

System Configuration

User management



Administration manual

for tenants

8/9/2022

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

Copyright © 2022 ASC Technologies AG. All rights reserved.

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

Contents

1	General information.....	6
2	Introduction.....	7
3	LDAP.....	9
3.1	Install certificate	9
3.2	Troubleshooting	10
4	Tenants module	11
4.1	Main view.....	11
4.1.1	Toolbar.....	11
4.2	Detail view	11
4.2.1	Tab Details.....	12
4.2.1.1	Add time zone.....	14
4.2.1.2	Group field System Availability	15
4.2.1.3	Group field Address	16
4.2.1.4	Group field Contact Person	17
4.2.2	Tab Passwords.....	17
4.2.2.1	Edit entry.....	22
4.2.3	Tab General Settings.....	23
4.2.3.1	Group field Inactivity	23
4.2.3.2	Group field SMTP Account	24
4.2.3.3	Group field Login Settings	25
4.2.3.4	Group field Miscellaneous Settings	26
4.2.3.5	Group field Random Search of Sessions.....	27
4.2.3.6	Group field Terms of Use.....	27
4.2.3.7	Group field INSPIRATIONneo Settings	27
4.2.4	Tab Key Management	27
4.2.5	Tab LDAP Connection Data	28
4.2.5.1	Edit LDAP connection data.....	29
4.2.6	Tab Web Service	30
5	Employees module	33
5.1	Main view.....	33
5.1.1	Toolbar.....	34
5.1.1.1	Show summary	35
5.1.1.2	Show locked employees	36
5.1.1.3	Make employee visible or not visible	36
5.1.1.4	Search	36
5.2	Detail view	37
5.2.1	Tab Details.....	38
5.2.1.1	Group field Employee Information	38
5.2.1.2	Group field Address	42

5.2.2	Tab Agent Data.....	42
5.2.2.1	Group field Telephony	43
5.2.2.2	Group field Chat.....	46
5.2.2.3	Group field Miscellaneous Settings	47
5.2.3	Tab Account.....	48
5.2.3.1	Authentication via LDAP	50
5.2.3.2	Assign combination user.....	50
5.2.3.3	Delete combination user assignment.....	51
5.2.3.4	Two-factor authentication	52
5.2.3.5	Authentication via PIN	52
5.2.4	Tab Settings.....	53
5.2.4.1	Group field Permissions.....	53
5.2.4.2	Group field Logging Settings	55
5.2.4.3	Group field Settings for Session Release	56
5.2.5	Tab Roles	58
5.2.5.1	Assign roles	58
5.2.5.2	Delete role assignment.....	59
5.2.6	Tab Individual Function Rights	59
5.2.7	Tab Conversation Rules	62
5.2.7.1	Assign conversation rules.....	63
5.2.7.2	Delete conversation rule assignment.....	64
5.2.8	Tab Organization Units.....	64
5.2.8.1	Assign organization units.....	65
5.2.8.2	Delete organization unit assignment.....	66
5.3	Create new employee.....	66
5.4	Edit employee	67
5.5	Delete employee	67
5.6	Create new employee with OAuth login.....	67
6	Organization Structure module	69
6.1	Main view	69
6.1.1	Toolbar.....	69
6.2	Detail view	70
6.2.1	Tab Details.....	71
6.2.2	Tab Members.....	71
6.2.2.1	Assign members	71
6.2.2.2	Delete member assignment.....	72
6.2.3	Tab Superiors	72
6.2.3.1	Assign superiors	73
6.2.3.2	Delete superior assignment	73
6.2.4	Tab Member Roles	73
6.2.5	Tab Superior Roles.....	74
6.3	Create new organization unit	74

6.4	Edit organization unit	75
6.5	Delete organization unit	75
7	Roles module	76
7.1	Main view	76
7.1.1	Toolbar	77
7.2	Detail view	78
7.2.1	Tab Details	78
7.2.2	Tab Employees	79
7.2.2.1	Assign users	79
7.2.2.2	Delete user assignment	80
7.2.3	Tab Function Rights	80
7.2.4	Tab Conversation Rules	82
7.2.4.1	Assign conversation rules	82
7.2.4.2	Delete conversation rule assignment	83
7.3	Create new role	83
7.4	Duplicate role	84
7.5	Edit role	85
7.6	Delete role	85
8	Conversation Rules module	86
8.1	Main view	87
8.1.1	Toolbar	87
8.2	Detail view	88
8.2.1	Define filter criteria	89
8.2.2	Tab Details	90
8.2.3	Tab Conversation Criteria	93
8.2.4	Tab Participant View Criteria	96
8.2.5	Tab Session Criteria	98
8.2.6	Tab Mapping	100
8.3	Create new conversation rule	100
8.4	Edit conversation rule	101
8.5	Delete conversation rule	102
9	Predefined function packages	103
9.1	Create agent	103
9.2	Create supervisor	104
9.3	Create superior	104
9.4	Create Coaching Advisor	104
9.5	Create superuser	105
	List of figures	107
	List of tables	111
	Glossary	112

General information

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

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

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

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

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

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

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

2 Introduction

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

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

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

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

- Tenants module

In the Tenants module, you can administrate your own tenant data.

See [chapter "Tenants module", p. 11.](#)

- Employees module

In the Employees module, you can create users, administrate their data, and assign function rights.

