) must be available containing the users which are supposed to use the *neo* recording system. Users must have been created as *User* there. They may exist in any combination of directories within the LDAP servers.

If you would like to use authentication via LDAP, go to the Tenants module to configure all connections to possible LDAP servers and to activate LDAP authentication in general. When configuring the individual users, you can then decide whether this user is supposed to be able 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 Login Settings", p. 24.
- Activate LDAP authentication for individual users.

  See chapter "Authentication via LDAP", p. 48.

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.

Fig. 1: Tenants module - main view

Name	Name which is displayed for the tenant in the system.
Customer ID	Name of the tenant.
Type	Type of tenant. • Tenant • Reseller
Country	Country of the tenant's address.
Creation Date	Date on which the tenant was created.
Updated	Date on which the tenant's information was updated for the last time.

4.1.1 Toolbar

The toolbar offers the following functions.

Fig. 2: Tenants module - toolbar

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

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

4.2 Detail view

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

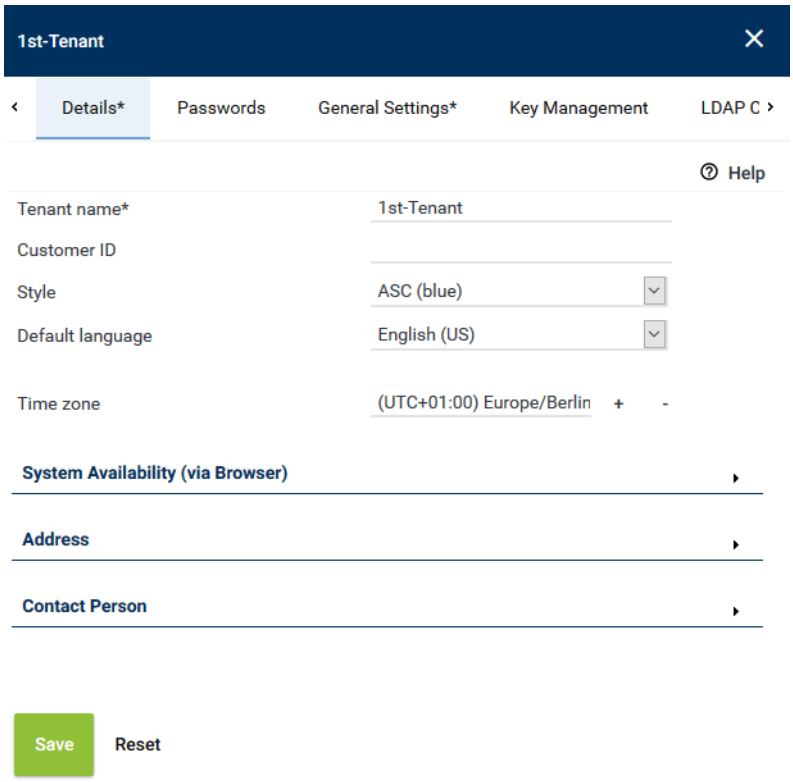

Fig. 3: Tenants module - detail view

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. 29.

4.2.1 Tab Details

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

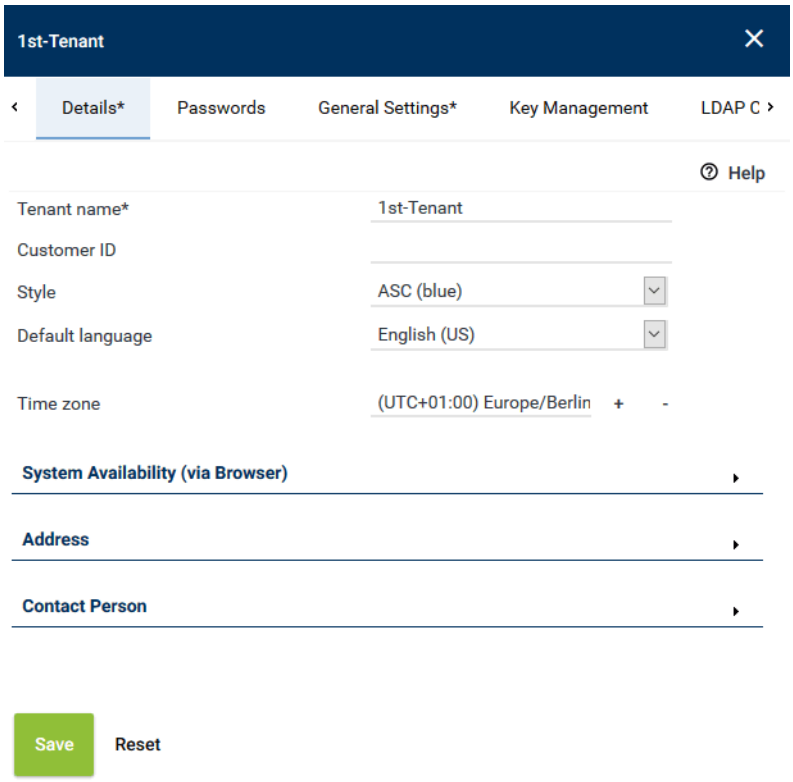

Fig. 4: Tenants module - tab Details

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

Tenant name	Your name as tenant.
Customer ID	Enter the customer ID.
Style	Layout in which the tenant sees the user interface of the system. Select one of the available layouts from the drop-down list.
Default language	Language in which the user interface of the system is displayed in your environment. Select the language from the drop-down list.
Time zone	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 chapter "Add time zone", p. 14. 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*:

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

3. Select a time zone from the list.

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*.

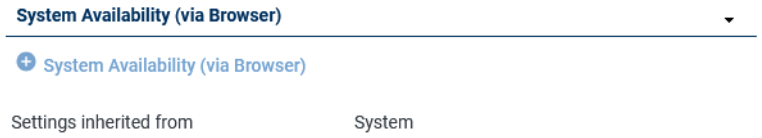

Fig. 9: System Availability (via Browser)

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.

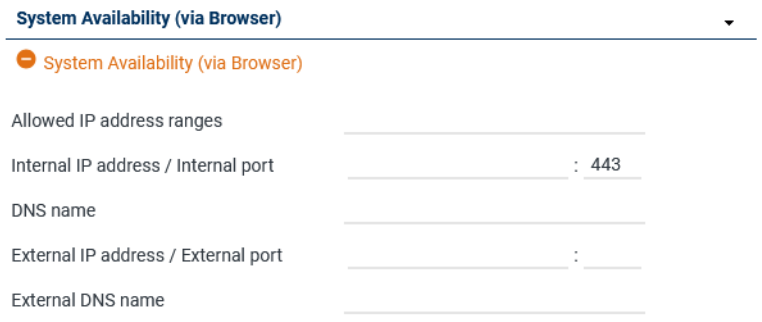

Fig. 10: Configure system availability

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

External IP address / External port	Enter the URL or the IP address and the port under which the Replay module can be reached via the browser from outside the local network.
External DNS name	Enter the external DNS name under which the Replay module can be reached via the browser from outside the local network. **NOTICE!** 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*.

7. 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

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

Fig. 11: Add address

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

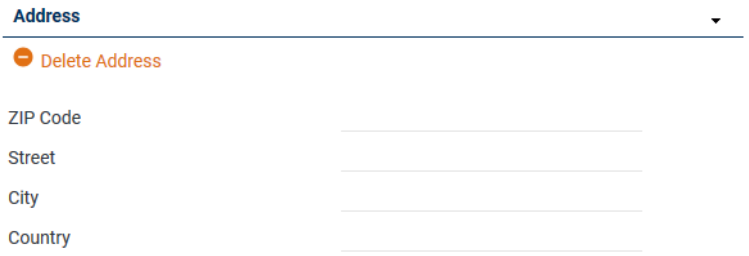

Fig. 12: Add address

4. 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

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

Fig. 13: Add contact person

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

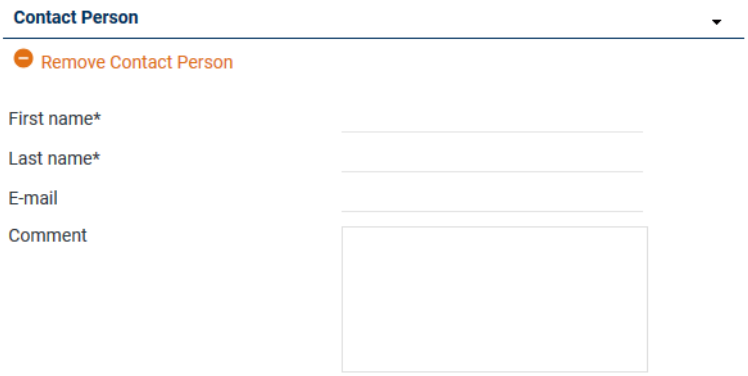

Fig. 14: Add contact person

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

4. 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.

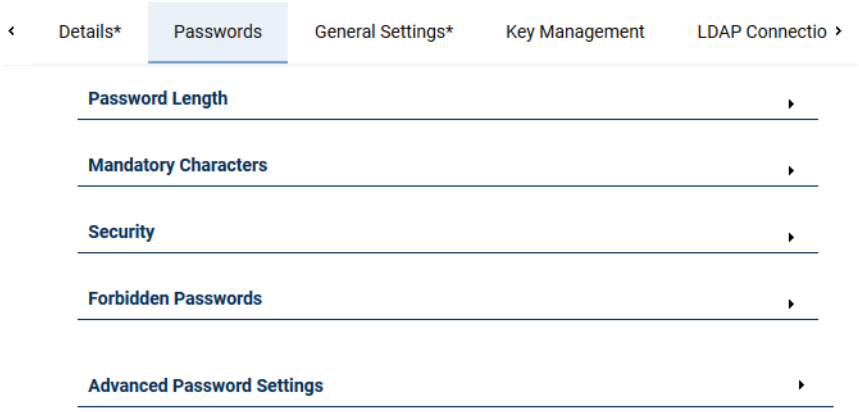

Fig. 15: Tenants module - tab Passwords

Password rules apply for all passwords which have been created for the first time or which are changed. Existing passwords are not checked.

Exceptions:

- *Validity*

  All passwords are check for their currently configured duration of validity on a daily basis.
- *Possible failed login attempts*

  For all passwords, the number of failed login attempts is monitored.

In the following cases, the defined password rules do **not** apply:

- Authentication via LDAP
- In the user account, the following option has been activated:
  Does not have to meet the password rules

Parameters containing 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.

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 ≥ *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.

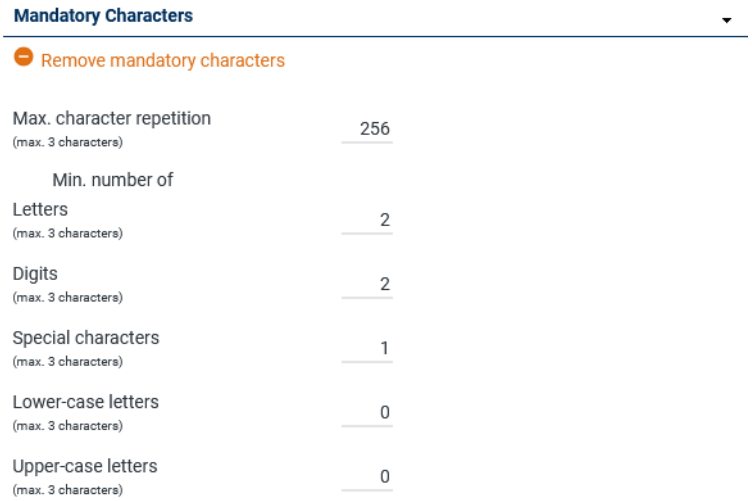

Fig. 17: Define mandatory characters

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 digits a password must contain at least.		
Min. number of special characters	Enter how many special characters a password must contain at least.		
	Valid special characters:		
	Full stop	.	
	Comma	,	
	Semicolon	;	
	Colon	:	
	Question mark	?	
	Exclamation mark	!	
	Quotation marks	""	
	Apostrophe	'	
	Hyphen	-	
	Dash	/	
	Brackets	() [] {}	
	Hashtag	#	
	Dollar sign	$	
	Percent sign	%	
	Ampersand	&	
	Asterisk	*	
	Plus sign	+	
	Inequality sign (greater-than, less-than sign)	<>	
	Equals sign	=	
	At sign	@	
	Caret	^	
	Underscore	_	
	Grave accent	`	
	Pipe (vertical bar)	|	
	Tilde	~	
	All other punctuation characters are interpreted as letters.		
Min. number of lower-case letters	Enter how many lower-case letters a password must contain at least.		
Min. number of upper-case letters	Enter how many upper-case letters a password must contain at least.		

4. 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

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

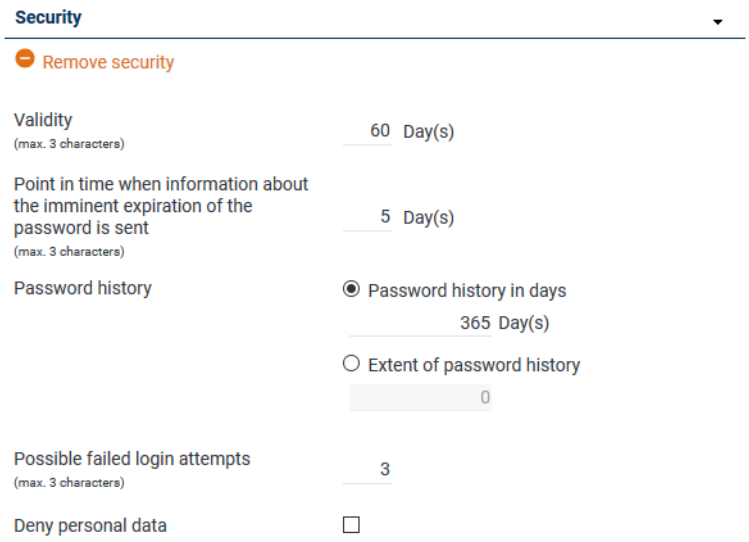

Fig. 18: Configure password security

Validity	Enter for how long a password is supposed to remain valid. *Validity = 0*: Passwords never expire
Point in time when information about the imminent expiration of the password is sent	Enter how many days before the expiration of the password users are to be reminded that they will have to change their password soon. *Point in time ... = 0*: User does not receive any information **NOTICE!** The value for the point in time to send information must be smaller than the value for the validity of the password.
Password history	Enter for how long the password history is supposed to be saved. Select one of the following options: • *Password history in days* For this option, enter for how long the passwords are supposed to be saved in the password history. • *Extent of password history* For this option, enter the number of passwords which are supposed to be saved in the password history. In both cases, the password history is never deleted entirely. If the entered value is reached, only the oldest entries are deleted.
Possible failed login attempts	Enter how often the user may enter an incorrect password before the account is locked. **NOTICE!** A locked account can be released again by any user with access to the Employees module and to the data of the locked user.
Deny personal data	Define whether users are allowed to use private data from their profiles for the password (e. g. name, user name, date of birth). ☑ = Personal data is not allowed.

	☐ = Personal data is allowed.

4. 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.

Fig. 19: Define forbidden passwords

Add	Adds a new entry to the list.
Delete	Deletes the selected entry from the list.
	Opens the selected entry for editing, see chapter "Edit entry", p. 22.

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 *Advanced Password Settings*.
2. Select whether the 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.

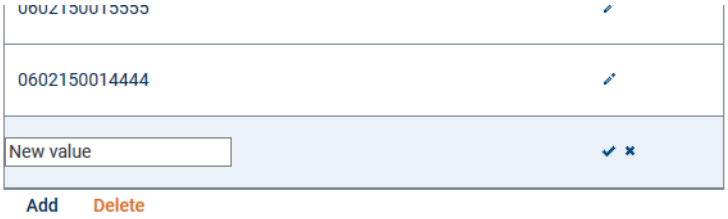

Fig. 21: Edit entry in the list

2. Adjust the entry.
3. 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.

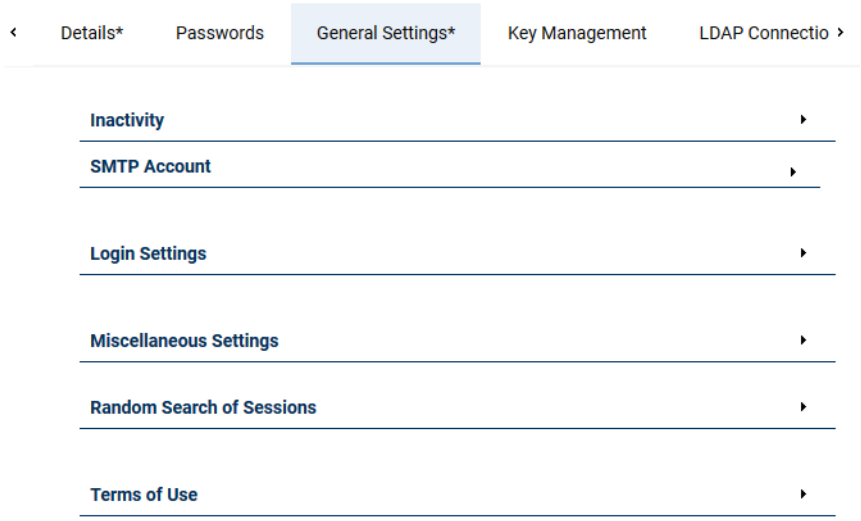

Fig. 22: Tenants module - tab General Settings

4.2.3.1 Group field Inactivity

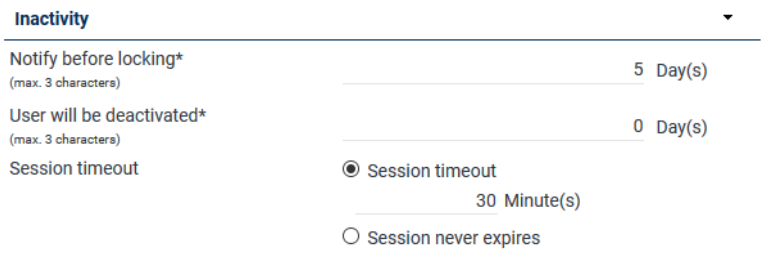

Fig. 23: Configure user activity

Notify before locking	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 *User will be deactivated*. *Notify before locking = 0*: User is not notified.

	The notification is sent to the e-mail address of the user.
User will be deactivated	Select after how many days of inactivity the account of the user is locked. *User will be deactivated = 0*: User is not deactivated.
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: If the user does not close the application by using the logoff function as recommended (menu item *(Logged in As) > Logoff*) but closes the browser directly, then the started session will never be finished. 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*.

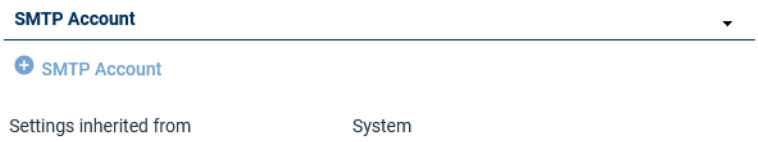

Fig. 25: SMTP account

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*.