See [chapter "Employees module", p. 33.](#)

- 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. 76.](#)

- 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. 69.](#)

- 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. 86.](#)



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.

Preliminary - For internal use only

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. 28.
- Always activate **LDAP** authentication.
See chapter "Group field Login Settings", p. 25.
- Activate **LDAP** authentication for individual users.
See chapter "Authentication via LDAP", p. 50.



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.

Preliminary - For internal use only

4 Tenants module

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

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

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

4.1 Main view

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

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

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

Fig. 1: Tenants module - main view

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

4.1.1 Toolbar

The toolbar offers the following functions.

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

Fig. 2: Tenants module - toolbar

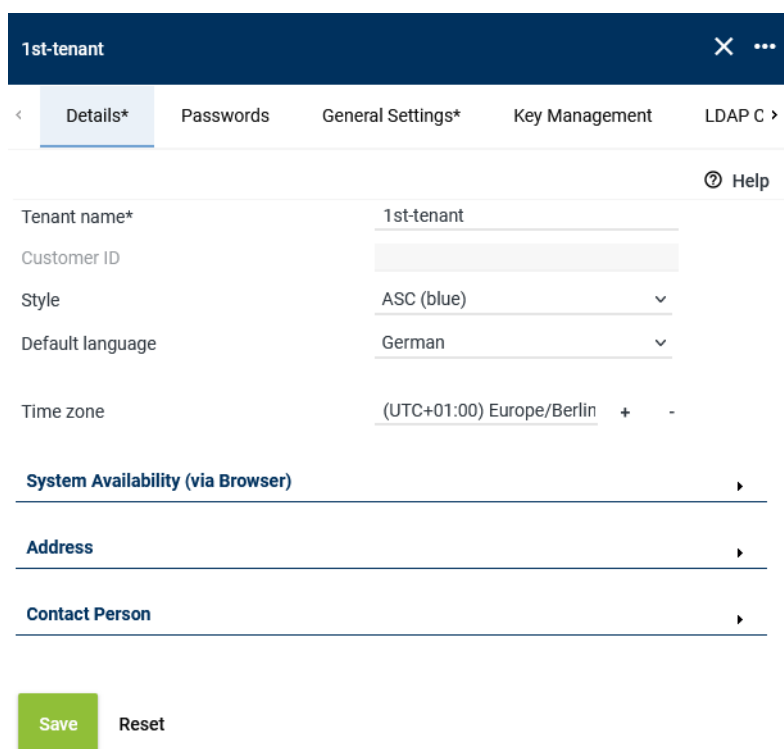
<i>Tenants</i>	This menu is currently not available	
<i>General</i>	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module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



For detailed 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.



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

Tenant name*	1st-tenant
Customer ID	
Style	ASC (blue) ▼
Default language	German ▼
Time zone	(UTC+01:00) Europe/Berlin + -

Below the form, there are three expandable sections: 'System Availability (via Browser)', 'Address', and 'Contact Person'. At the bottom, there are 'Save' and 'Reset' buttons.

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. 23.](#)
- **Key management**
Here, you can define the method which is supposed to be used to encrypt the conversations.
See [chapter "Tab Key Management", p. 27.](#)
- **LDAP Connection Data**
Here, you can configure [LDAP](#) connections.
See [chapter "Tab LDAP Connection Data", p. 28.](#)
- **Web Service**
Here, you can configure the usage of the Web Service.
See [chapter "Tab Web Service", p. 30.](#)