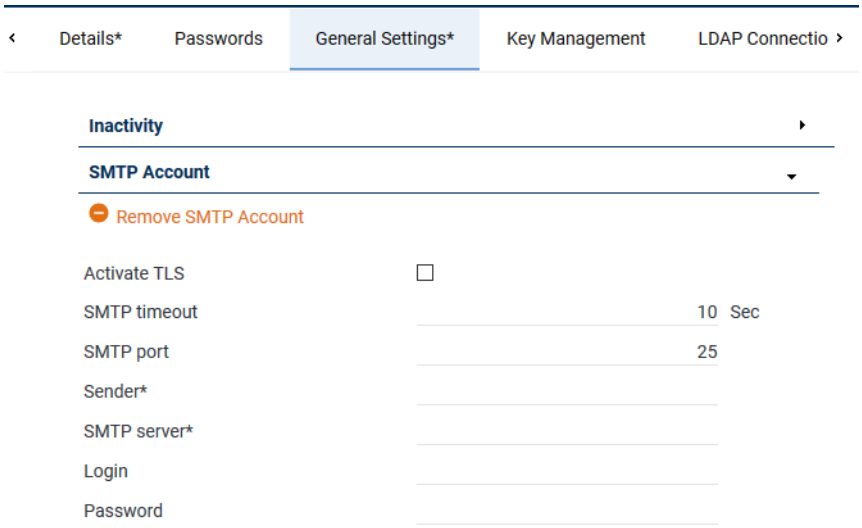

Fig. 26: Add SMTP account

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:

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

Here, you can activate or deactivate the authentication via LDAP as well as the entry field for replay via phone for the users of your environment as a rule.

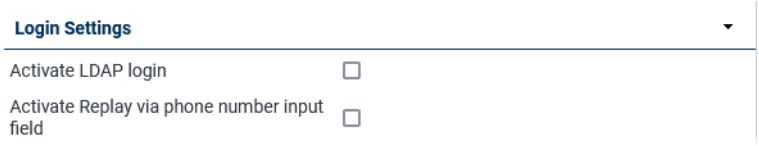

Fig. 27: Login Settings

Activate LDAP login	Activate or deactivate the authentication via LDAP. ☑ = LDAP login has been activated. ☐ = LDAP login has not been activated.
Activate Replay via telephone number input field	Activate or deactivate the entry field to enter the replay via phone number when logging in to POWER*play* Web. ☑ = Field to enter replay via phone number is displayed on the login screen of POWER*play* Web. ☐ = Field to enter replay via phone number is not displayed on the login screen of POWER*play* Web.

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

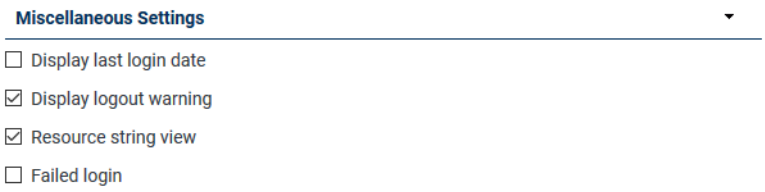

Fig. 28: Configure miscellaneous settings

Display last login date	Select whether you would like to have the date of the last login displayed in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Display logout warning	Select whether you would like to issue a logout warning in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Resource string view	Select whether you would like to display the button to activate the resource string view in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Failed login	Select whether you would like to display the information about a failed login in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.

4.2.3.5 Group field Random Search of Sessions

Fig. 29: Configure session search results

Maximum number of search results	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

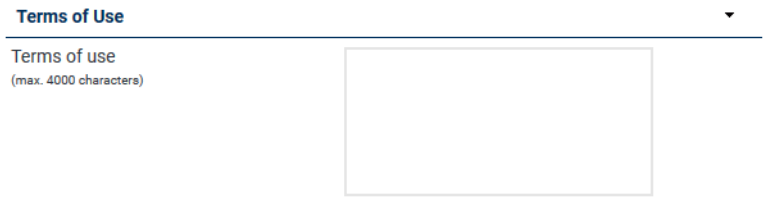

Fig. 30: Configure terms of use

Terms of use	Here, you can enter terms of use. The terms of use are displayed in the browser upon logging in to the application *neo* and must be confirmed by clicking on *OK*.

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.

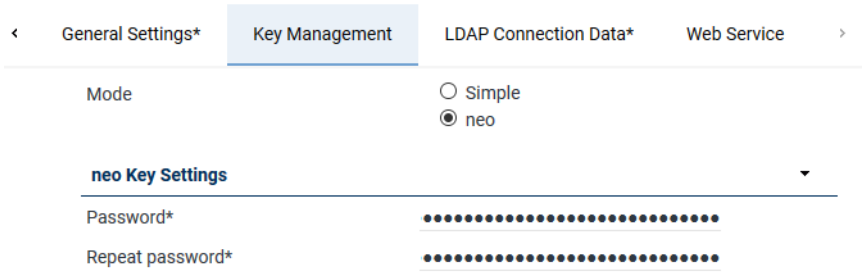

Fig. 31: Tenants module - tab Key Management

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 Login Settings", p. 24).

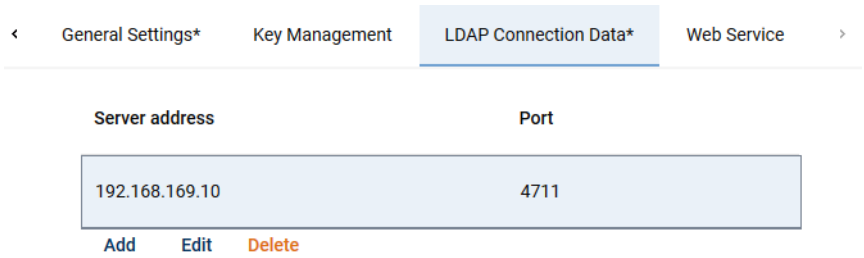

Fig. 32: Tenants module - tab LDAP Connection Data

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

4.2.5.1 Edit LDAP connection data

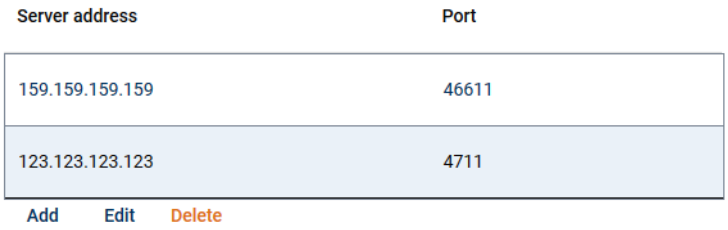

Fig. 33: LDAP Connection Data

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

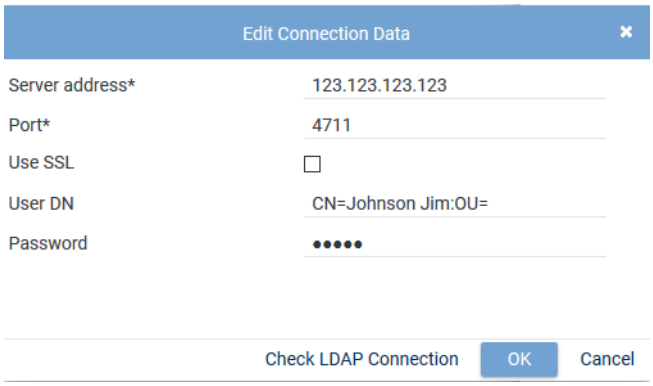

Fig. 34: Edit LDAP connection data (example)

Server address	IP address of the LDAP server.
Port	Port on the LDAP server which is used to establish a connection. By default, the following port is used: 389 = LDAP connection, unencrypted 636 = LDAP connection, encrypted
Use SSL	Activate or deactivate the usage of the SSL protocol. ☑ = SSL is used. ☐ = SSL is not used.

	NOTICE! SSL can only be used if the LDAP server supports SSL.
User DN	Distinguished name (DN) of the user required for the authentication to the LDAP server.
Password	Password required for the authentication to the LDAP server.

2. Complete all fields or only the mandatory ones.
3. 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*.
4. 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.

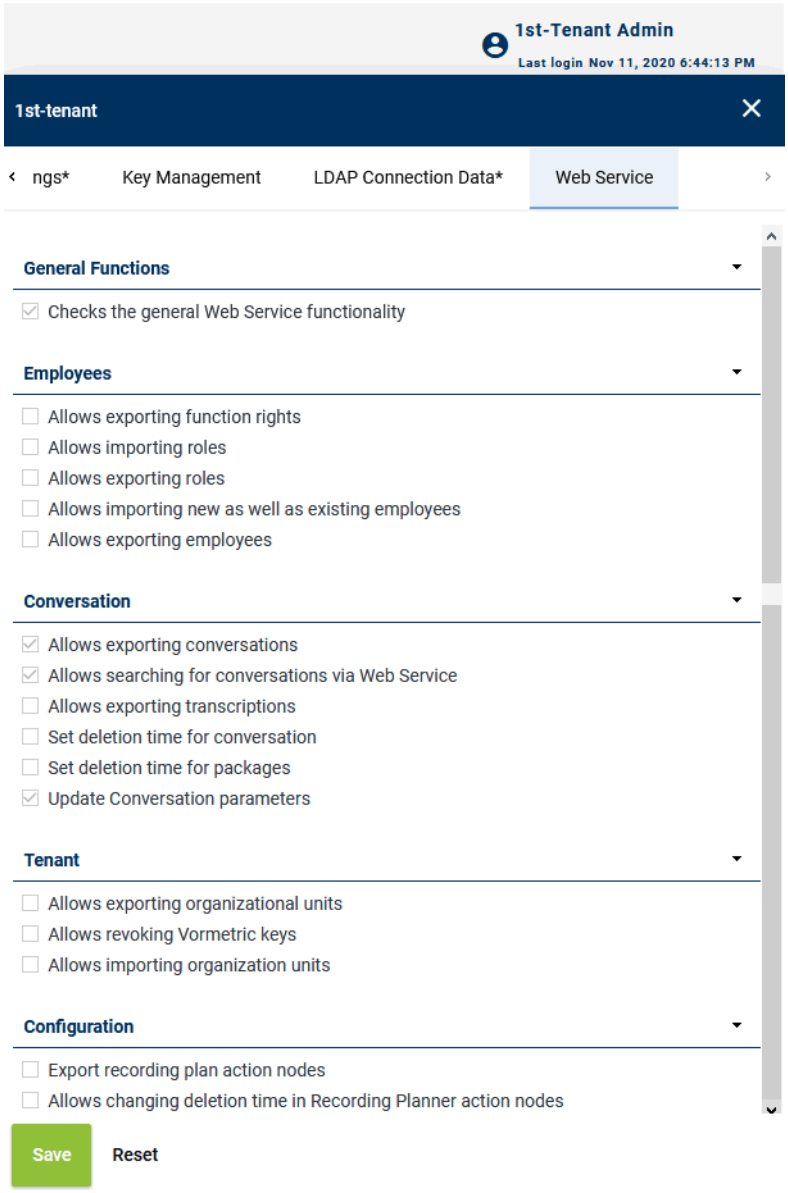

Fig. 35: Display web service functions

☑ = Function has been activated.

☐ = Function has been deactivated.

Group field General Functions

Checks the general web service functionality	Shows whether you can check the functionality of the Web Service.

Group field Employees

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

Group field Configuration

Allows importing audio analysis configurations	Shows whether importing audio analysis configurations is possible.
Allows importing Recording Planner action nodes	Shows whether importing Recording Planner action nodes is possible.
Allows exporting audio analysis configurations	Shows whether exporting audio analysis configurations is possible.
Allows exporting Recording Planner action nodes	Shows whether exporting Recording Planner action nodes is possible.
Allows changing deletion time in Recording Planner action nodes	Shows whether changing the deletion time in Recording Planner action nodes is possible.
Allows importing recording plan profiles	Shows whether importing recording plan profiles is possible.
Allows exporting recording plan profiles	Shows whether exporting recording plan profiles is possible.

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.

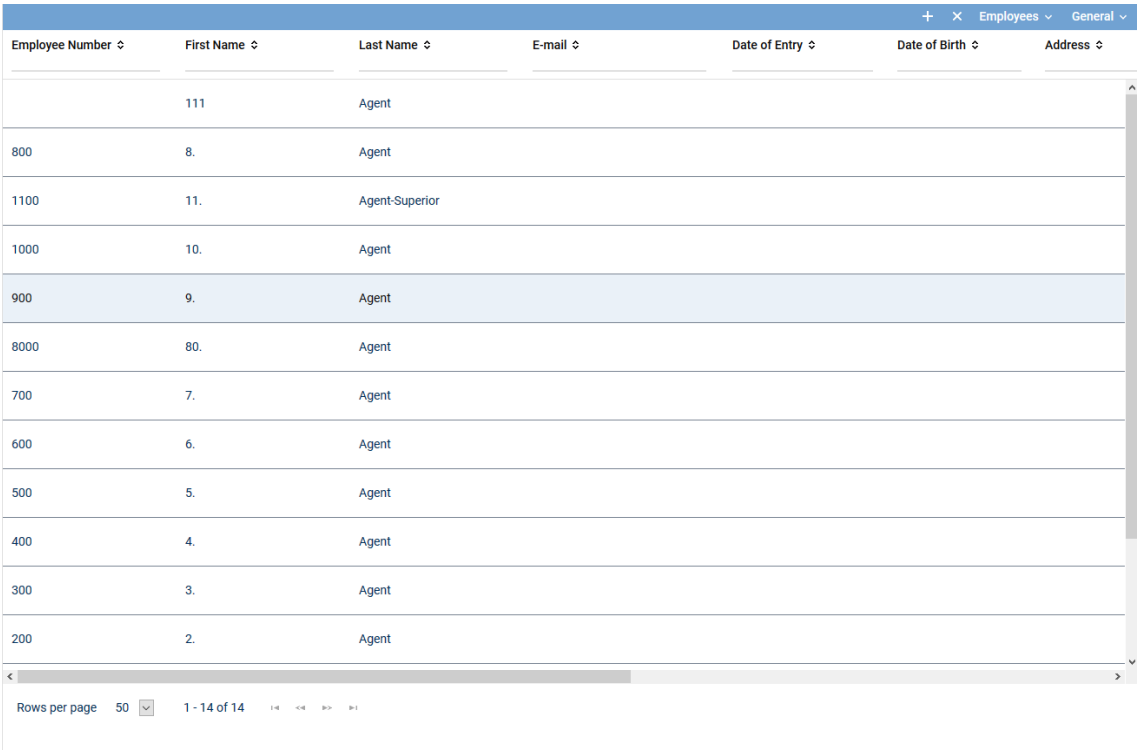

Fig. 36: Employees module - main view

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

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

5.1.1 Toolbar

The toolbar offers the following functions.

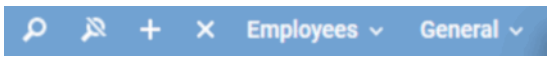

Fig. 37: Employees module - toolbar

	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria (see chapter "Search", p. 35). The icon *(Search)* is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all manually entered search criteria. The search is started without manual filter settings.
	Add	Creates a new employee (see chapter "Create new employee", p. 63).
	Delete	Deletes the selected employee.
Employees	*Summary*	Lists all function rights of the selected employee (see chapter "Show summary", p. 34).
	Show locked employees/Show all employees	Lists only the locked employees in the main view (see chapter "Show locked employees", p. 35).
	Make employee visible or not visible	Function which makes the selected employee visible or not visible for others (see chapter "Make employee visible or not visible", p. 35).

	Display agent's shift schedule	Opens a window in which you can see the shift schedule of the selected agent. **NOTICE!** The icon is only displayed if the connection to the Teleopti server has been activated. **NOTICE!** 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.
	Export User Data	Exports the user data of the employee of the current tenant in XML format.
General	*Print*	Prints the table of the main view.
	Adjust table	Opens a window in which you can adjust the following settings for the main view: • Displayed information • Order of the displayed columns • Number of rows per page
	General Help	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.
	Module Help	By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.

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

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.

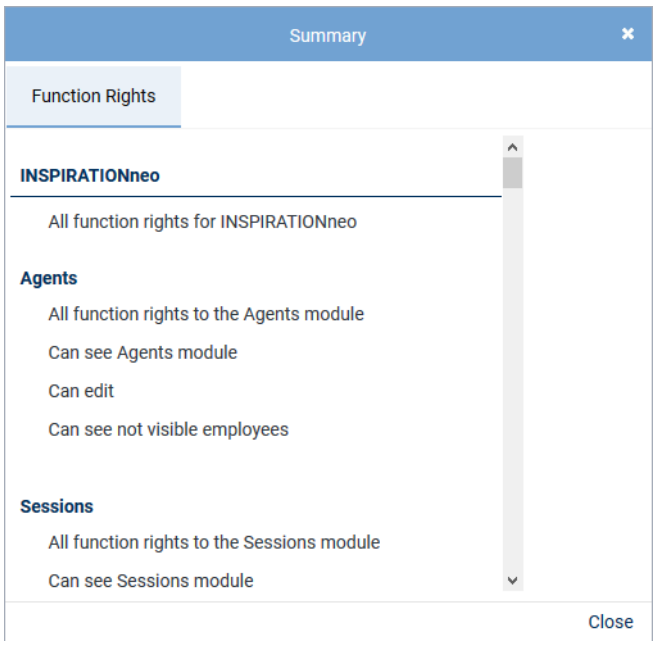

Fig. 38: Summary of the function rights

	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.

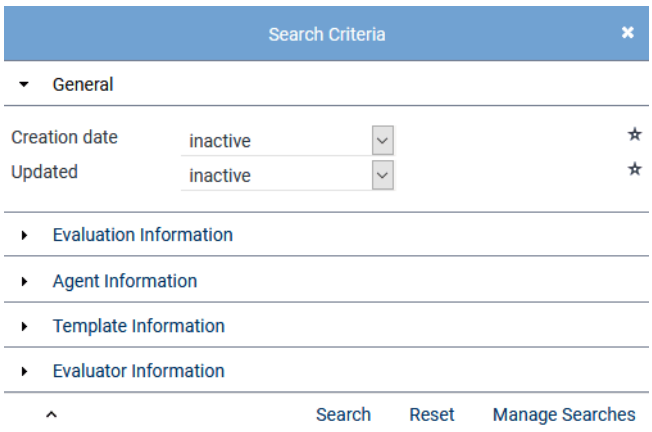

Fig. 39: Window Search Criteria (example)

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.

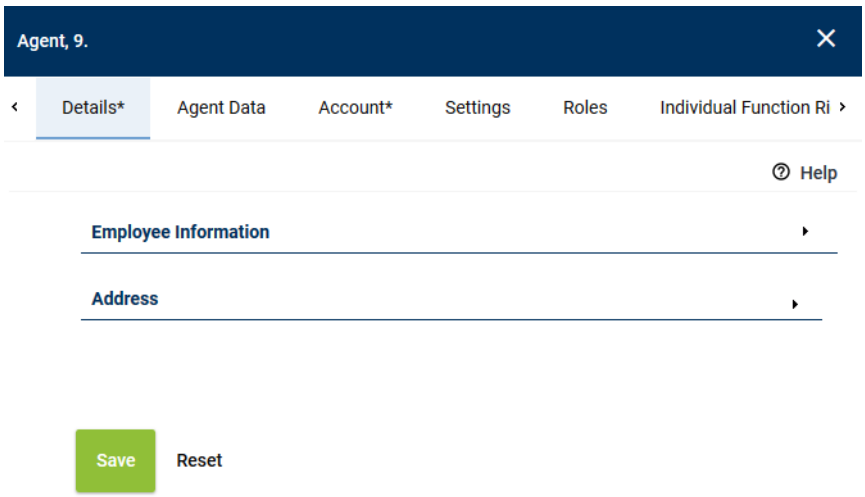

Fig. 40: Employees module - detail view

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. 37.

- *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. 41.

- *Account*

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

  See chapter "Tab Account", p. 47.

- *Settings*

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

  See chapter "Tab Settings", p. 50.

- *Roles*

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

See chapter "Tab Roles", p. 55.

- *Individual Function Rights*

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

  See chapter "Tab Individual Function Rights", p. 56.

- *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. 59.

- *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. 61.