4.2.1 Tab Details

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

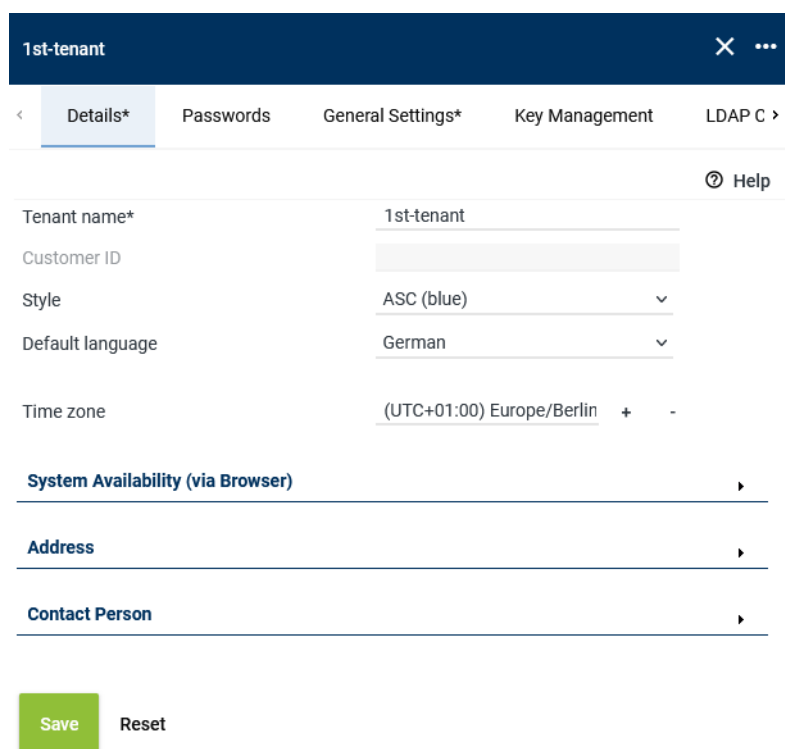




Fig. 4: Tenants module - tab Details

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


<i>Tenant name</i>	Your name as tenant.
<i>Customer ID</i>	<p>Displays the customer ID that you have been assigned by your system provider or reseller.</p> <p>NOTICE! The assignment of customer IDs is subject to the hierarchy in the system: The customer ID that a system provider assigns to a reseller or to a tenant cannot be changed or deleted by this reseller or tenant.</p>
<i>Style</i>	<p>Layout in which the tenant sees the user interface of the system.</p> <p>Select one of the available layouts from the drop-down list.</p>
<i>Default language</i>	<p>Language in which the user interface of the system is displayed in your environment.</p> <p>Select the language from the drop-down list.</p>
<i>Time zone</i>	<p>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 employee separately. The configuration in the Employees module has a higher priority.</p> <p>To select the time zone, click on the button . See chapter "Add time zone", p. 14.</p> <p>To delete the selection, click on the button .</p> <p>NOTICE! If no selection is made, the time zone of the higher-level tenant or reseller or of the system provider in the last instance is used. If the system provider has not configured a time zone, <i>UNKNOWN</i> is displayed.</p>

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


- Click on the button  on the right of the entry field.

Fig. 5: Add time zone

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

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

Example:

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

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

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

- Select a time zone from the list.



Time Difference ↕	Continent/Region ↕
UTC-12:00	Etc/GMT+12
UTC-11:00	Pacific/Pago_Pago
UTC-11:00	Pacific/Samoa
UTC-11:00	Pacific/Niue
UTC-11:00	US/Samoa
UTC-11:00	Etc/GMT+11
UTC-11:00	Pacific/Midway

Rows per page 20 1 - 20 of 616

Add Cancel

Fig. 7: Add time zone

- 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

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

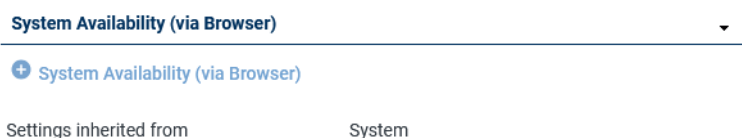


System Availability (via Browser)

+ System Availability (via Browser)

Fig. 8: System Availability (via Browser)

- 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*.



System Availability (via Browser)

+ System Availability (via Browser)

Settings inherited from System

Fig. 9: System Availability (via Browser)

- 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.
- To configure system availability (via browser), proceed as follows:
- In the title bar of the group field, click on the button + *System Availability (via Browser)*.
- Enter the addresses you would like to use.

System Availability (via Browser) ▼

● System Availability (via Browser)

Allowed IP address ranges _____

Internal IP address / Internal port _____ : 443

DNS name _____

External IP address / External port _____ :

External DNS name _____

Fig. 10: Configure system availability

Allowed IP 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*.

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

4.2.1.3 Group field Address

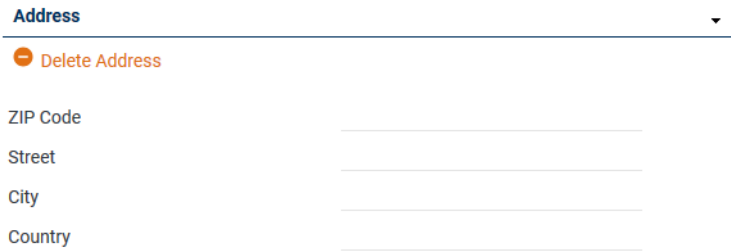
- If you would like to add a contact address, open the group field Address.