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.

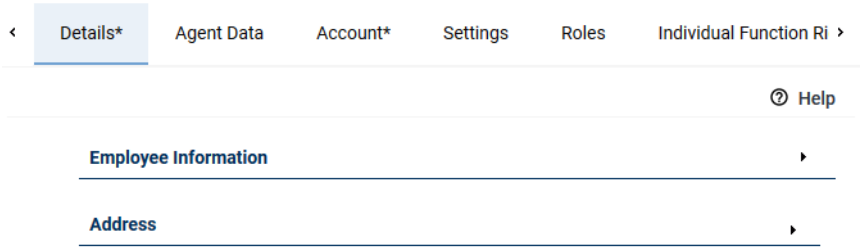

Fig. 41: Employees module - tab Details

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*.

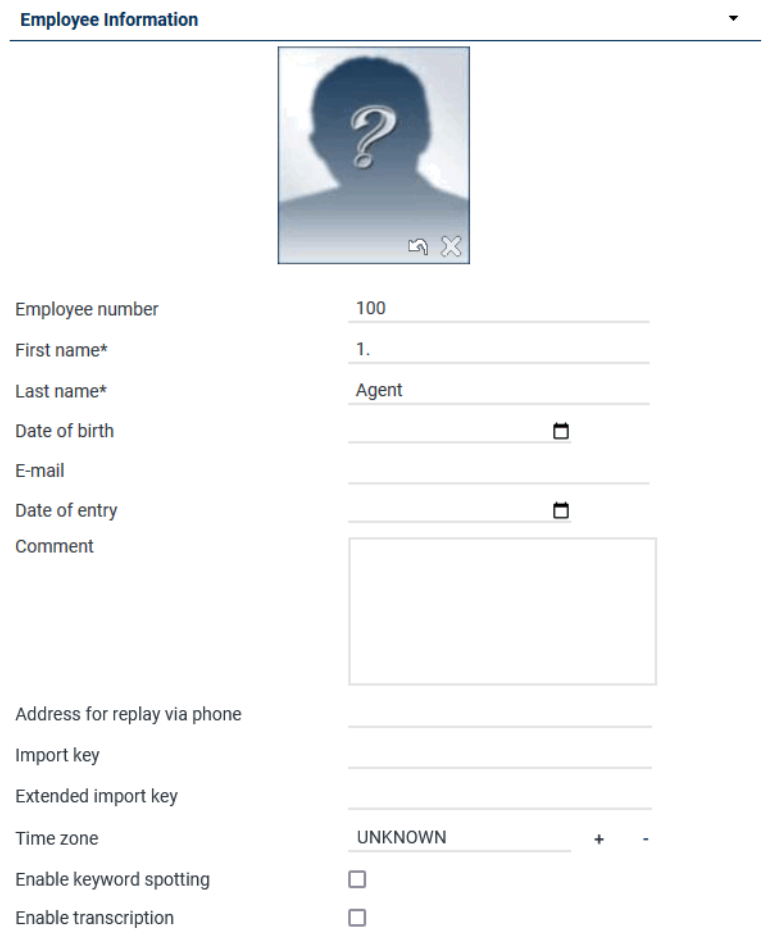

Fig. 42: Edit employee information

	Placeholder for the employee's photo. See chapter "Upload or delete image", p. 40.
Employee Number	ID of the employee.
First Name	First name of the employee.
Last Name	Last name of the employee.
Date of birth	Date of birth of the employee. You can enter the date directly via the keyboard or via the icon.
E-mail	E-mail address of the employee.
Date of Entry	Day on which the employee was hired. You can enter the date directly via the keyboard or via the icon.
Comment	Comment on the employee information.
Address for replay via phone	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: • Extension if it has been configured in the PBX for replay via phone. • Complete phone number, e. g. *06021 5001 1015* if the PBX is connected to the public telephone network. • IP address if it has been configured.

	• MAC address if it has been configured. • SIP address, e. g. *Extension@IP-Address*.
Import key	Key to unambiguously identify an employee imported from an external source. 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. In addition, the import key is used when transferring (export/import) recordings from a *neo* system to another *neo* 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. **NOTICE!** 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.
Extended import key	Extended key to unambiguously identify employees imported from an external source. The extended import key is used whenever the standard import key is not sufficient for an unambiguous identification. An example where the extended import key is used is during the import of calls from the application Recording Insights. Here, the import key alone is not sufficient as the users come from different LDAP systems and several attributes are compiled in an extended import key for unambiguous identification. When the employee's data is imported for the first time, the import key is entered here automatically. With every new import, this import key is checked to determine whether the employee has already been imported. In addition, the import key is used during the export/import of recordings from one *neo* system to another *neo* system to map the recordings to the agents. If the employee does not have an automatically generated import key, you can enter an import key manually for this purpose. **NOTICE!** If you change an import key manually, the employee will not be recognized as having been imported before already. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordings.
Time zone	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 To select the time zone, click on the button + . See chapter "Add time zone", p. 14. To delete the selection, click on the button - .
Activate keyword spotting	Select whether the employee's conversations are supposed to be considered for the speech analysis method *keyword spotting*. ☑ = Consider for keyword spotting ☐ = Do not consider for keyword spotting **NOTICE!** This option is only available in systems with a cloud license.

Activate transcription	Select whether the employee's conversations are supposed to be considered for the speech analysis method *Transcription*. ☑ = Consider for transcription ☐ = Do not consider for transcription **NOTICE!** This option is only available in systems with a cloud license.

5.2.1.1.1 Upload or delete image

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

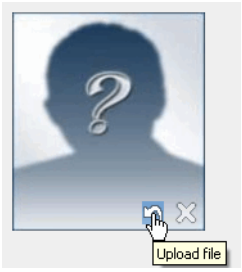

Fig. 43: Upload image

⇨ The window *Upload File* appears.

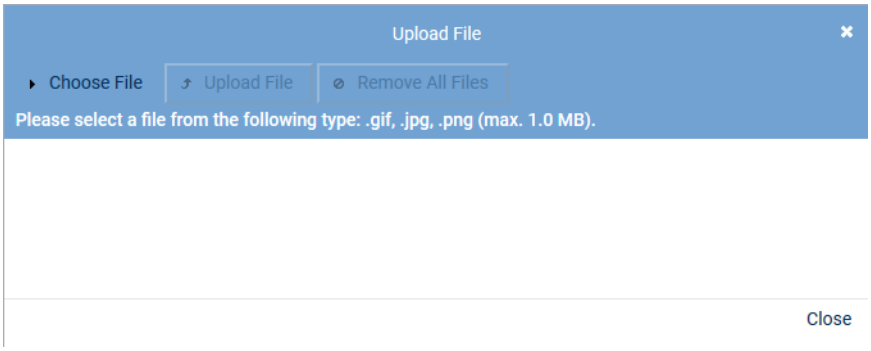

Fig. 44: Upload File

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.

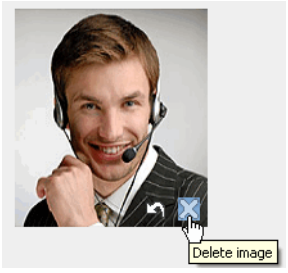

Fig. 45: Delete image (example)

⇨ 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.

Fig. 47: Add address

4. 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. 43.

To configure screen recording for agents, see chapter "Configure screen recording", p. 46.

To configure the recording of the agent's chats, see chapter "Configure chat recording", p. 45.

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. 55.

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. 56.

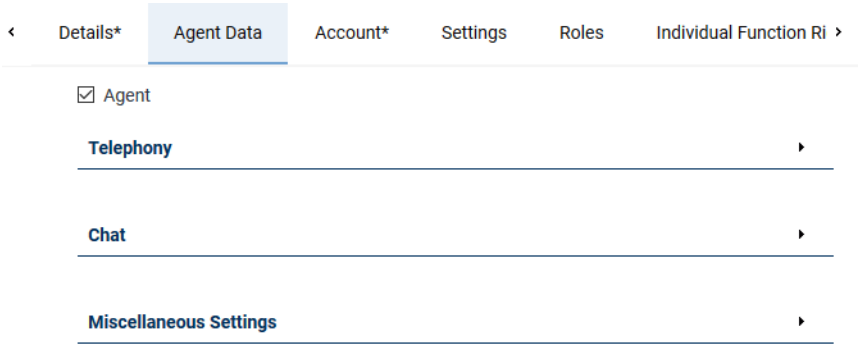

Fig. 48: Employees module - tab Agent Data

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*.

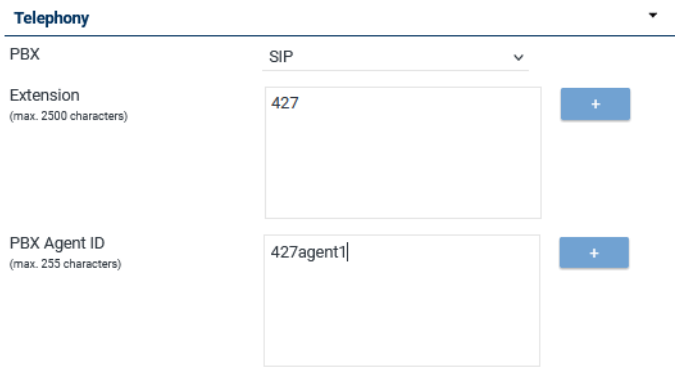

Fig. 49: Agent Data - Telephony

PBX	PBX via which the agent's conversations are made. Select the PBX from the drop-down list.
Extension	Extensions which are supposed to be assigned to the agent. Enter the extensions in the entry field or click on the icon + to select an extension assigned to the tenant by the system provider in the opening window. **NOTICE!** Use commas to separate the different extensions.
PBX Agent ID	IDs which have been saved in the PBX for the agent, too. By means of these IDs the recording system can identify an agent and his participation in a conversation. Enter the IDs of the agent in the entry field or click on the icon + to select a PBX Agent ID assigned to the tenant by the system provider in the opening window. **NOTICE!** Use commas to separate the different IDs.

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*.

5.2.2.1.2 Add extension

1. Select the extension you would like to add in the list and click on the button *Add*. To select several entries, select the respective entries while holding the [Ctrl] key down.
   To discard the entries, click on the button *Cancel*.

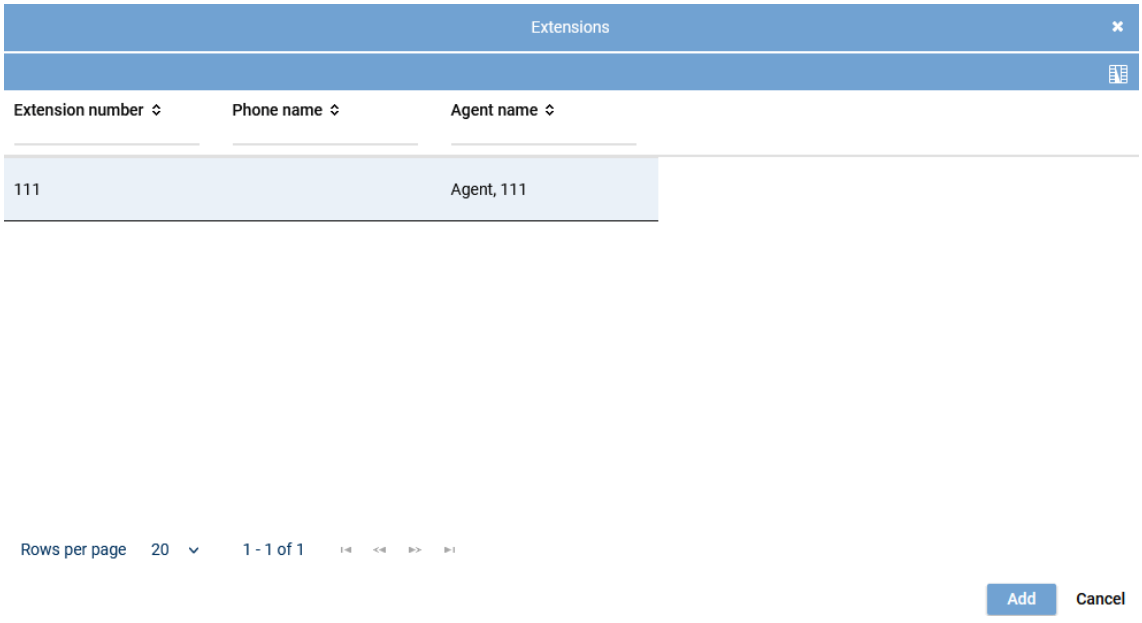

Fig. 50: Add extension (example)

The list only displays those extensions that are actually available to the tenant which includes extensions that have already been assigned to an agent. However, it is not possible to assign already assigned extensions to another agent.

5.2.2.1.3 Add PBX Agent ID

1. Select the PBX Agent ID you would like to add in the list and click on the button *Add*. To select several entries, select the respective entries while holding the [Ctrl] key down.
   To discard the entries, click on the button *Cancel*.

Fig. 51: Add PBX Agent ID (example)

The list only displays those PBX Agent IDs that are actually available to the tenant which includes extensions that have already been assigned to an agent. However, it is not possible to assign already assigned PBX Agent IDs to another agent.

5.2.2.2 Group field Chat

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

Fig. 52: Agent Data - Chat

Chat system	Chat server via which the agent's chats run. Select the chat server from the drop-down list.
Chat ID	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 IDs of the agent in the entry field or click on the icon + to select a chat ID assigned to the tenant by the system provider in the opening window. **NOTICE!** 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. 41.
2. Open the group field *Chat* in the tab *Agent Data*, see chapter "Group field Chat", p. 44.
3. Select the chat system from the drop-down list.
4. Enter the agent's chat ID in the entry field.

5.2.2.2.2 Add chat ID

1. Select the extension you would like to add in the list and click on the button *Add*. To select several entries, select the respective entries while holding the [Ctrl] key down.
   To discard the entries, click on the button *Cancel*.

Fig. 53: Add chat ID (example)

The list only displays those chat IDs that are actually available to the tenant which includes extensions that have already been assigned to an agent. However, it is not possible to assign already assigned chat IDs to another agent.

5.2.2.3 Group field Miscellaneous Settings

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

Fig. 54: Agent Data - Miscellaneous Settings

Login name	Windows login name of the agent. Enter the Windows login name in the entry field. **NOTICE!** The Windows login name is used for the following features: • *Screen recording* (application SCREEN*rec*)
Computer name	Name of the computer that the agent uses. Enter the computer name in the entry field. **NOTICE!** The computer name is used for the following features: • *Screen recording* (application SCREEN*rec*) • *Replay via phone*
Dispatcher	This function is not available yet.
Video recording	Select whether video recordings of the employee are supposed to be saved. ☑ = Video recordings are saved. ☐ = 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 SCREEN*rec* 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 SCREEN*rec* either uses the agent's *login name* or the *computer name*, see chapter "Group field Miscellaneous Settings", p. 45. 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 SCREEN*rec* 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.

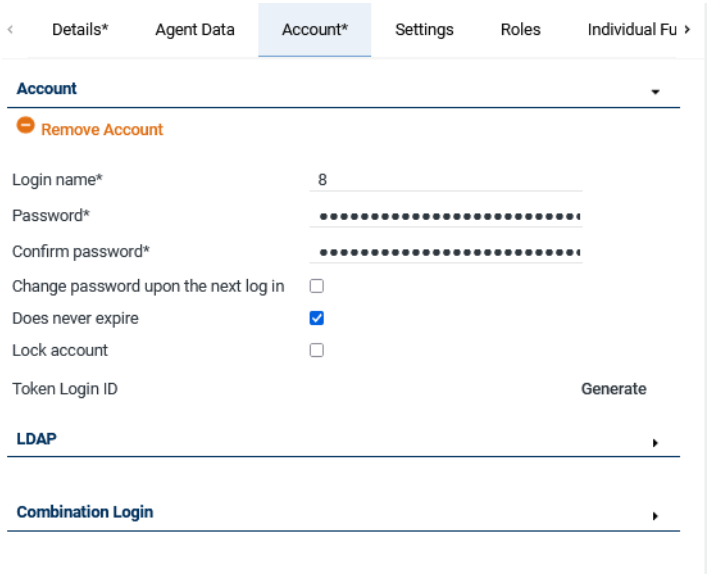

Fig. 55: Employees module - tab Account

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*.

Fig. 56: Add account

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

User name	Enter the login name which is required for the employee to log in to the system. **NOTICE!** We recommend to enter an e-mail address as user name to ensure an unambiguous mapping of users. **NOTICE!** If the function *SSO* login is used, the login name has to consist of the Windows login name and the domain. Format: *Domain\Windows_login_name* **NOTICE!** If you use the function *Last Call Repeat*, you must use exclusively digits here.
Password	Enter the password which is required for the employee to log in to the system. **NOTICE!** If you use the function *Last Call Repeat*, you may use numbers only here.
Confirm password	Enter the password for the employee again.

Change password upon the next login	Activate this option if the employee is supposed to change the password upon logging in the next time.
Does never expire	Activate this option if the password is never supposed to expire. **NOTICE!** This option is not available for superusers.
Does not have to meet the password rules	Activate this option if the password does not necessarily have to be consistent with the password rules. **NOTICE!** Password rules can be defined in the Tenants module in the tab *Passwords*. **NOTICE!** This option is not available for superusers.
Lock account	This option allows locking the employee's account. In the main view, you can filter for this criterion, see chapter "Show locked employees", p. 35. **NOTICE!** This option is not available for superusers.
Token login ID	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 *Generate*. This login ID is configured to automate login for this employee. **NOTICE!** This option is only available for tenants.
POWERplay Web for Xpert login ID	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 *Generate*. This login ID is configured by the system manager of OpenScape Xpert to automate login for this employee. **NOTICE!** This option is only available for tenants.

4. If you would like to remove the account, click on the button *Remove account* in the title bar of the group field.
5. To activate the authentication via LDAP for the employee, see chapter "Authentication via LDAP", p. 48.
6. To assign the employee a combination user, see chapter "Assign combination user", p. 48.

5.2.3.1 Authentication via LDAP

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

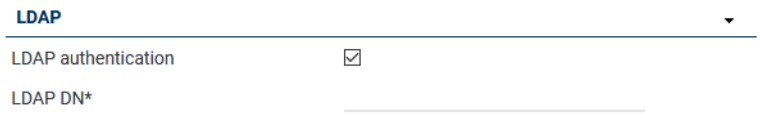

Fig. 57: Activate authentication via LDAP

3. Enter the complete Distinguished Name (DN) of the user in the field *LDAP DN*.
4. 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)*.

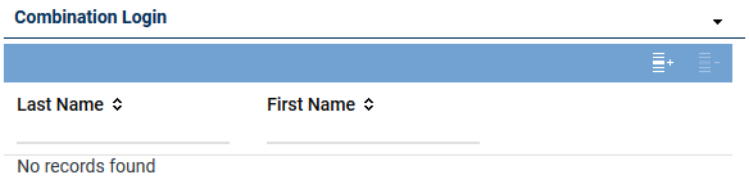

Fig. 58: Assign combination user

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.