Address ▼

● Add Address

Fig. 11: Add address

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



Address ▼

✖ Delete Address

ZIP Code _____

Street _____

City _____

Country _____

Fig. 12: Add address

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

4.2.1.4 Group field Contact Person

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

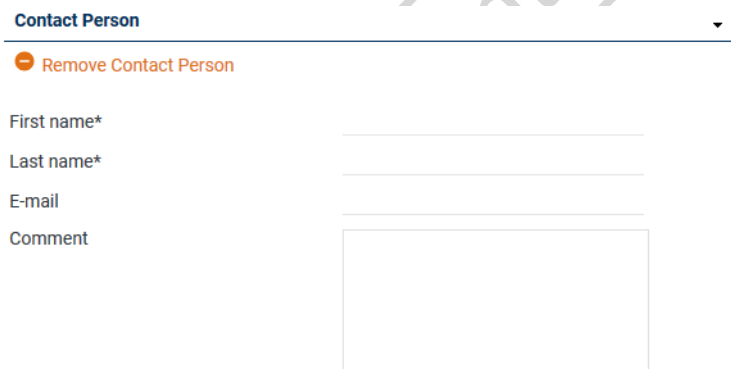


Contact Person ▼

+ Add Contact Person

Fig. 13: Add contact person

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



Contact Person ▼

✖ Remove Contact Person

First name* _____

Last name* _____

E-mail _____

Comment

Fig. 14: Add contact person



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

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

4.2.2 Tab Passwords

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

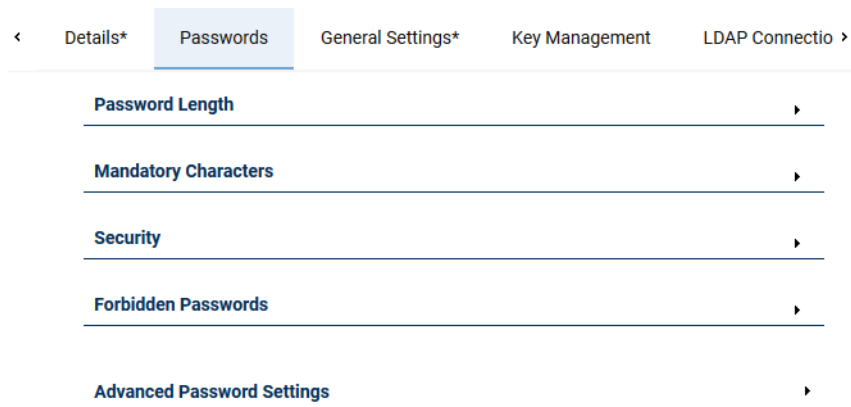


Fig. 15: Tenants module - tab Passwords

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

- In the field *Maximum length*, enter the maximum number of characters mandatory for the password.

NOTICE! *Maximum length* must be \geq *minimum length*.

- 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

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

Mandatory Characters


 Remove mandatory characters

Max. character repetition (max. 3 characters)	<u>256</u>
Min. number of	
Letters (max. 3 characters)	<u>2</u>
Digits (max. 3 characters)	<u>2</u>
Special characters (max. 3 characters)	<u>1</u>
Lower-case letters (max. 3 characters)	<u>0</u>
Upper-case letters (max. 3 characters)	<u>0</u>


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.	
<i>Min. number of lower-case letters</i>	Enter how many lower-case letters a password must contain at least.	
<i>Min. number of upper-case letters</i>	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.

Security ▼

● Remove security

Validity
(max. 3 characters) Day(s)

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

Password history

☒ Password history in days
 Day(s)

☐ Extent of password history

Possible failed login attempts
(max. 3 characters)


Deny personal data ☐

Fig. 18: Configure password security



<i>Validity</i>	Enter for how long a password is supposed to remain valid. <i>Validity = 0: Passwords never expire</i>
<i>Point in time when information about the imminent expiration of the password is sent</i>	Enter how many days before the expiration of the password users are to be reminded that they will have to change their password soon. <i>Point in time ... = 0: User does not receive any information</i> NOTICE! The value for the point in time to send information must be smaller than the value for the validity of the password.
<i>Password history</i>	Enter for how long the password history is supposed to be saved. Select one of the following options: <ul style="list-style-type: none"> • <i>Password history in days</i> For this option, enter for how long the passwords are supposed to be saved in the password history. • <i>Extent of password history</i> 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.
<i>Possible failed login attempts</i>	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.
<i>Deny personal data</i>	Define whether users are allowed to use private data from their profiles for the password (e. g. name, user name, date of birth). <input checked="" type="checkbox"/> = Personal data is not allowed. <input type="checkbox"/> = Personal data is allowed.

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

Group field Forbidden Passwords


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

Forbidden Passwords

Server	
System	

Add **Delete**


Fig. 19: Define forbidden passwords

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.

Advanced Password Settings

Password rules can be ignored ☐

Fig. 20: Define advanced password settings


Password rules can be ignored





☒ = Password rules can be ignored.

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

☐ = Password rules cannot be ignored.



4.2.2.1 Edit entry

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

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

Add Delete

Fig. 21: Edit entry in the list

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

4.2.3 Tab General Settings

Here, you can change several general settings.

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

Inactivity ▶

SMTP Account ▶

Login Settings ▶

Miscellaneous Settings ▶

Random Search of Sessions ▶

Terms of Use ▶

INSPIRATIONneo Settings ▶

Fig. 22: Tenants module - tab General Settings

4.2.3.1 Group field Inactivity

Inactivity ▼

Notify before locking* 5 Day(s)
(max. 3 characters)

User will be deactivated* 0 Day(s)
(max. 3 characters)

Session timeout


☒ Session timeout 30 Minute(s)
☐ Session never expires

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.
<i>User will be deactivated</i>	<p>Select after how many days of inactivity the account of the user is locked.</p> <p><i>User will be deactivated</i> = 0: User is not deactivated.</p>
<i>Session timeout</i>	<p>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:</p> <ul style="list-style-type: none"> • <i>Session timeout</i> This option activates the session timeout. Enter a value between 5 and 1440. • <i>Session never expires</i> This option deactivates the session timeout and enables endless sessions. <p>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.</p>



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

4.2.3.2

Group field SMTP Account

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

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



Fig. 24: SMTP account

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

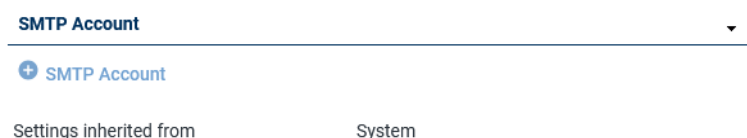



Fig. 25: SMTP account

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

5. In the title bar of the group field, click on the button  *SMTP Account*.

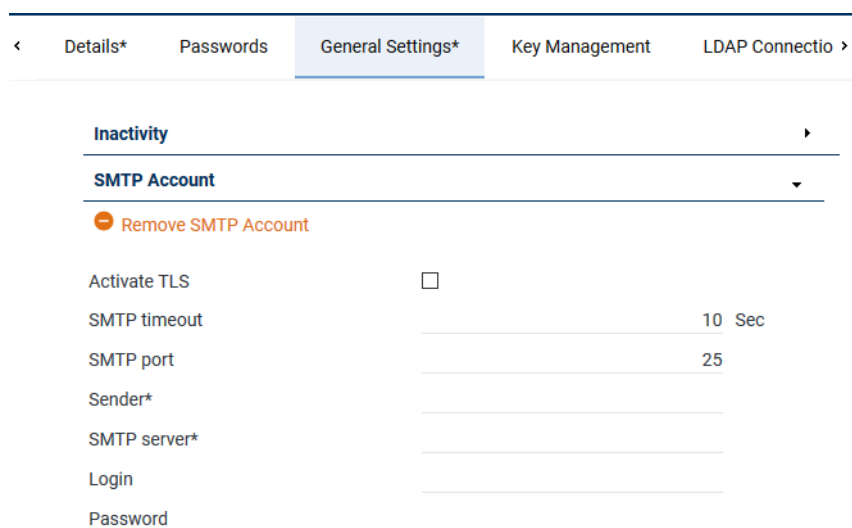




Fig. 26: Add SMTP account



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

6. Complete the following fields:

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

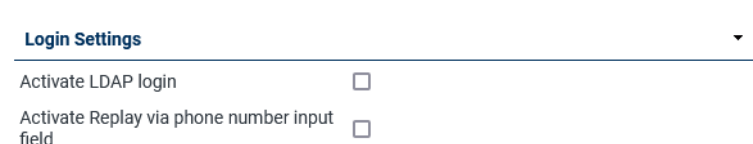


Fig. 27: Login Settings

<i>Activate LDAP login</i>	<p>Activate or deactivate the authentication via LDAP.</p> <p><input checked="" type="checkbox"/> = LDAP login has been activated. <input type="checkbox"/> = LDAP login has not been activated.</p>
<i>Activate Replay via telephone number input field</i>	<p>Activate or deactivate the entry field to enter the replay via phone number when logging in to POWERplay Web.</p> <p><input checked="" type="checkbox"/> = Field to enter replay via phone number is displayed on the login screen of POWERplay Web. <input type="checkbox"/> = Field to enter replay via phone number is not displayed on the login screen of POWERplay Web.</p>



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. 28).

4.2.3.4

Group field Miscellaneous Settings

Miscellaneous Settings

- ☒ Display last login date
- ☒ Display logout warning
- ☒ Resource string view
- ☐ Failed login
- ☒ Activate digital signature check

Fig. 28: Configure miscellaneous settings

<i>Display last login date</i>	<p>Select whether you would like to have the date of the last login displayed in all applications</p> <p><input checked="" type="checkbox"/> = Display has been activated. <input type="checkbox"/> = Display has not been activated.</p>
<i>Display logout warning</i>	<p>Select whether you would like to display a logout warning in all applications.</p> <p><input checked="" type="checkbox"/> = Display has been activated. <input type="checkbox"/> = Display has not been activated.</p>
<i>Resource string view</i>	<p>Select whether you would like to display the button to activate the resource string view in all applications.</p> <p><input checked="" type="checkbox"/> = Display has been activated. <input type="checkbox"/> = Display has not been activated.</p>
<i>Failed login</i>	<p>Select whether you would like to display the information about a failed login in all applications.</p> <p><input checked="" type="checkbox"/> = Display has been activated. <input type="checkbox"/> = Display has not been activated.</p>
<i>Activate digital signature check</i>	<p>Select whether you would like to compare checksums for new recordings or imports to display a digital signature in the application POWERplay Web.</p> <p><input checked="" type="checkbox"/> = Check has been activated. <input type="checkbox"/> = Check has not been activated.</p>

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

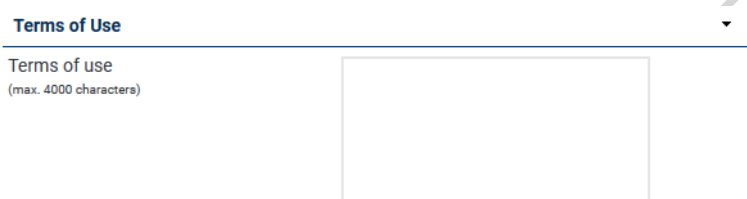


Fig. 30: Configure terms of use

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.

4.2.3.7 Group field INSPIRATIONneo Settings



Fig. 31: INSPIRATIONneo Settings (example)

Number of evaluations to be considered for risk value Enter how many evaluations are supposed to be taken into account when calculating the risk value of an agent.

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.

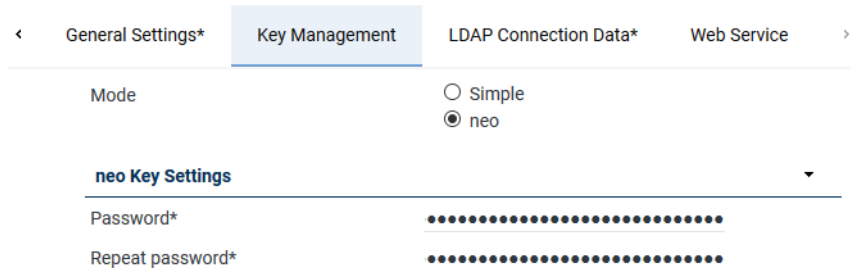


Fig. 32: Tenants module - tab Key Management

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.