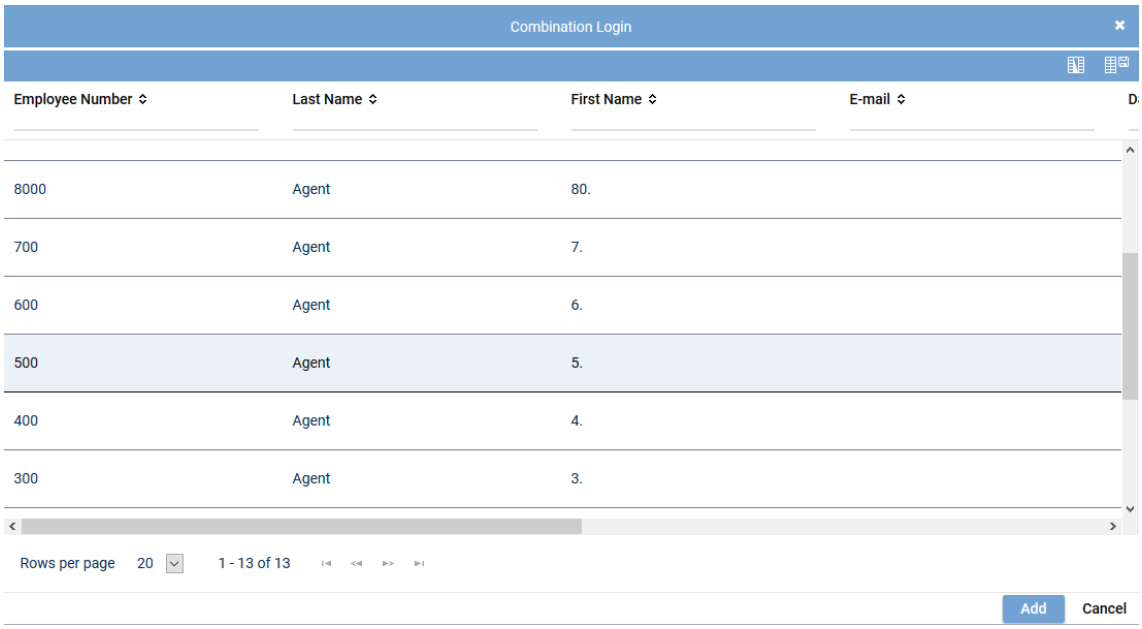

Fig. 59: Add combination user

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)*.

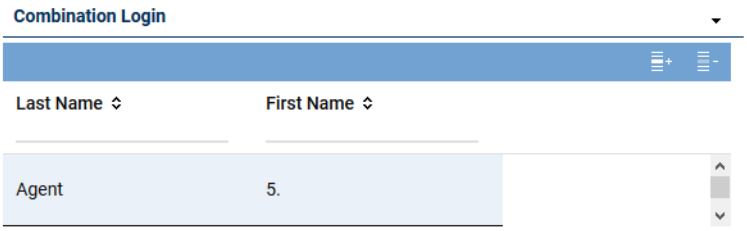

Fig. 60: Delete combination user assignment

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.

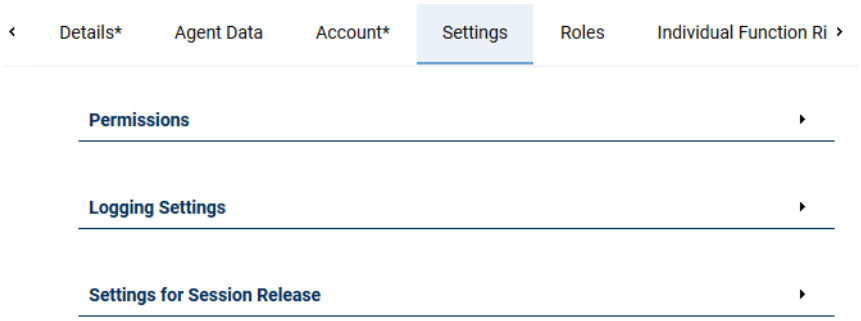

Fig. 61: Employees module - tab Settings

5.2.4.1 Group field Permissions

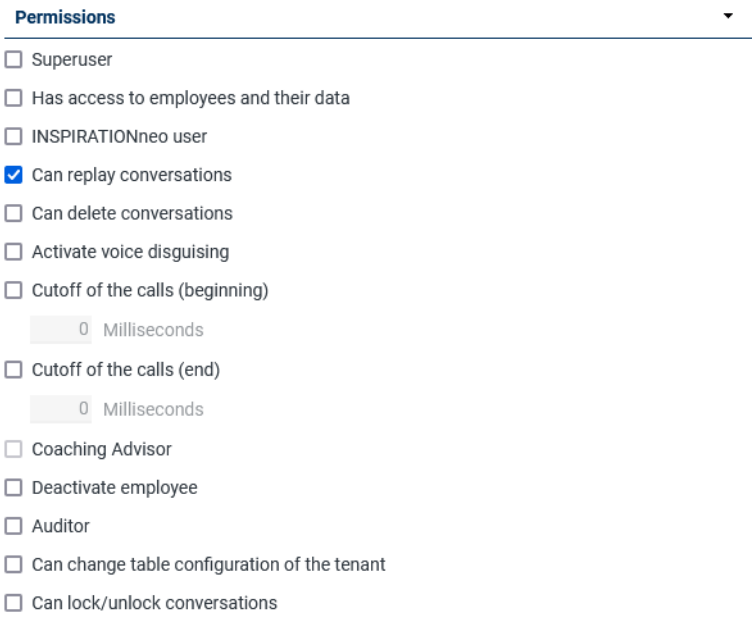

Fig. 62: Configure permissions

☑ = Right has been activated.

☐ = Right has been deactivated.

Superuser	This right assigns all function rights in the system to the user if their licenses are available.

Has access to employees and their data	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. Without this right, the user can only see the data of other employees if he is the superior of the organization unit (see chapter "Tab Organization Units", p. 61). In this case, he can exclusively see the data of the members of these organization units and his own data.
INSPIRATIONneo user	This right enables the user to log in to the application INSPIRATION*neo*. **NOTICE!** If this right has been deactivated, it is not possible to log in to the application INSPIRATION*neo*.
Can replay conversations	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.
Can delete conversations	This right allows the user to delete a conversation in the application POWER*play* Web. This option is license-dependent.
Activate voice disguising	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.
Cutoff of the calls (beginning)	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.
Cutoff of the calls (end)	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.
Coaching Advisor	This right allows the user to record coaching advisor sessions by means of the application CLIENT*command*. Coaching advisor session are simulated sessions which are recorded for training purposes. These sessions are displayed in the Coaching Advisor module of the application INSPIRATION*neo*. For a user to be able to access the Coaching Advisor module, you have to assign the respective right in the tab *Individual Function Rights* to the user. See chapter "Tab Individual Function Rights", p. 56.
Deactivate employee	This right allows deactivating an employee. ☑ = Employee has been deactivated. ☐ = Employee has been activated. A deactivated employee will not be recorded anymore. A deactivated employee can no longer log in to the *neo* applications. Changing the status of a deactivated employee is not possible before 30 days have passed.
Auditor	This right allows the user to audit (record and evaluate) the screen activities of agents. In an audit, only the screen activities without the call are recorded. Auditors have restricted agent rights and can only see their own sessions and evaluations which are required to audit the respective agent.

	As the superior of an organization unit, the user has access to the data of the agents in this organization unit. When the above function right *Has access to employees and their data* has been activated, the user has access to all agents and their data. To enable an auditor to use INSPIRATION*neo*, the above function right *INSPIRATIONneo user* must have been activated. To enable an auditor to record the screen activities of agents, the client application SCREEN*rec* must have been installed on the agents' client computers. In the Recording Planner module, the conversation type *work item* must have been selected in the detail view of the recording plan.
Can change table configuration of the tenant	This right allows the user to change the default table configuration for the employees of the tenant. This applies to the main view of the respective modules as well as to dialog windows.
Can lock/unlock conversations	This right allows the user to locked conversations or to unlock locked conversations.

For information about the installation and usage of the client application SCREEN*rec* refer to the installation manual for tenants *Installation SCREENrec* and to the user manual for tenants *SCREENrec scan Editor*.

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

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

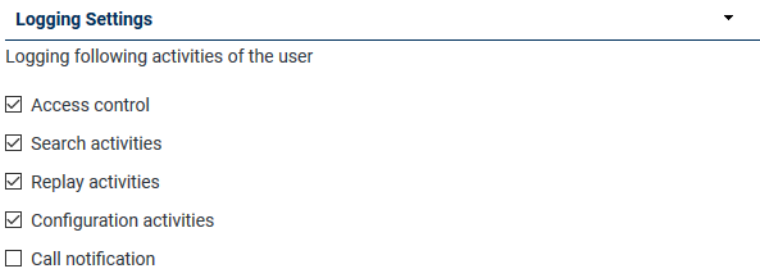

Fig. 63: Configure logging

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

☑ = Logging has been activated.

☐ = Logging has been deactivated.

Access control	If this option has been activated, the system logs when the user has signed in to and off from the system.

Search activities	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.
Replay activities	If this option has been activated, the replay activities of the user are logged to be able to see which conversations have been replayed.
Configuration activities	If this option has been activated, all adjustments of the configuration on behalf of the user are logged.
Call notification	If this option has been activated, the employee receives a notification containing the following conversation data once the conversation is over. Call ID, date, time from, time until, phone numbers of the participants The audit notification *EMPLOYEE_CONV_MAIL* must have been activated and configured. See administration manual *ASC System Configuration - Notifications module (for tenants)*.

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*neo* to release sessions for evaluation.

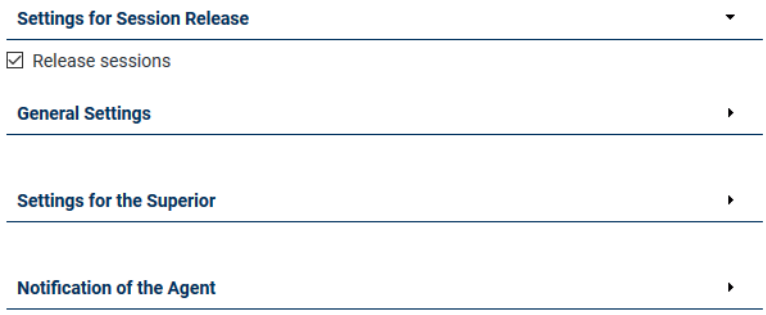

Fig. 64: Set session release for agents

Release sessions	☑ = Agents have to release their sessions so that they can be evaluated. The settings from the subordinated group fields are applied. ☐ = 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

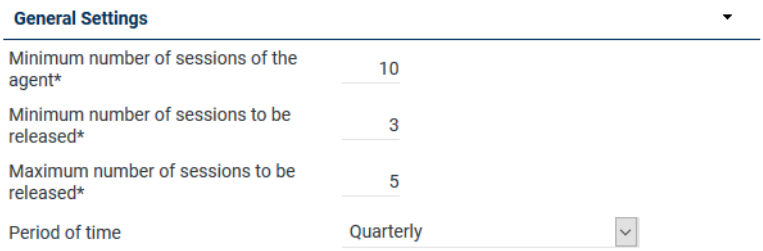

Fig. 65: Session release - General Settings

Minimum number of sessions of the agent	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.
Minimum number of sessions to be released	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. 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.
Maximum number of sessions to be released	Select how many sessions the agent can release within the defined period time at the maximum.
Period of time	Select the period of time that the settings of the session release are supposed to refer to. Select the period from the drop-down list.

Group field Settings for the Superior

Select which sessions the superior can see and evaluate.

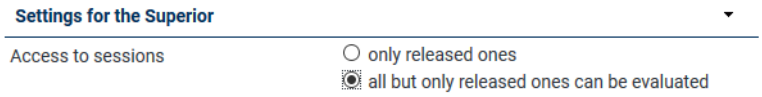

Fig. 66: Session release - Settings for the Superior

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 e 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.

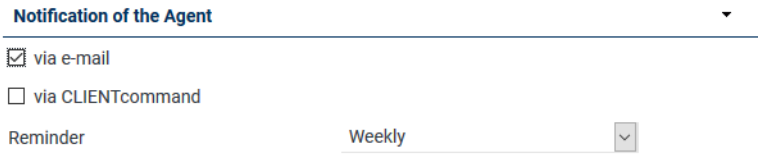

Fig. 67: Session release - Notification of the Agent

via e-mail	☑ = The agent is informed via e-mail. ☐ = The agent is not informed via e-mail.
via CLIENTcommand	☑ = The agent is informed in the application CLIENT*command*. ☐ = The agent is not informed in the application CLIENT*command*.
Reminder	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.

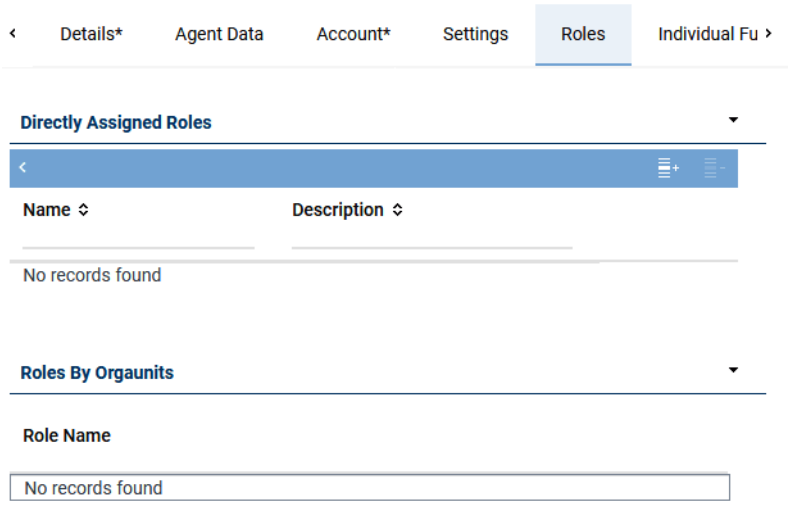

Fig. 68: Employees module - tab Roles

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)*.

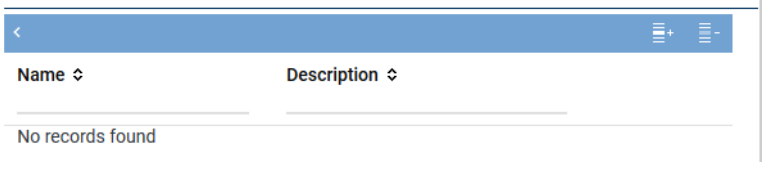

Fig. 69: Assign roles

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.

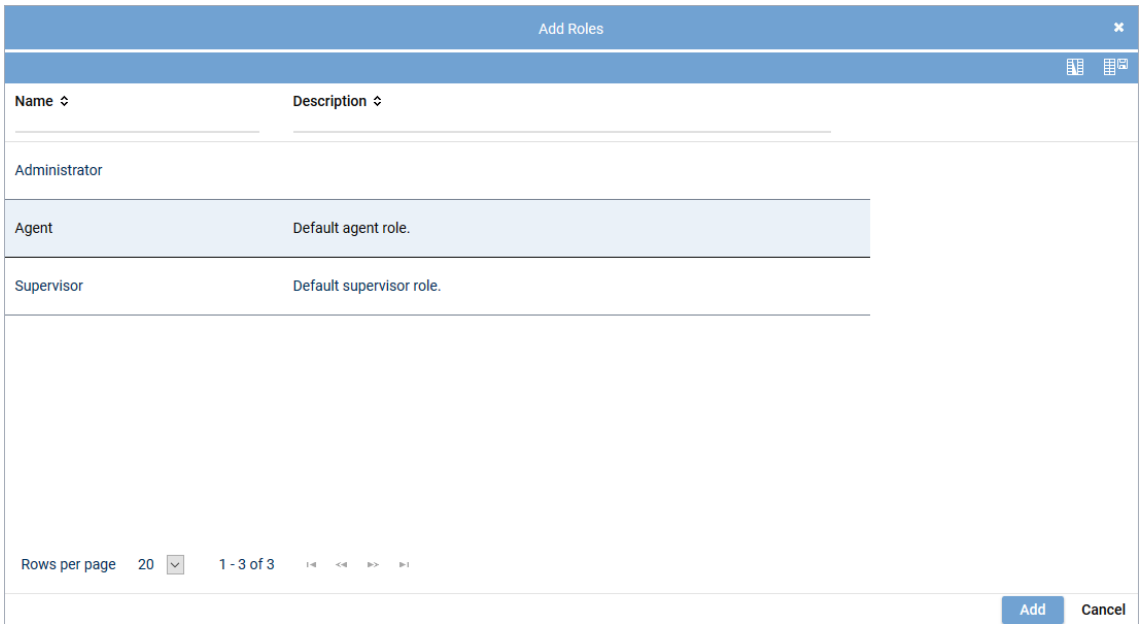

Fig. 70: Add role

3. 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

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

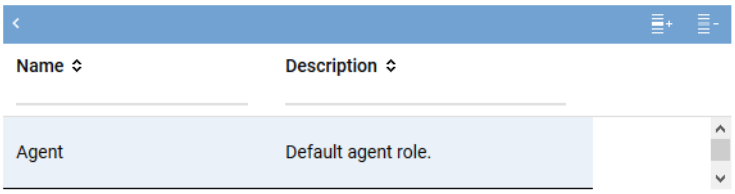

Fig. 71: Delete role assignment

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.

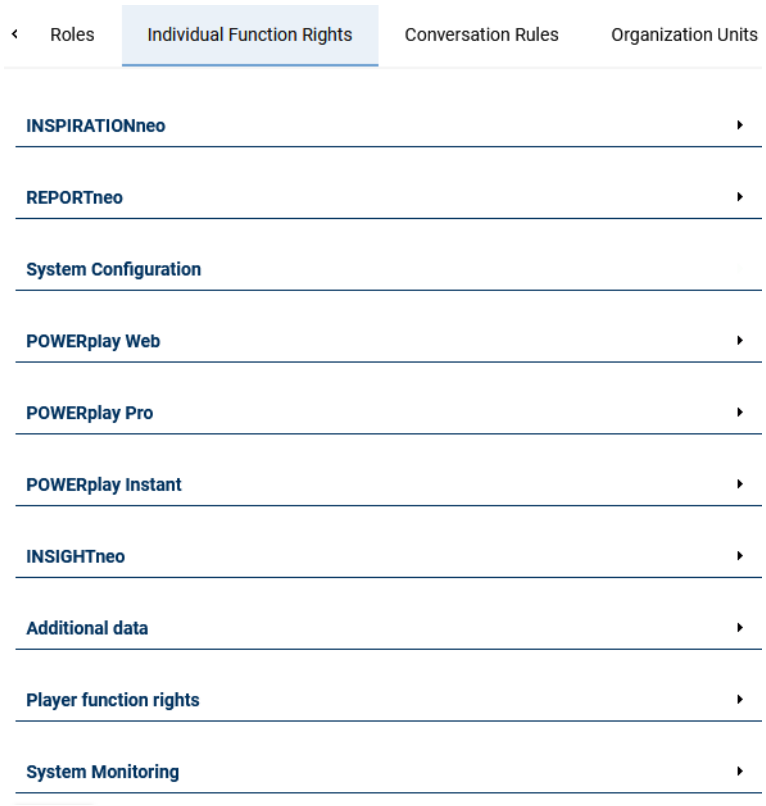

Fig. 72: Employees module - tab Individual Function Rights (example)

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

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

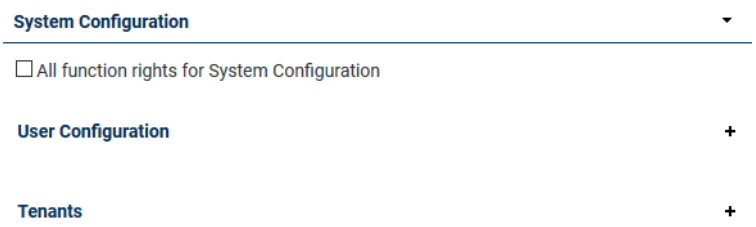

Fig. 73: Function rights - display sections (example)

2. 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.

3. 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.

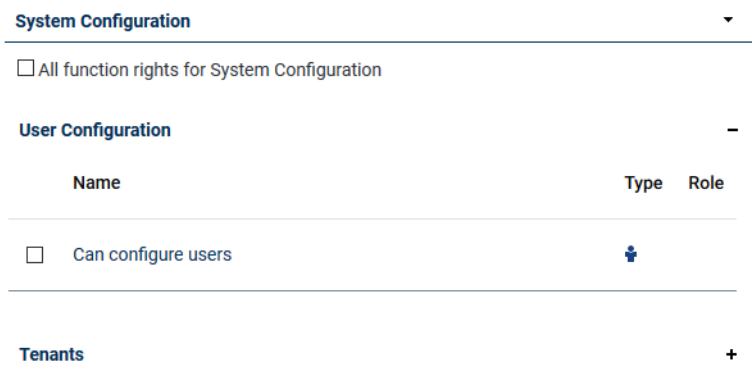

Fig. 74: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. ☑ = individual function right ☐ = 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 ✓ = role right **NOTICE!** In the window *Summary*, you can see via which role the function right has been assigned, see chapter "Show summary", p. 34.

Tab. 1: Function rights

4. 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.
5. 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	This function right allows removing edit locks. 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.

Tab. 2: Function rights INSPIRATIONneo > Evaluation templates

Group field Player

The options in the group field *Player* are implemented by all ASC player components offering the respective function. These are POWER*play* Pro, POWER*play* Web, and INSPIRATION*neo*.

Can create bookmark	This function right allows setting bookmarks to mark and comment sections of conversations.
Can edit bookmark	This function right allows editing comments (replay hints) about the bookmarks.
Can delete bookmark	This function right allows deleting bookmarks to mark and comment sections of conversations.
Can create mute section	This function right allows muting conversation sections for selected participants.
Can edit mute section	This function right allows editing participants to be muted.
Can delete mute section	This function right allows deleting the muting for selected participants.
Can confirm keyword	This function right allows setting the accuracy of the spotted keyword to 100 %.
Can export voice recordings	This function right allows exporting voice recordings.
Can export screen and video recordings	This function right allows exporting screen and video recordings.
Can export conversation data	This function right allows exporting the meta data of a list of search result (e. g. in POWER*play* Pro. Exporting meta data does not require any additional data export right.
Can set session category	This function right allows editing the assignment of sessions to categories in the player. This function is temporarily unavailable.
Can export chat recordings and text messages	This function right allows exporting chat recordings and text messages (SMS or SDS.

Tab. 3: Function rights player

5.2.7 Tab Conversation Rules

Here, you can display and assign the conversation rules for the employees.

Conversation rules can be defined in the Conversation Rules module.

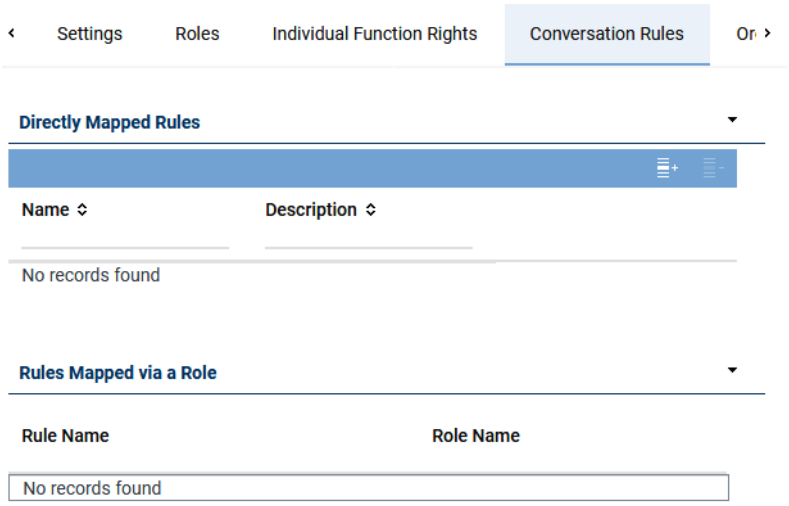

Fig. 75: Employees module - tab Conversation Rules

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*play* Web	• Conversation module • Participant View module
POWER*play* Pro	• Conversation module • Participant View module
INSPIRATION*neo*	• Sessions module • Calibrations module • Audio Analysis module

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. 60 and chapter "Delete conversation rule assignment", p. 61.

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)*.

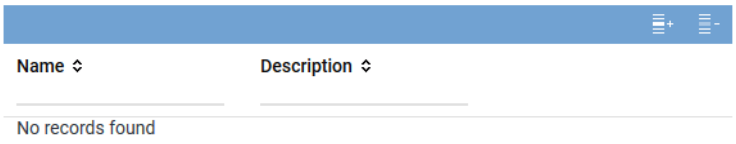

Fig. 76: Assign conversation rule

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.

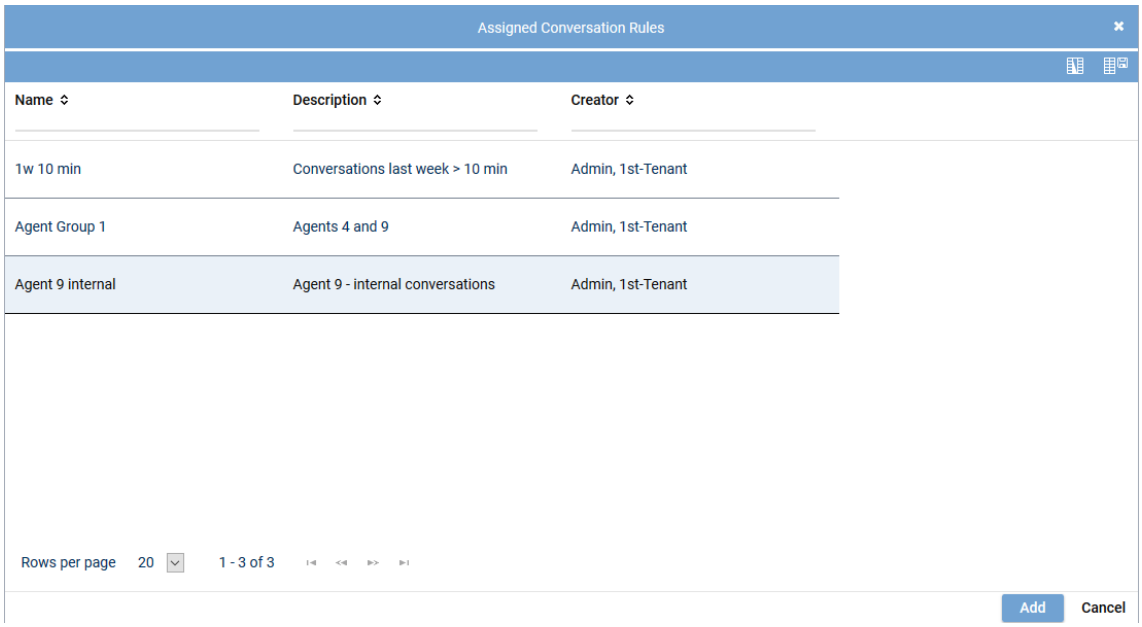

Fig. 77: Add conversation rules

3. 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

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

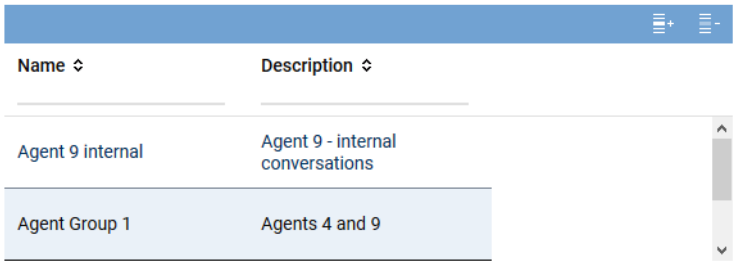

Fig. 78: Delete conversation rule assignment

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. 50) 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.

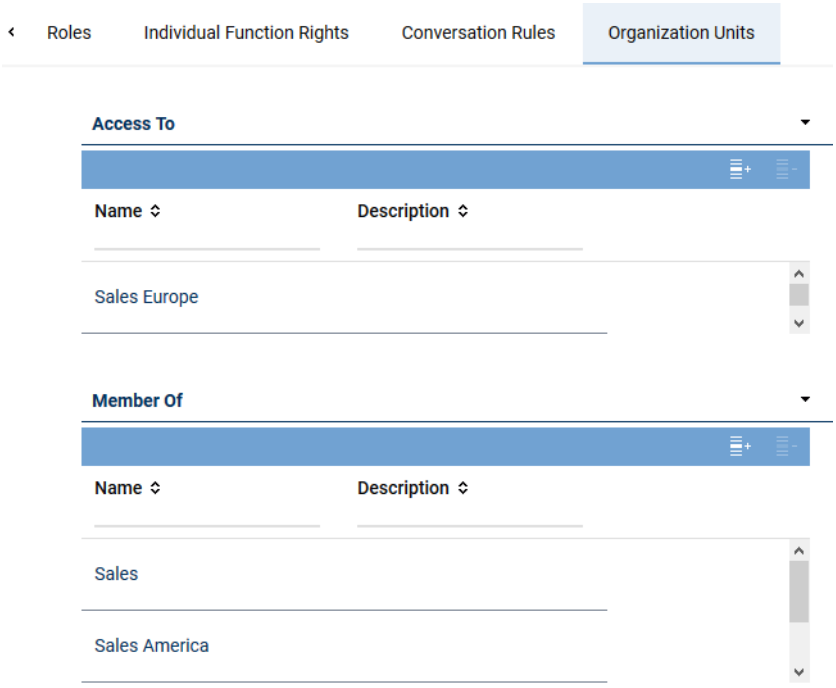

Fig. 79: Employees module - tab Organization Units

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 chapter "Assign organization units", p. 62 and chapter "Delete organization unit assignment", p. 63.

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 chapter "Assign organization units", p. 62 and chapter "Delete organization unit assignment", p. 63.

5.2.8.1 Assign organization units

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

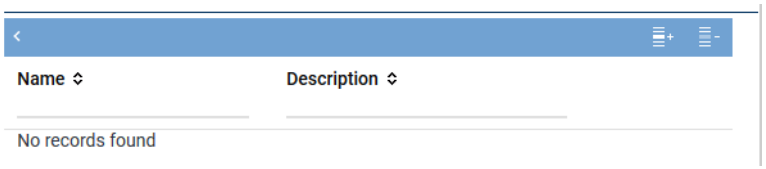

Fig. 80: Assign organization units

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.

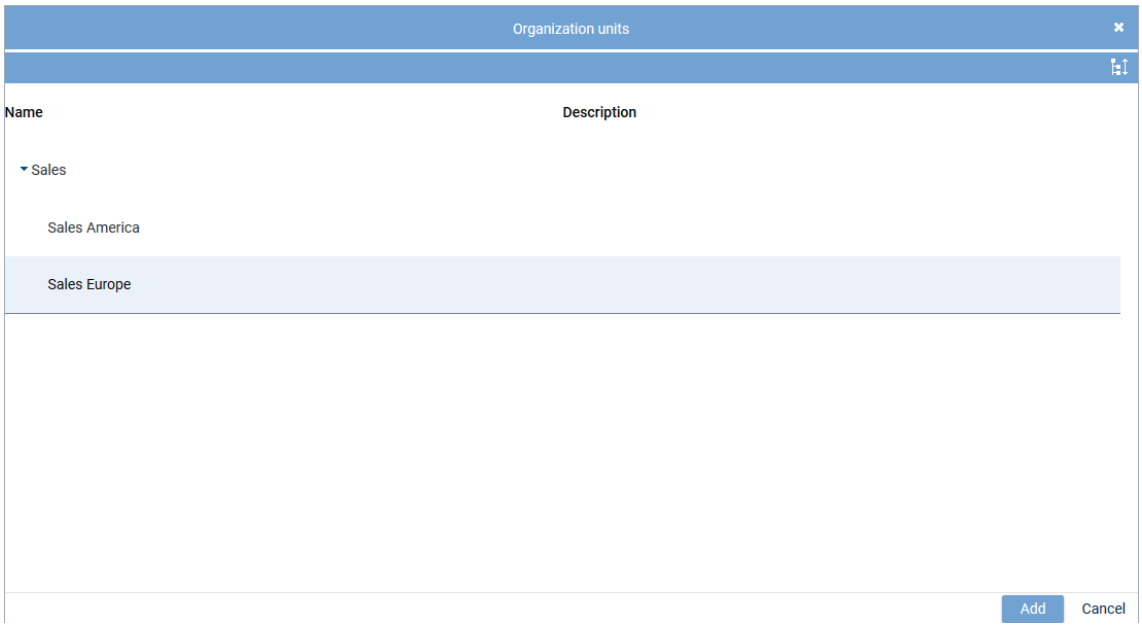

Fig. 81: Add organization units

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

3. 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

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

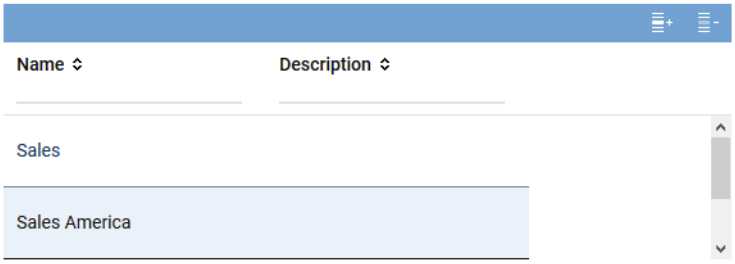

Fig. 82: Delete organization unit assignment

5.3 Create new employee

1. Click on the icon *(Add)* in the toolbar.
2. 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.
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*.

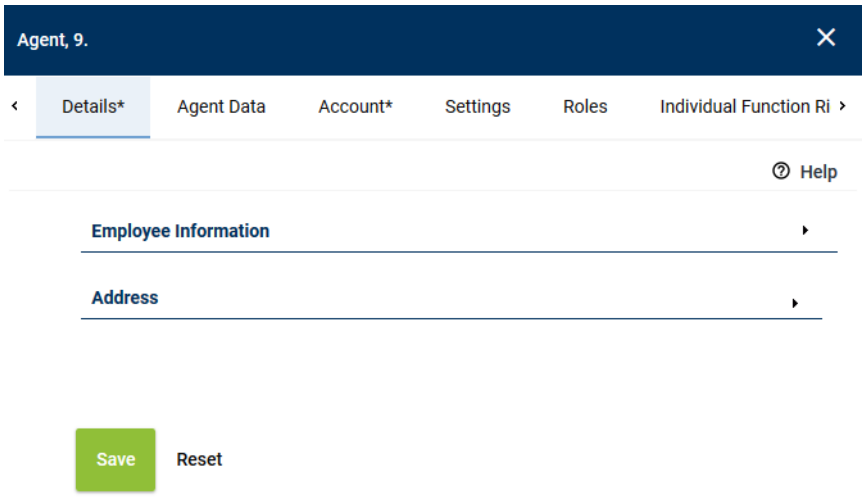

Fig. 83: Save employee

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.

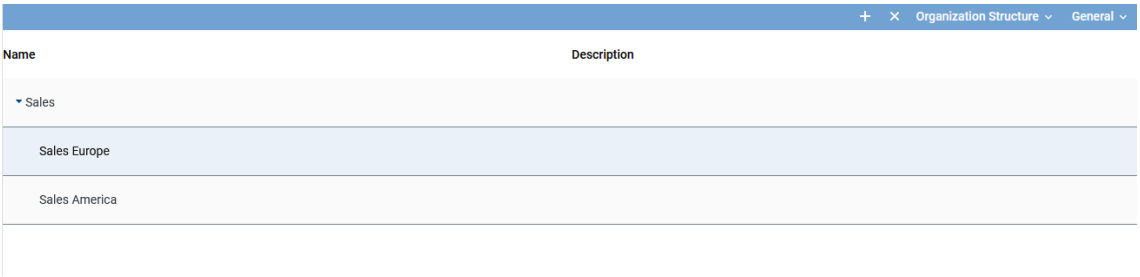

Fig. 84: Organization Structure module - main view

The following information is displayed in the main view:

Name	Name of the organization unit.
Description	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. 85: Organization Structure module - toolbar

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

+	*Create*	Creates a new organization unit (see chapter "Create new organization unit", p. 71).
×	*Delete*	Deletes the selected organization unit (see chapter "Delete organization unit", p. 72).

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

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

6.2 Detail view

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

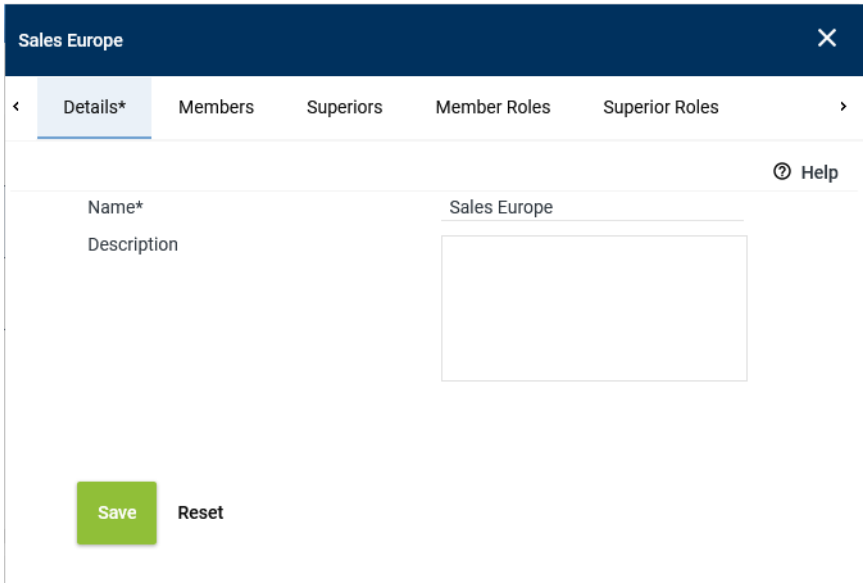

Fig. 86: Organization Structure module - detail view

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. 68.

- *Members*

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

  See chapter "Tab Members", p. 68.

- *Superiors*

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

  See chapter "Tab Superiors", p. 69.

- *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. 70.

- *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. 71.

6.2.1 Tab Details

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

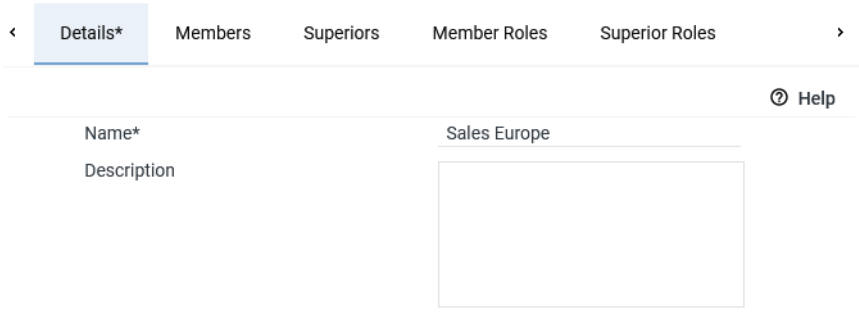

Fig. 87: Organization Structure module - tab Details

Name	Name of the organization unit.
Description	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.