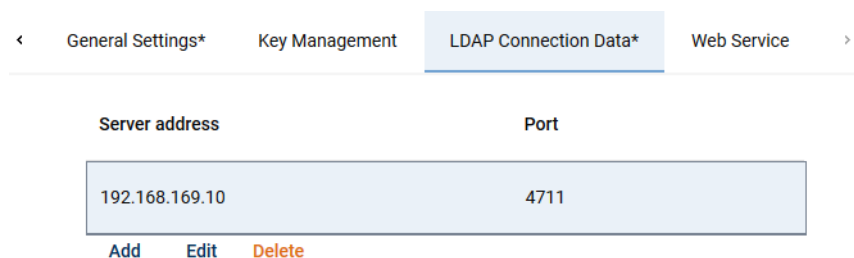
For more information about key management refer to the administration manual for system providers *Encryption of recordings*.

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. 25](#)).



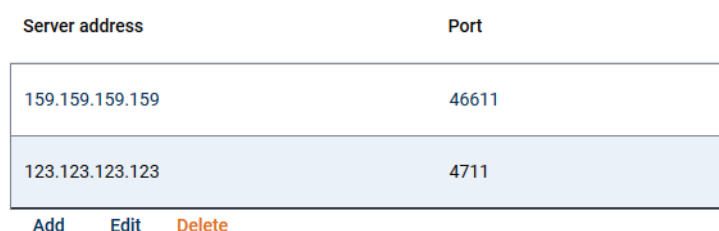
Server address	Port
192.168.169.10	4711

Add Edit Delete

Fig. 33: 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. 29).
Edit	Opens the selected entry for editing (see chapter "Edit LDAP connection data", p. 29).
Delete	Deletes the selected entry from the list.

4.2.5.1 Edit LDAP connection data

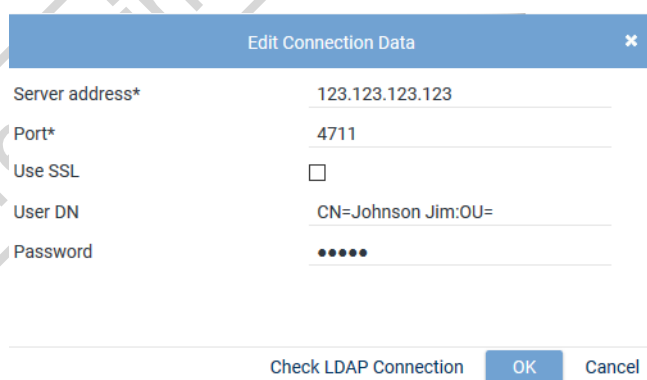


Server address	Port
159.159.159.159	46611
123.123.123.123	4711

Add Edit Delete

Fig. 34: LDAP Connection Data

- To configure a new [LDAP](#) connection, click on the button *Add*.
To edit an existing [LDAP](#) connection, click on the button *Edit*.



Edit Connection Data

Server address*

123.123.123.123

Port*

4711

Use SSL

☐

User DN

CN=Johnson Jim:OU=

Password

.....

Check LDAP Connection

OK

Cancel

Fig. 35: 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.

	<input checked="" type="checkbox"/> = SSL is used. <input type="checkbox"/> = SSL is not used. NOTICE! SSL can only be used if the LDAP server supports SSL .
<i>User DN</i>	Distinguished name (DN) of the user required for the authentication to the LDAP server.
<i>Password</i>	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*.