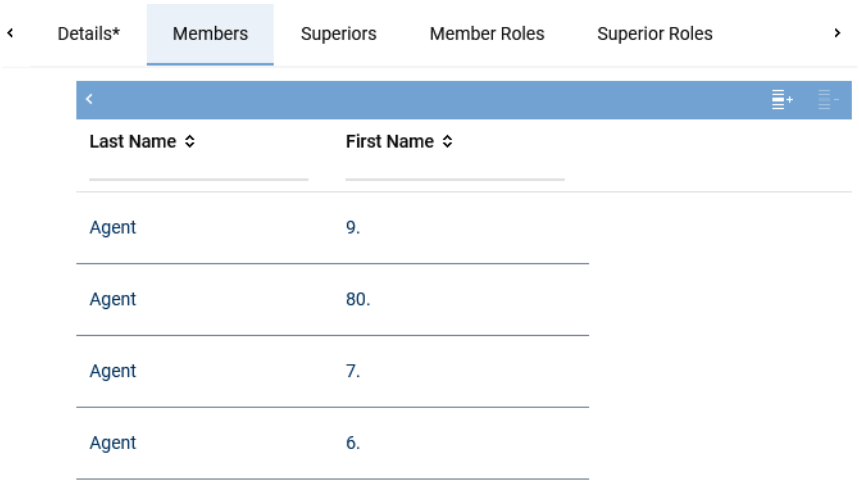

Fig. 88: Organization Structure module - tab Members

6.2.2.1 Assign members

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

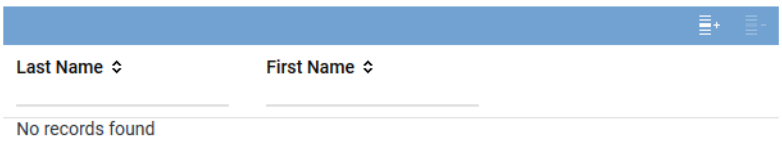

Fig. 89: Assign users

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.

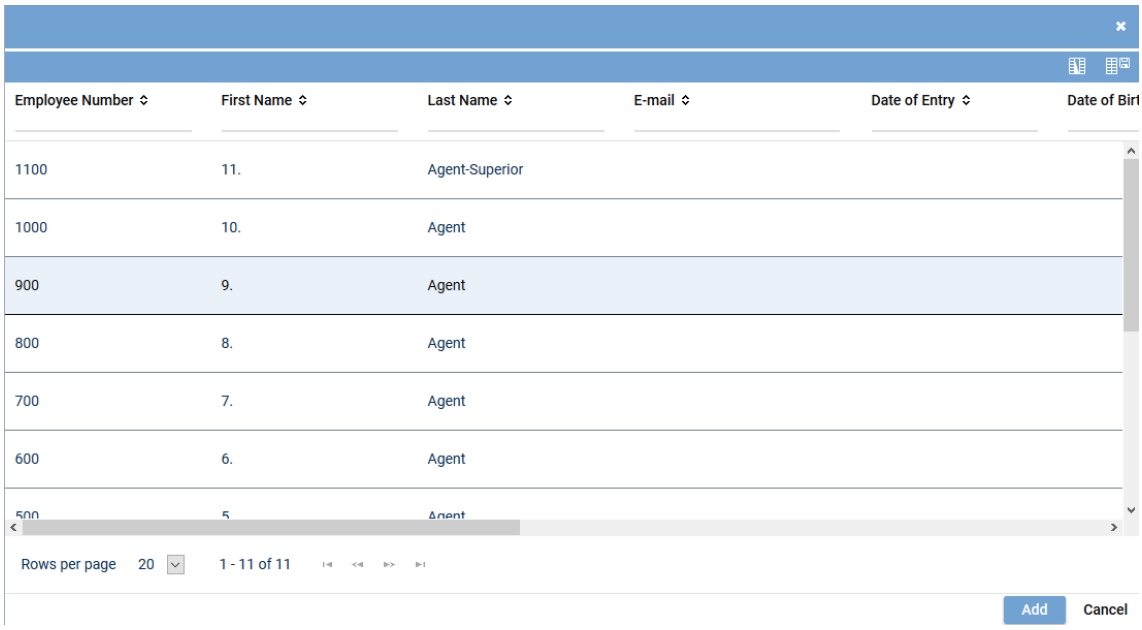

Fig. 90: Add user

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

6.2.2.2 Delete member assignment

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

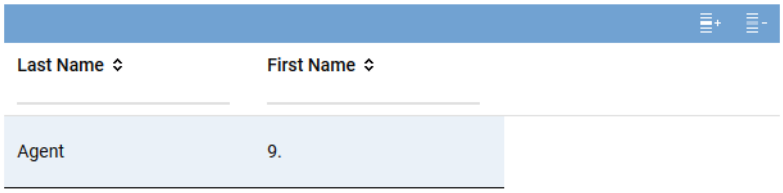

Fig. 91: Delete user assignment

6.2.3 Tab Superiors

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

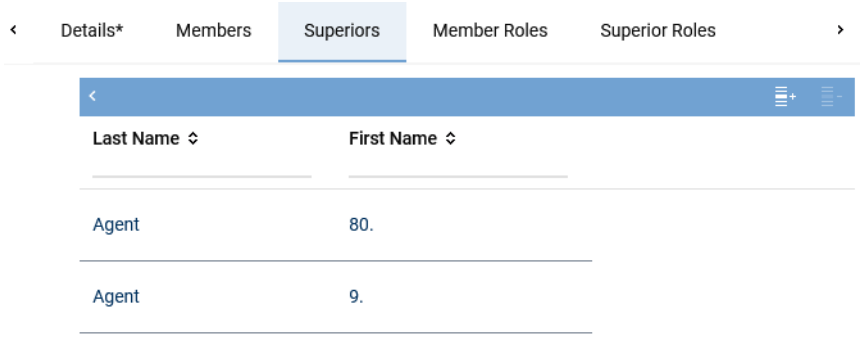

Fig. 92: Organization Structure module - tab Superiors

6.2.3.1 Assign superiors

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

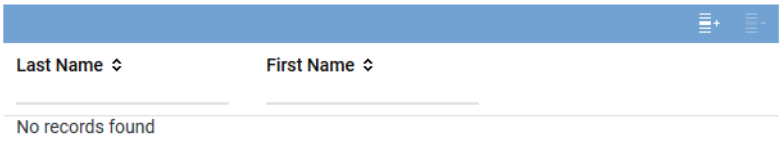

Fig. 93: Assign users

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.

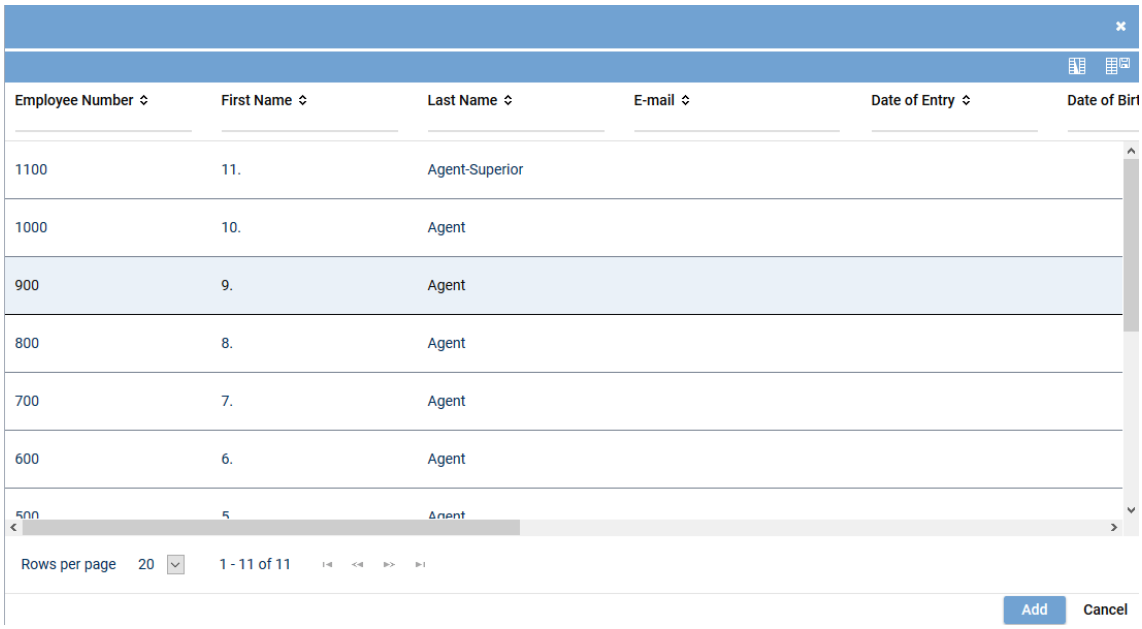

Fig. 94: Add user

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)*.

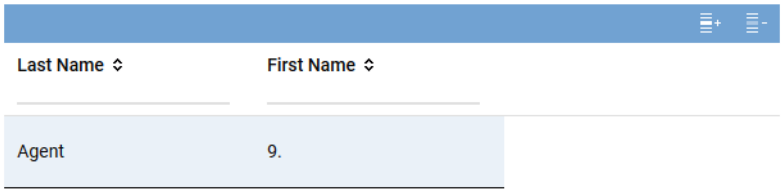

Fig. 95: Delete user assignment

6.2.4 Tab Member Roles

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

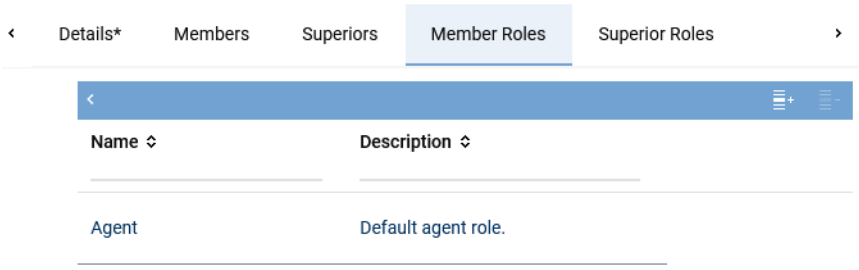

Fig. 96: Organization Structure module - tab Member Roles

For a description of how to add roles, see chapter "Assign roles", p. 55.

For a description of how to remove roles, see chapter "Delete role assignment", p. 56.

6.2.5 Tab Superior Roles

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

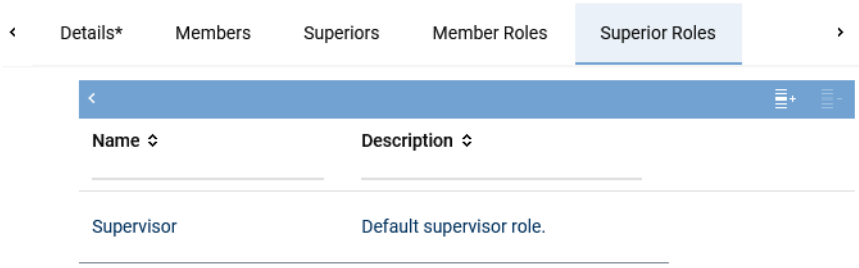

Fig. 97: Organization Structure module - tab Superior Roles

For a description of how to add roles, see chapter "Assign roles", p. 55.

For a description of how to remove roles, see chapter "Delete role assignment", p. 56.

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. 67).
   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*.

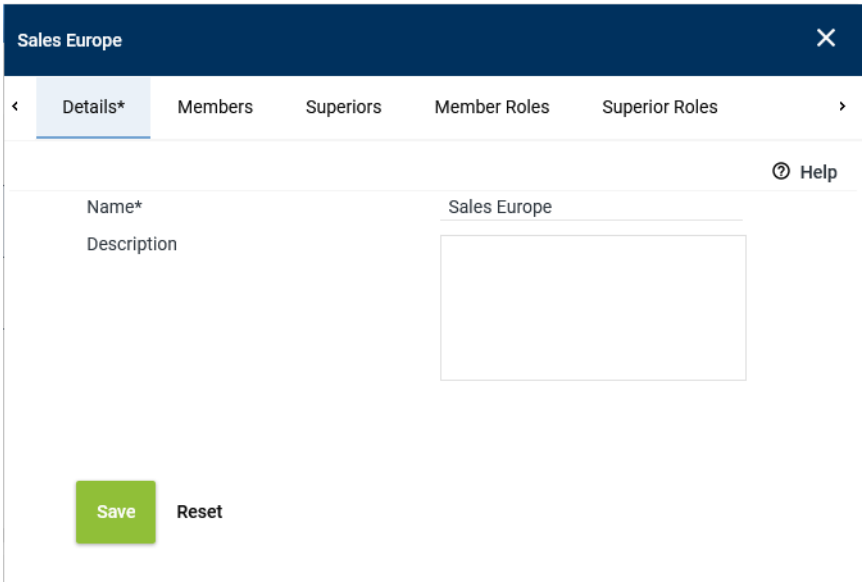

Fig. 98: Save organization unit

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. 67. 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*.

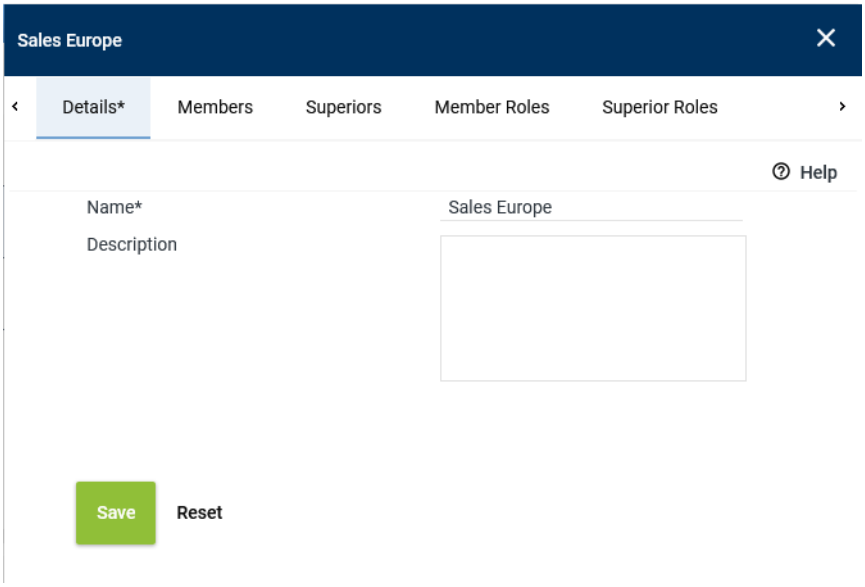

Fig. 99: Save changes

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.

7 Roles module

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. 81). 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.

7.1 Main view

In the main view, all saved roles are displayed.

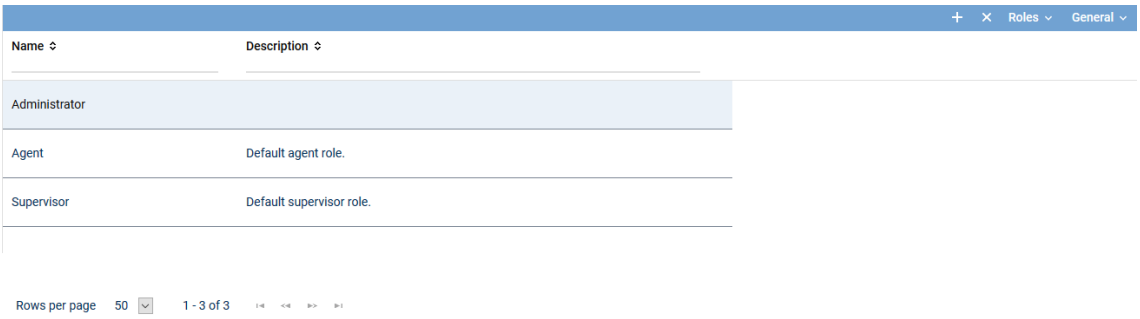

Fig. 100: Roles module - main view

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

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

7.1.1 Toolbar

The toolbar offers the following functions.

Fig. 101: Roles module - toolbar

 	*Search*	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 35. The icon  *(Search)* is displayed whenever the search has been adjusted by means of a filter.
	*Reset search*	Resets all manually entered search criteria. The search is started without manual filter settings.
	*Create*	Creates a new role (see chapter "Create new role", p. 80).
	*Delete*	Deletes the selected role (see chapter "Delete role", p. 82).
Roles	*Duplicate with Employees*	Creates a copy of the selected role (see chapter "Duplicate role", p. 81).
	Duplicate Without Employees	Creates a copy of the selected role (see chapter "Duplicate role", p. 81).
General	*Print*	Prints the table of the main view.
	Adjust table	Opens a window in which you can adjust the following settings for the main view: • Displayed information • Order of the displayed columns • Number of rows per page
	General Help	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.
	Module Help	By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.

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

7.2 Detail view

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

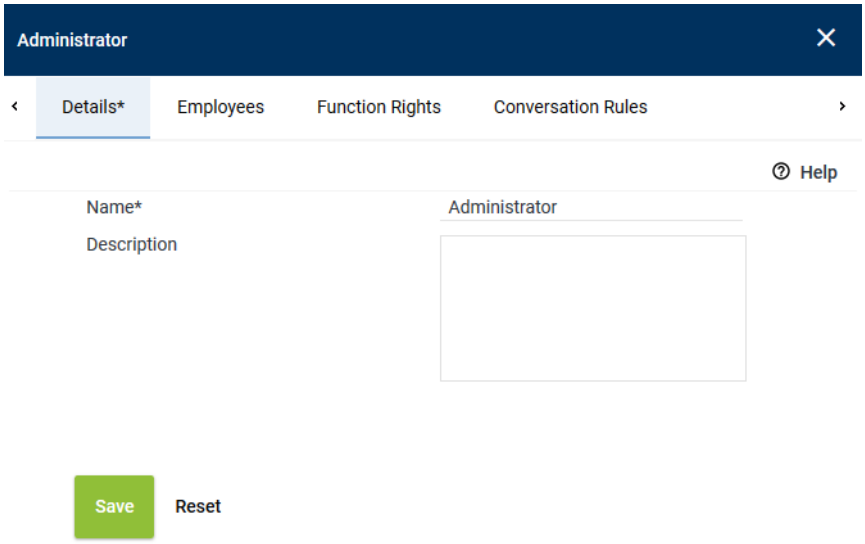

Fig. 102: Roles module - detail view

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. 75.

- *Employees*

  Here, you can display the users who have been assigned the role and edit the user assignment.

  See chapter "Tab Employees", p. 76.

- *Function Rights*

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

  See chapter "Tab Function Rights", p. 77

- *Conversation Rules*

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

  See chapter "Tab Conversation Rules", p. 79.

7.2.1 Tab Details

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

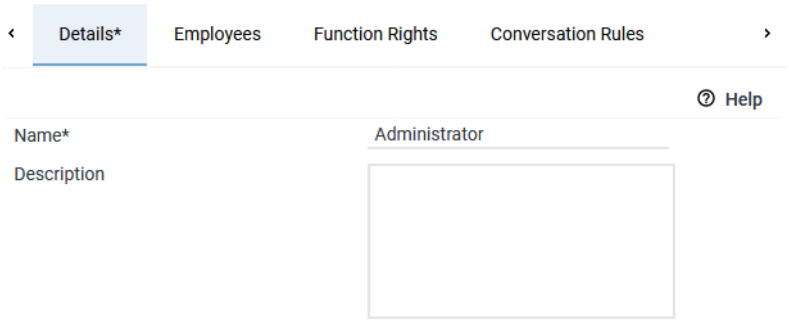

Fig. 103: Roles module - tab Details

Name	Name of the role.
Description	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.

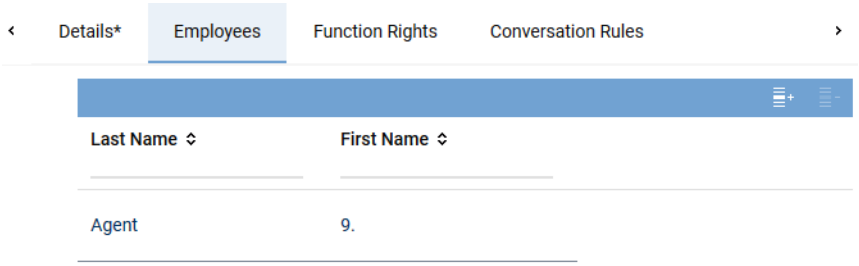

Fig. 104: Roles module - tab Employees

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)*.

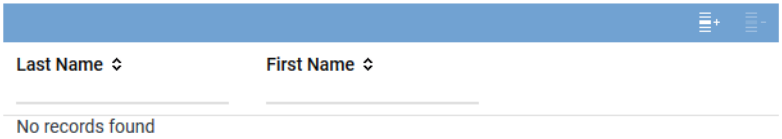

Fig. 105: Assign users

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.

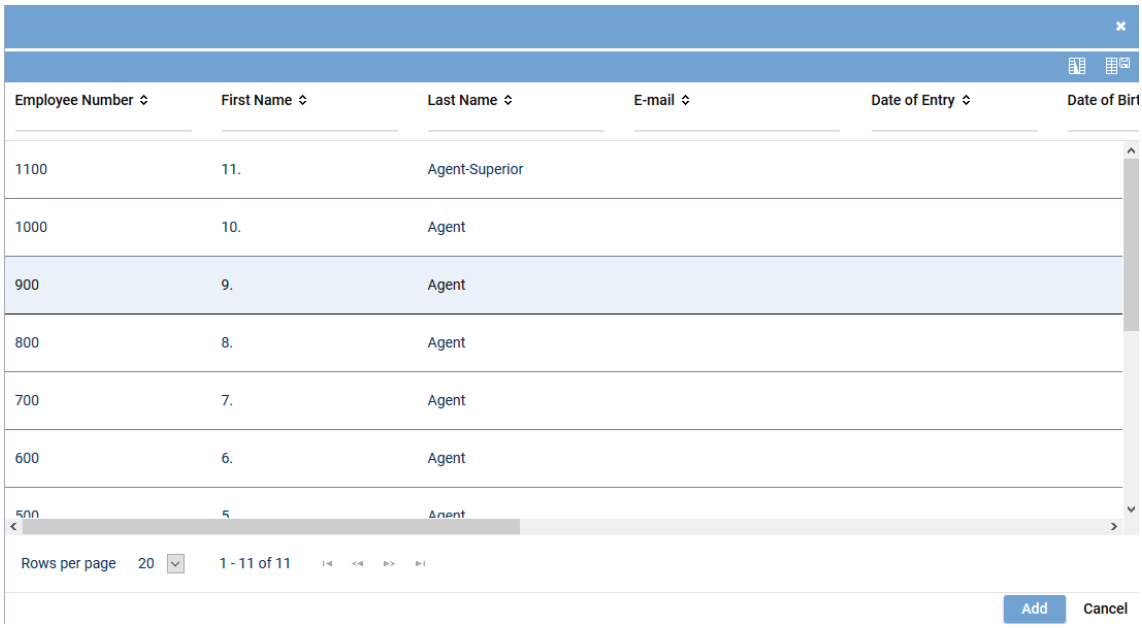

Fig. 106: Add user

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

7.2.2.2 Delete user assignment

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

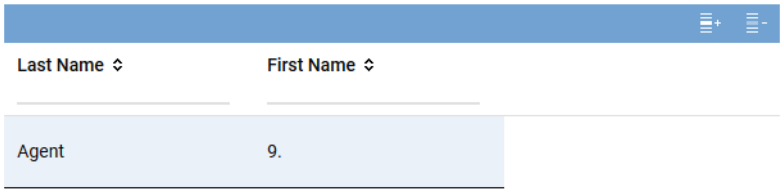

Fig. 107: Delete user assignment

7.2.3 Tab Function Rights

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

Fig. 108: Roles module - tab Function Rights (example)

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

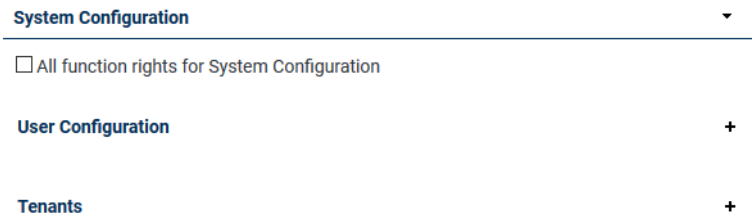

Fig. 109: Function rights - display sections (example)

2. 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.

3. 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.

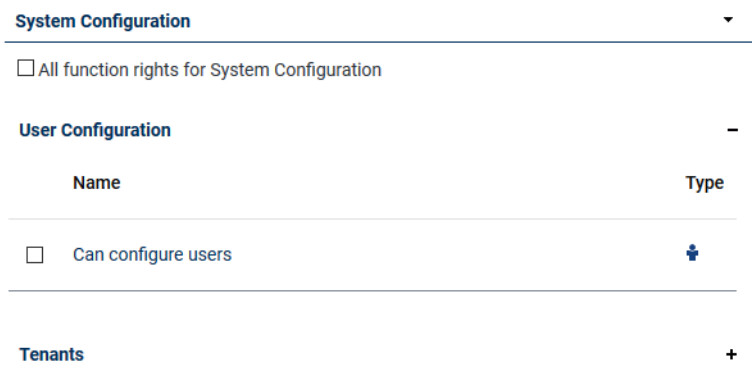

Fig. 110: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. ☑ = individual function right ☐ = 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)

Tab. 4: Function rights

4. 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.
5. 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.

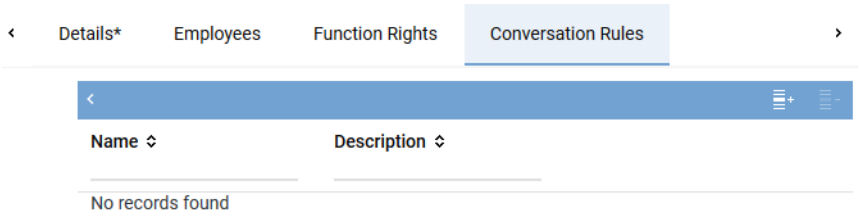

Fig. 111: Roles module - tab Conversation Rules Object Rules

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

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

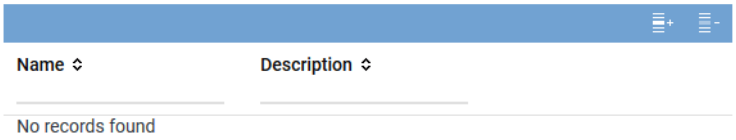

Fig. 112: Assign conversation rule

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.

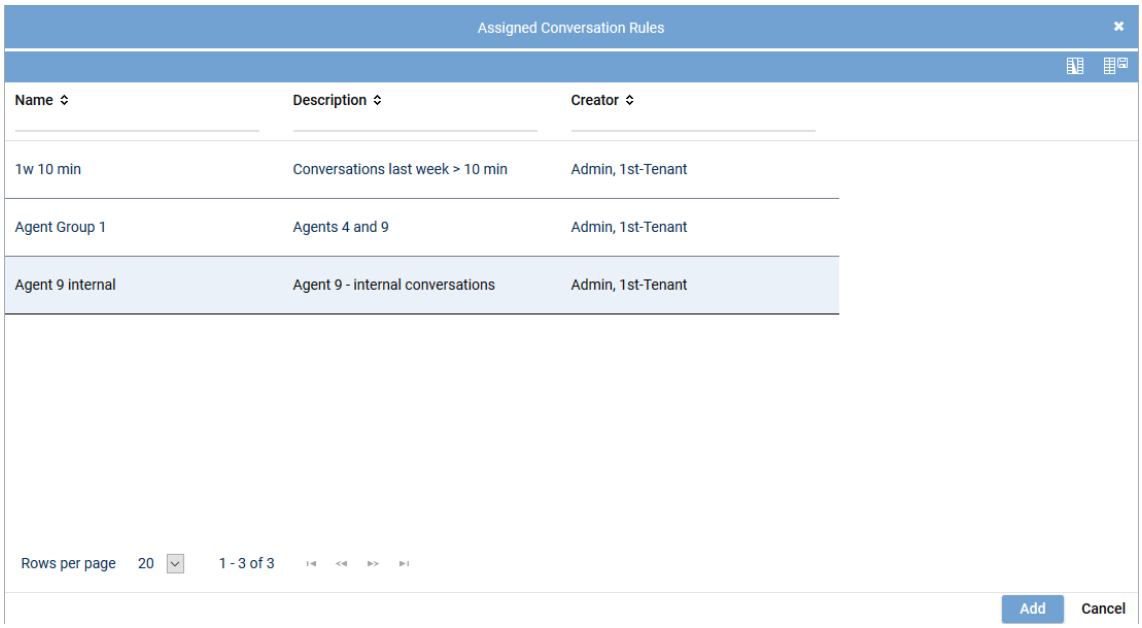

Fig. 113: Add conversation rules

3. 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

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

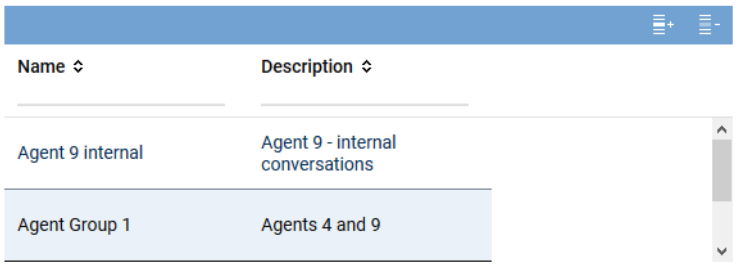

Fig. 114: Delete conversation rule assignment

7.3 Create new role

1. Click on the icon *(Create)* in the toolbar.
2. 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.

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*.

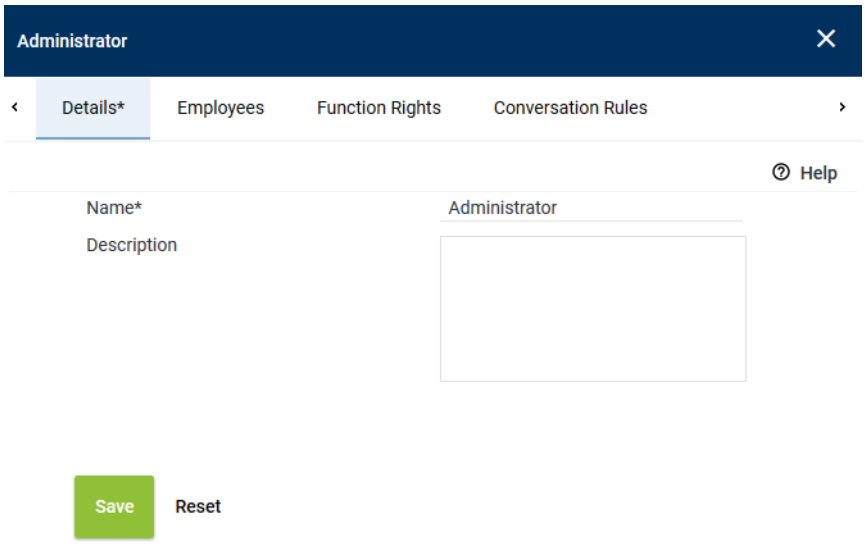

Fig. 115: Save role

7.4 Duplicate role

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

Duplicate with Employees	Creates a copy of the selected role with the assigned employee.
Duplicate Without Employees	Creates a copy of the selected role without the assigned employee.

4. A copy of the role is created in the detail view.
5. Enter a new name for the copied role.
6. Adjust all settings in the tabs of the detail view as described in the respective chapters (see chapter "Detail view", p. 75).
   You can change tabs without buffering without risking the loss of your settings.
7. 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*.

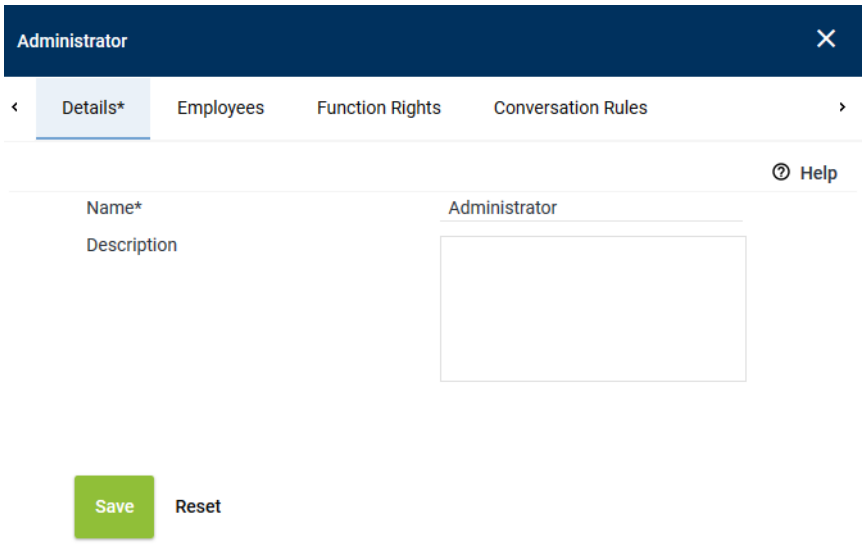

Fig. 116: Save role

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. 75. 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*.

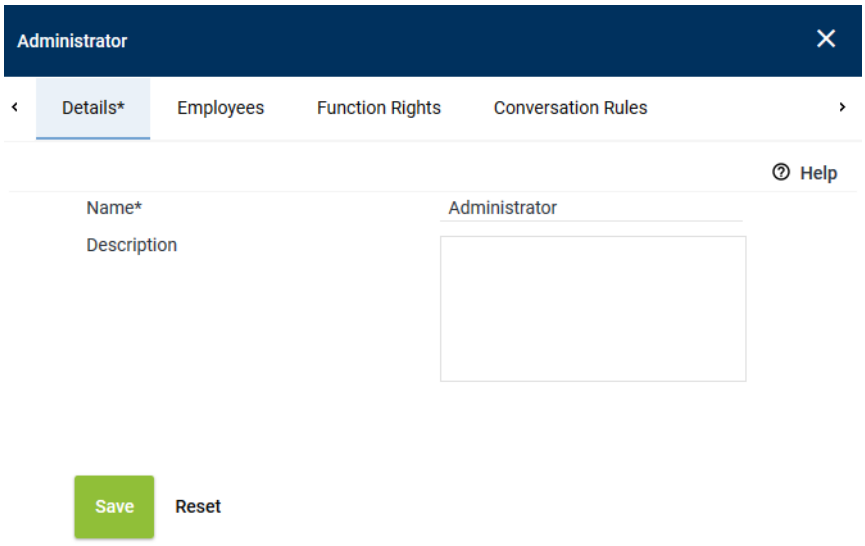

Fig. 117: Save changes

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.

8 Conversation Rules module

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*play* Web	• Conversation module • Participant View module
POWER*play* Pro	• Conversation module • Participant View module
INSPIRATION*neo*	• Sessions module • Calibrations module • Audio Analysis module

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.

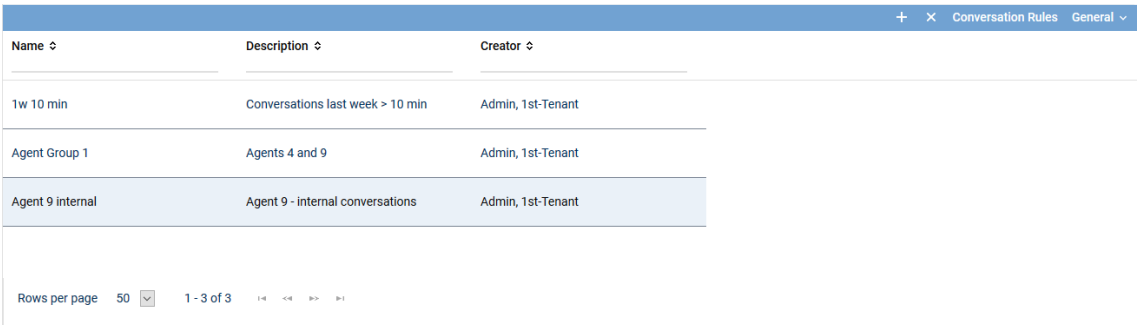

Fig. 118: Conversation Rules module - main view

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

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

8.1.1 Toolbar

The toolbar offers the following functions.

Fig. 119: Conversation Rules module - toolbar

	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 35. The icon *(Search)* is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all manually entered search criteria. The search is started without manual filter settings.
	Create	Creates a new conversation rule (see chapter "Create new conversation rule", p. 94).
	Delete	Deletes the selected conversation rule (see chapter "Delete conversation rule", p. 96).
Conversation Rules		This menu is currently not available
General	*Print*	Prints the table of the main view.
	Adjust table	Opens a window in which you can adjust the following settings for the main view: • Displayed information • Order of the displayed columns • Number of rows per page
	General Help	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.
	Module Help	By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.

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

8.2 Detail view

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

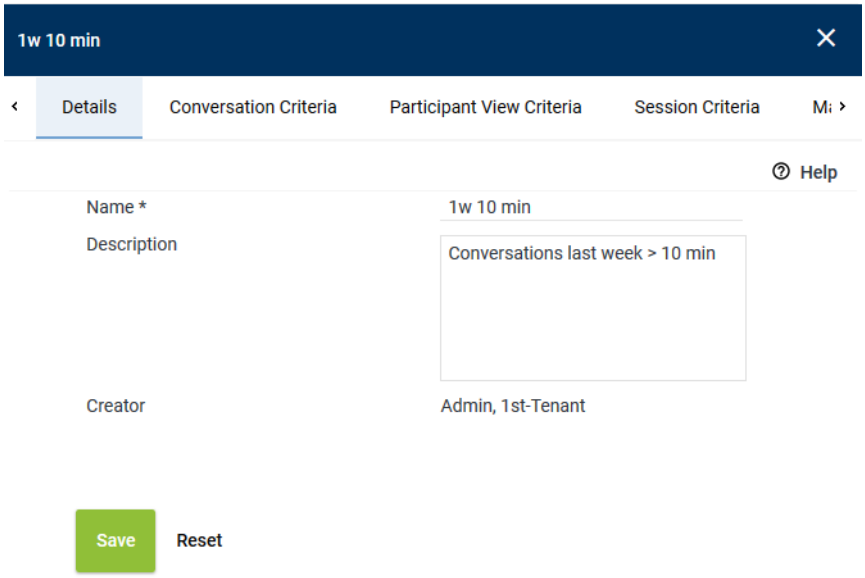

Fig. 120: Conversation Rules module - detail view

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. 87.
- *Conversation Criteria*

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

  See chapter "Tab Conversation Criteria", p. 87.
- *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. 90.
- *Session Criteria*

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

  See chapter "Tab Session Criteria", p. 92.
- *Assignment*

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

  See chapter "Tab Mapping", p. 94.

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.

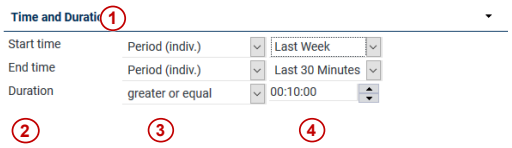

Fig. 121: Filter criteria

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:

inactive	The filter criterion is ignored.
equal	All conversations which exactly meet the entered value are displayed as filter result. Enter the value directly into the entry field via the keyboard.
in	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 + via the keyboard. Consequently, click on the button + to apply the value in the list. To remove a value from the list, click on the icon x on the right of the value.
greater or equal	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.
Period of time	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.