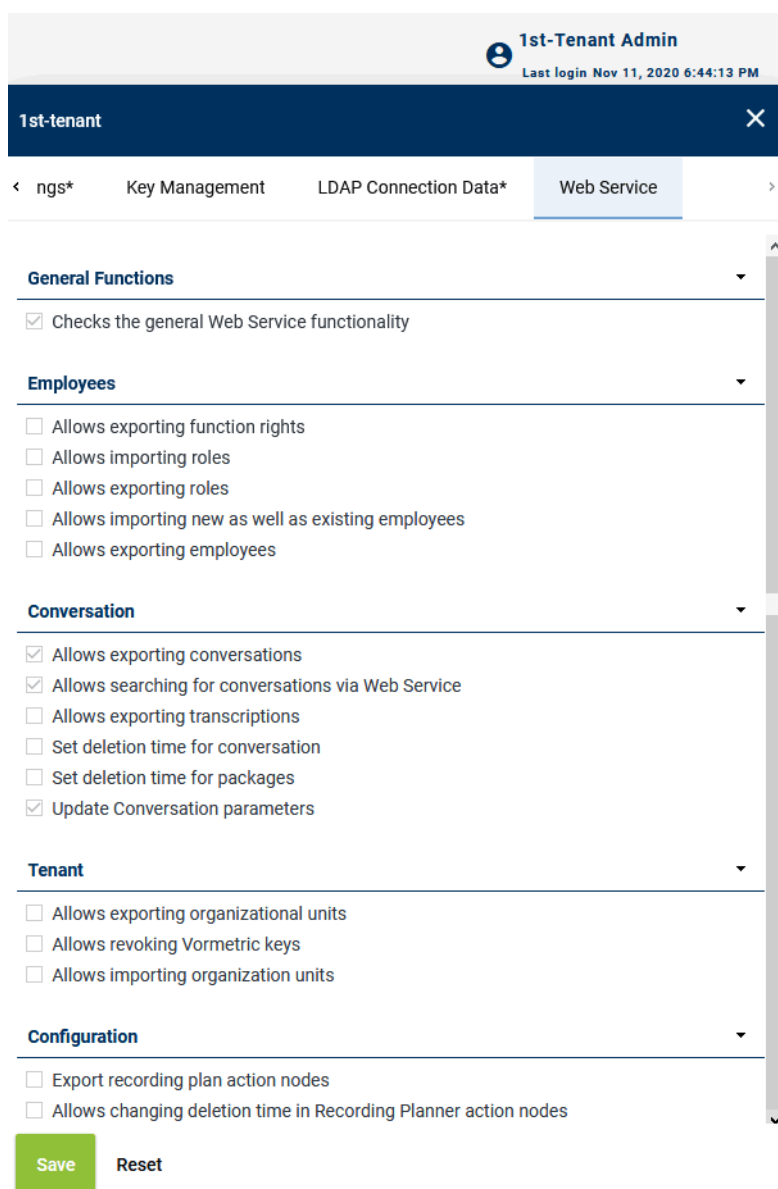
4.2.6 Tab Web Service

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.



1st-Tenant Admin
Last login Nov 11, 2020 6:44:13 PM

1st-tenant

< ngs* Key Management LDAP Connection Data* **Web Service** >

General Functions

- ☒ Checks the general Web Service functionality

Employees

- ☐ Allows exporting function rights
- ☐ Allows importing roles
- ☐ Allows exporting roles
- ☐ Allows importing new as well as existing employees
- ☐ Allows exporting employees

Conversation

- ☒ Allows exporting conversations
- ☒ Allows searching for conversations via Web Service
- ☐ Allows exporting transcriptions
- ☐ Set deletion time for conversation
- ☐ Set deletion time for packages
- ☒ Update Conversation parameters

Tenant

- ☐ Allows exporting organizational units
- ☐ Allows revoking Vormetric keys
- ☐ Allows importing organization units

Configuration

- ☐ Export recording plan action nodes
- ☐ Allows changing deletion time in Recording Planner action nodes

Save **Reset**

Fig. 36: Display web service functions

- ☒ = Function has been activated.
☐ = Function has been deactivated.

Group field General Functions

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

Group field Employees

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

Group field Conversation

<i>Allows exporting conversations</i>	Shows whether conversations can be exported via the Web Service. The exported conversations are saved as WAVE files.
<i>Allows searching for conversations via Web Service</i>	Shows whether conversations can be searched via the Web Service.
<i>Allows exporting transcriptions</i>	Shows whether transcriptions can be exported via the Web Service.
<i>Set deletion time for conversation</i>	Shows whether a deletion time can be set for the conversations.
<i>Set deletion time for packages</i>	Shows whether a deletion time can be set for packages via the Web Service.

Group field Tenant

<i>Allows exporting organization units</i>	Shows whether organization units can be exported via the Web Service.
<i>Allows revoking Vormetric keys</i>	Shows whether a Vormetric keys can be revoked via the Web Service.
<i>Allows importing organization units</i>	Shows whether organization units can be imported via the Web Service.

Group field Configuration

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

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

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

Fig. 37: Employees module - main view

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

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






5.1.1

Toolbar

The toolbar offers the following functions.



Fig. 38: Employees module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria (see chapter "Search", p. 36). The icon  (Search) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Add</i>	Creates a new employee (see chapter "Create new employee", p. 66).
	<i>Delete</i>	Deletes the selected employee.
<i>Employees</i>	<i>Summary</i>	Lists all function rights of the selected employee (see chapter "Show summary", p. 35).
	<i>Show locked employees/Show all employees</i>	Lists only the locked employees in the main view (see chapter "Show locked employees", p. 36).
	<i>Make employee visible or not visible</i>	Function which makes the selected employee visible or not visible for others (see chapter "Make employee visible or not visible", p. 36).

	<i>Display agent's shift schedule</i>	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.
	<i>Export User Data</i>	Exports the user data of the employee of the current tenant in XML format.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • Displayed information • Order of the displayed columns • Number of rows per page
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



For detailed 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.

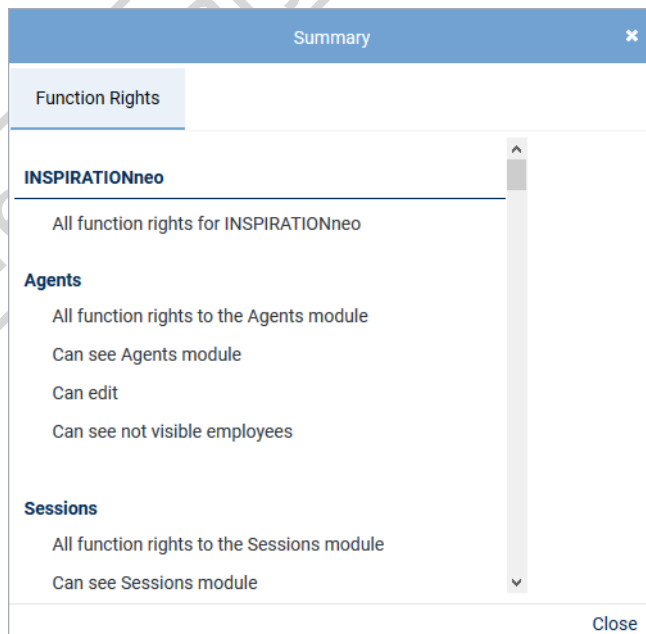


Fig. 39: Summary of the function rights



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.