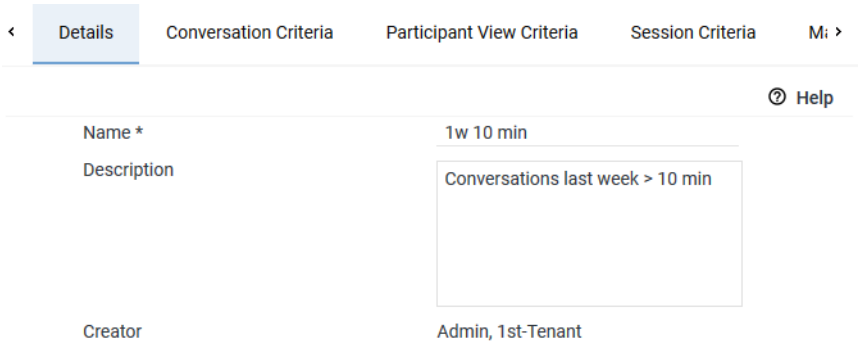

Fig. 122: Conversation Rules module - tab Details

Name	Name of the conversation rule.
Description	Description of the conversation rule.
Creator	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. 86.

Fig. 123: Conversation Rules module - tab Conversation Criteria

Group field Conversation Information

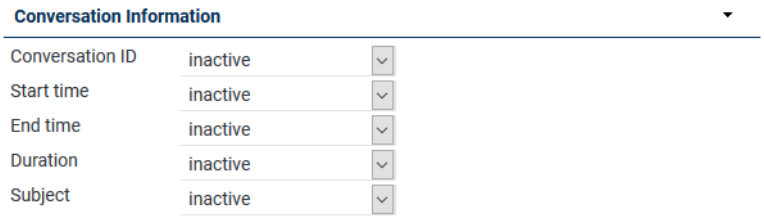

Fig. 124: Conversation Criteria - Conversation Information (example)

Conversation ID	This ID clearly identifies the conversation.
Start time	Period of time when the conversation was started.
End time	Period of time when the conversation was ended.
Duration	Duration of the conversation.
Subject	Subject of the conversation.

Group field Statistics of the Conversation

Fig. 125: Conversation criteria - Statistics of the Conversation (example)

Duration of Ringing Sections	Duration of ringing sections

Duration of Hold Sections	Duration of hold sections
Duration of Connected Sections	Duration of the connected sections
Conversation ID of Callback Request	Conversation ID of callback request

Group field Calling Party Information

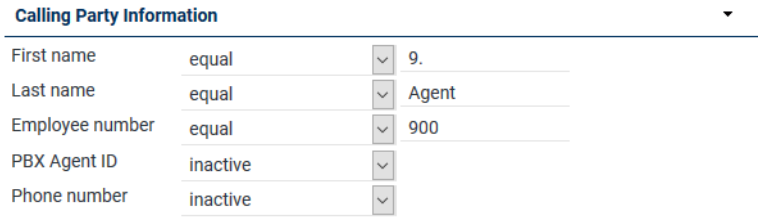

Fig. 126: Conversation Criteria - Calling Party Information (example)

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

First name	First name of the calling party.
Last name	Last name of the calling party.
Employee number	Employee number of the calling party.
PBX Agent ID	ID of the calling agent. This ID has been saved in the PBX and clearly identifies the calling party.
Phone number	Complete phone number of the calling party.

Group field Called Party Information

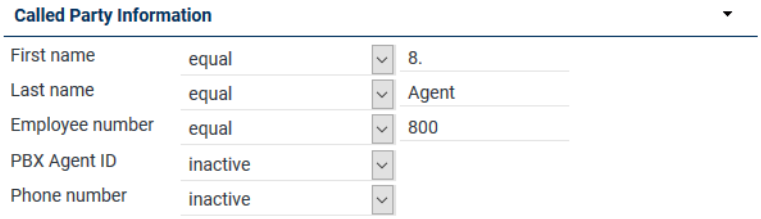

Fig. 127: Conversation Criteria - Called Party Information (example)

First name	First name of the called party.
Last name	Last name of the called party.
Employee number	Employee number of the called party.
PBX Agent ID	ID of the called agent. This ID has been saved in the PBX and clearly identifies the called party.
Phone number	Complete phone number of the called party.

Group field 1st-Connected Participant Information

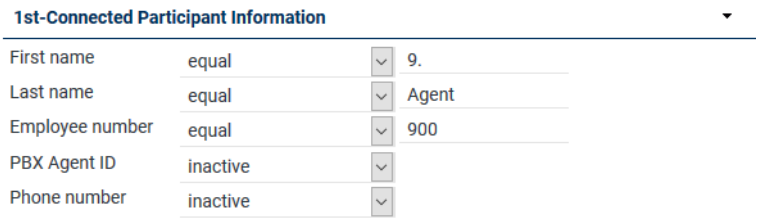

Fig. 128: Conversation Criteria - 1st-Connected Participant Information (example)

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

Group field Additional Data

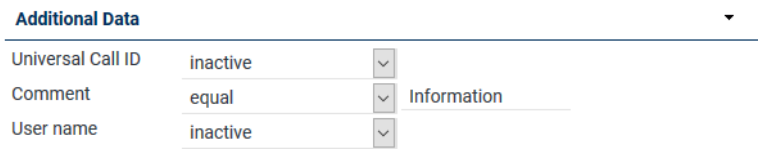

Fig. 129: Conversation Criteria - Additional Data (example)

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

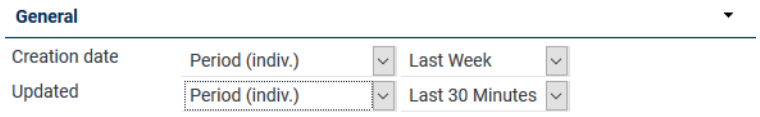

Fig. 130: Conversation Criteria - General (example)

Creation date	Date on which the conversation was saved in the system.
Updated	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. 86.

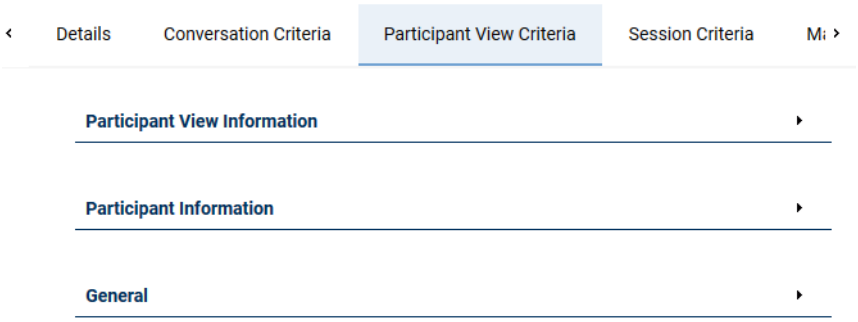

Fig. 131: Conversation Rules module - tab Participant View Criteria

Group field Conversation Information

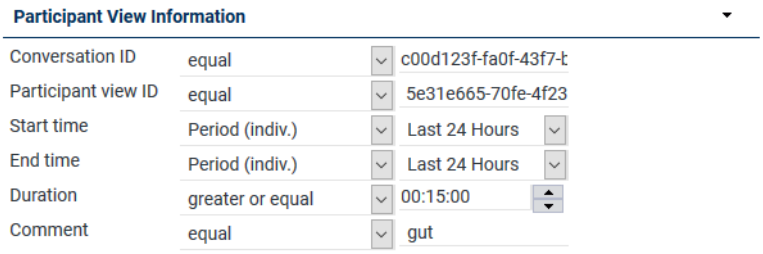

Fig. 132: Participant View Criteria - Conversation Information

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

Group field Participant Information

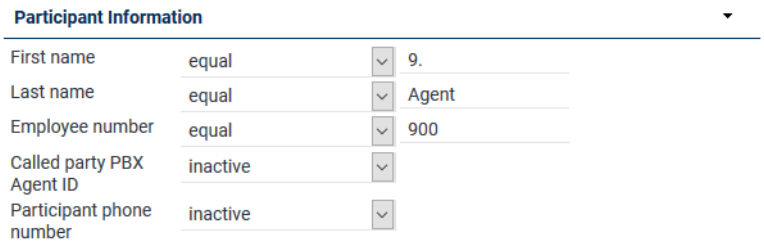

Fig. 133: Participant View Criteria - Participant Information (example)

First name	First name of any participant.
Last name	Last name of any participant.
Employee number	Employee number of any participant.

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

Group field General

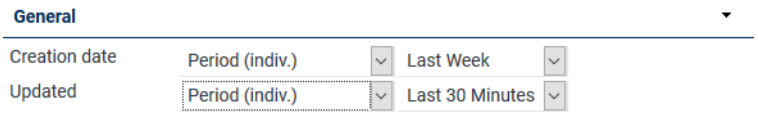

Fig. 134: Participant View Criteria - General (example)

Creation date	Date on which the participant view of the conversation was saved in the system.
Updated	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. 86.

Fig. 135: Conversation Rules module - tab Session Criteria

Group field Agent Information

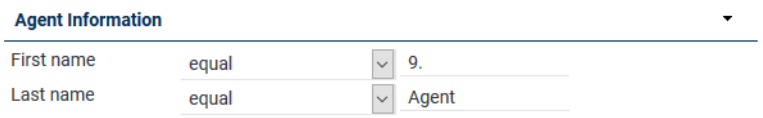

Fig. 136: Session Criteria - Agent Information (example)

First name	First name of any agent who has participated in the session.
Last name	Last name of any agent who has participated in the session.

Group field Time and Duration

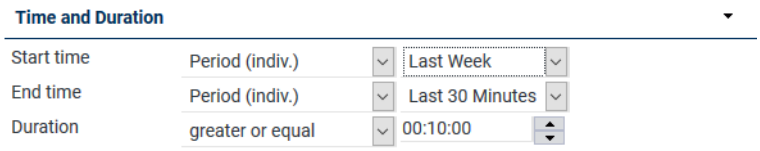

Fig. 137: Session Criteria - Time and Duration (example)

Start time	Period of time when the session was started.
End time	Period of time when the session was ended.
Duration	Session duration.

Group field CTI Information

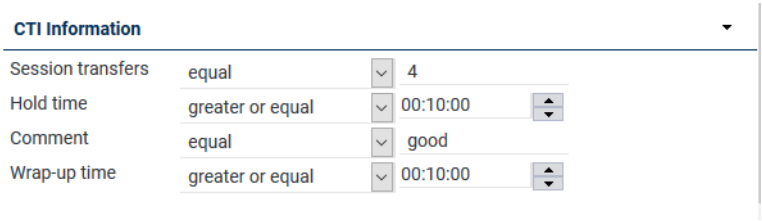

Fig. 138: Session Criteria - CTI Information (example)

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

Group field Categories

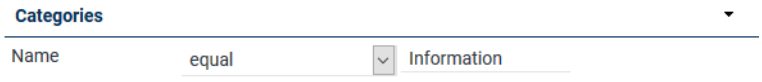

Fig. 139: Session Criteria - Categories (example)

Name	Name of the category that the session belongs to.

Group field General

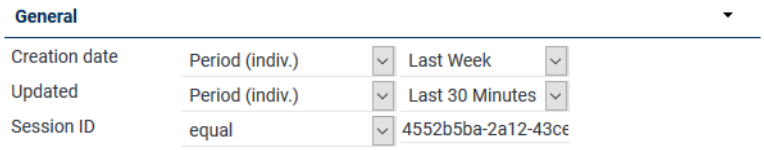

Fig. 140: Session Criteria - General (example)

Creation date	Date on which the session was saved in the system.
Updated	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

Fig. 141: Session Criteria - Organization Units (example)

Of the agent	Organization unit of the agent who has participated in the session.
Of the calling party	Organization unit of the calling party who has participated in the session.
Of the called party	Organization unit of the called party who has participated in the session.
Of the 1st-connected	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.

Fig. 142: 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:

Create New	A completely new conversation rule is created.
Create Clone	*This function is currently unavailable.*

3. Adjust the respective settings in the tabs of the detail view (see chapter "Detail view", p. 85).
   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*.

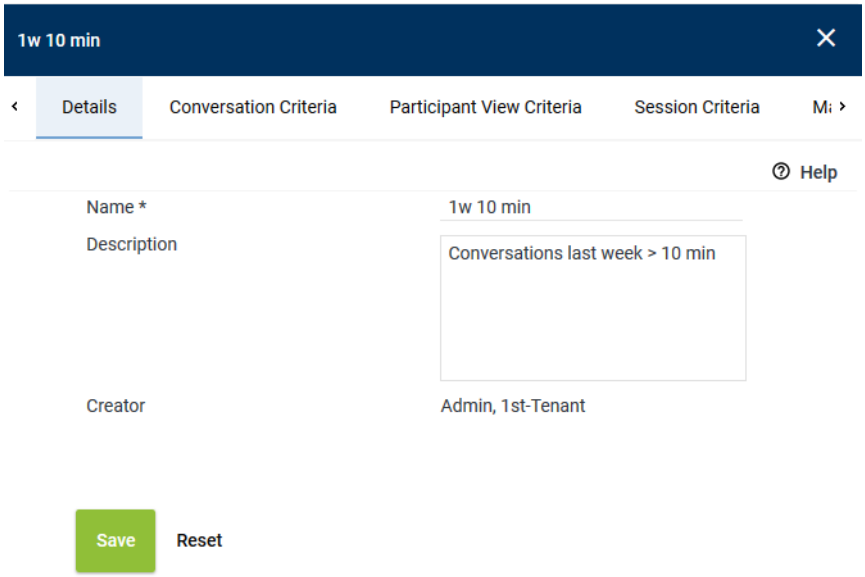

Fig. 143: Save conversation rule

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.

1. In the main view, select the conversation rule you would like to edit.
2. Adjust the respective settings in the tabs of the detail view (see chapter "Detail view", p. 85).
   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*.

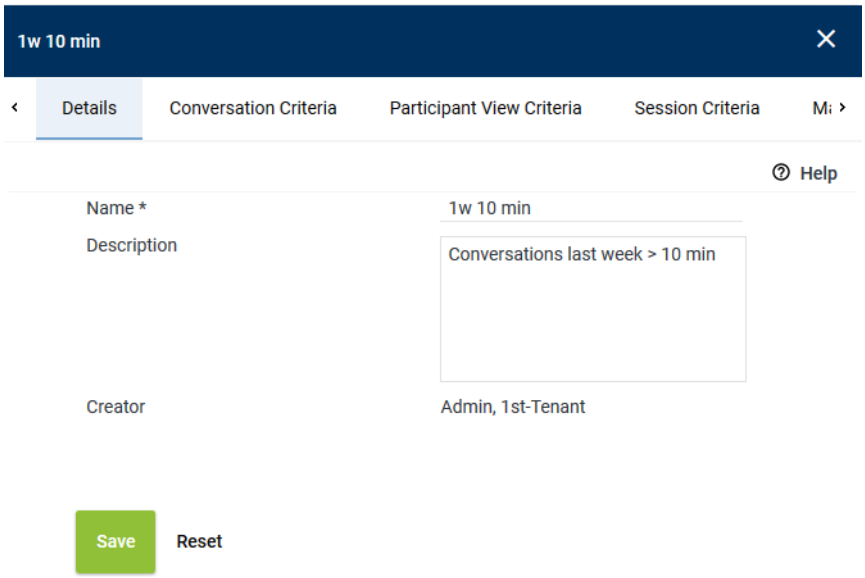

Fig. 144: Save changes

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*neo*

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

  See chapter "Create agent", p. 97.

- **Supervisor** (only for tenants)

  Supervisors have the following function rights at their disposal:

  – All modules and functions in the application INSPIRATION*neo*

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

  See chapter "Create supervisor", p. 98.

- **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. 98.

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

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

  By means of the application CLIENT*command*, 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*neo*.

  See chapter "Create Coaching Advisor", p. 98.

- **Superuser**

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

  See chapter "Create superuser", p. 99.

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. 41.
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. 55.
   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. 56.

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

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. 56.

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. 55.
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. 50.

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. 70.
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. 61.

9.4 Create Coaching Advisor

✓ The user has the right *Has access to agents and their data*, see chapter "Tab Settings", p. 50.

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*.

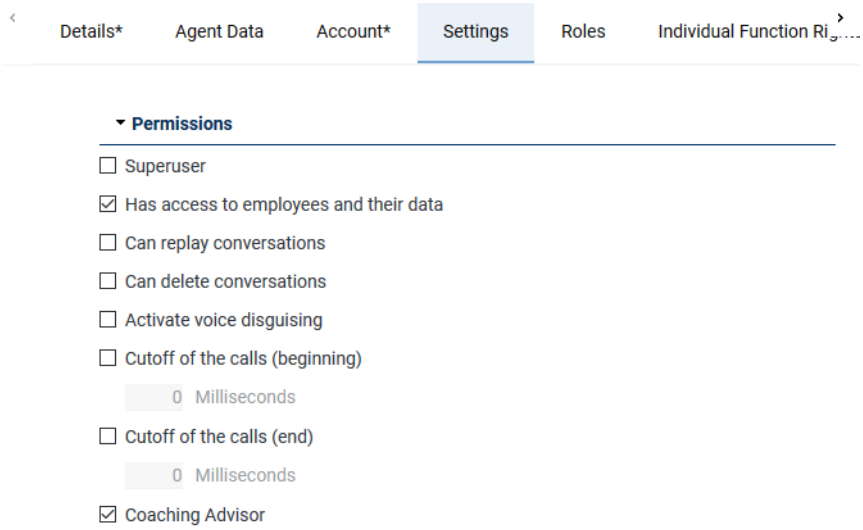

Fig. 145: Create Coaching Advisor

6. Click on the tab *Individual Function Rights*.
7. Open the group field INSPIRATION*neo*.
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*.

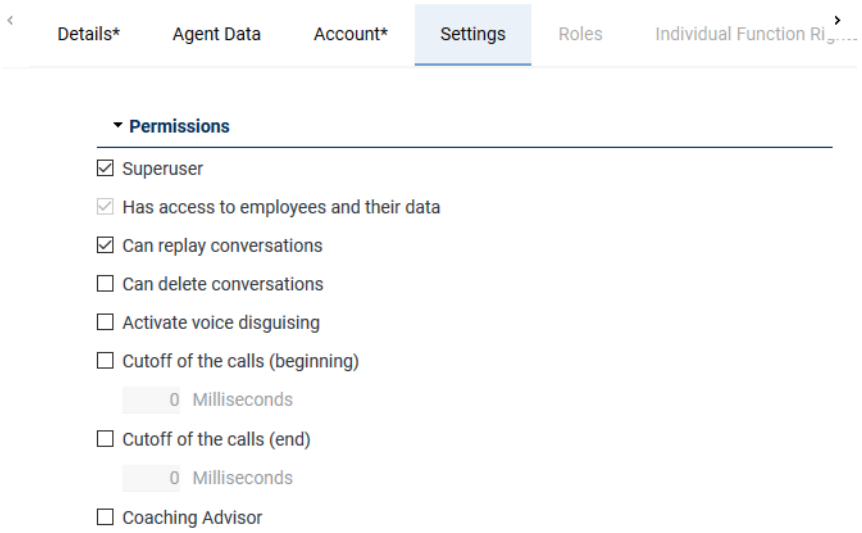

Fig. 146: Create superuser

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

List of tables

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, former name Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

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.