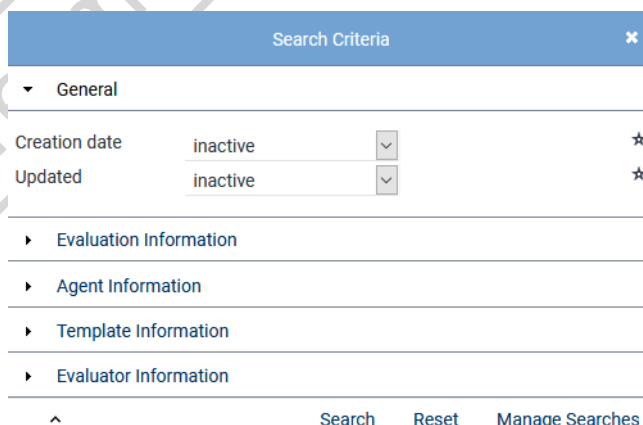





Fig. 40: Window Search Criteria (example)

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.

- 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.

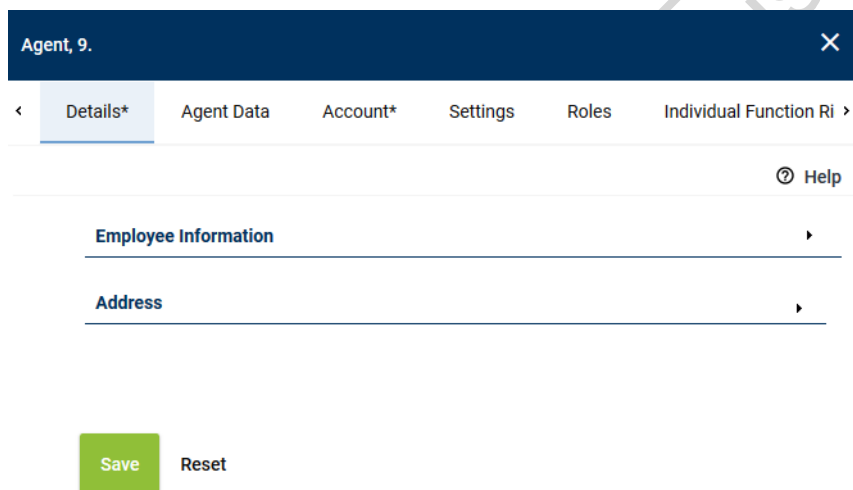


Fig. 41: Employees module - detail view

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. 38](#).

- *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. 42](#).

- *Account*

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

See [chapter "Tab Account", p. 48](#).

- *Settings*

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

See [chapter "Tab Settings", p. 53](#).

- *Roles*

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

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

- *Individual Function Rights*

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

See [chapter "Tab Individual Function Rights", p. 59](#).

- *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. 62](#).

- *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. 64](#).

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.

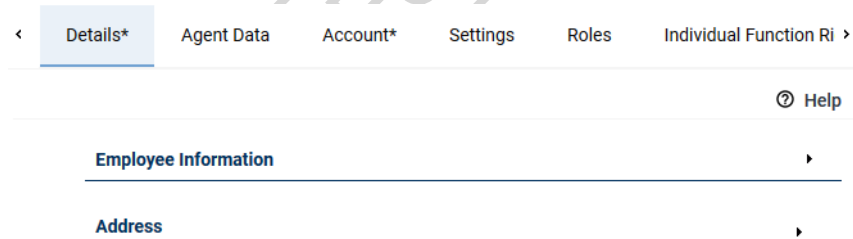



Fig. 42: Employees module - tab Details



Entering an address is optional.




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

5.2.1.1 Group field Employee Information

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


Employee Information




Employee number

First name*

Last name*

Date of birth 

E-mail



Date of entry 

Comment

Address for replay via phone

Import key

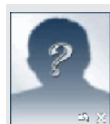
Extended import key

Time zone  

Enable keyword spotting ☐

Enable transcription ☐



Fig. 43: Edit employee information



Placeholder for the employee's photo.

See [chapter "Upload or delete image", p. 41.](#)

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: <ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • MAC address if it has been configured. • SIP address, e. g. <i>Extension@IP-Address</i>.
<i>Import key</i>	<p>Key to unambiguously identify an employee imported from an external source.</p> <p>When importing the employee information for the first time, the import key is entered here automatically. Upon each new import, this import key is checked to determine whether the employee has already been imported before.</p> <p>In addition, the import key is used when transferring (export/import) recordings from a 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.</p> <p>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.</p>
<i>Extended import key</i>	<p>Extended key to unambiguously identify employees imported from an external source.</p> <p>The extended import key is used whenever the standard import key is not sufficient for an unambiguous identification.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<i>Time zone</i>	<p>Shows the time zone in which the conversations are supposed to be displayed in the replay applications. The settings which have been configured for the respective employee prevail over the default settings in the Tenants module</p> <p>To select the time zone, click on the button . See chapter "Add time zone", p. 14.</p> <p>To delete the selection, click on the button .</p>
<i>Activate keyword spotting</i>	<p>Select whether the employee's conversations are supposed to be considered for the speech analysis method <i>keyword spotting</i>.</p> <p><input checked="" type="checkbox"/> = Consider for keyword spotting</p> <p><input type="checkbox"/> = Do not consider for keyword spotting</p> <p>NOTICE! This option is only available in systems with a cloud license.</p>

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.

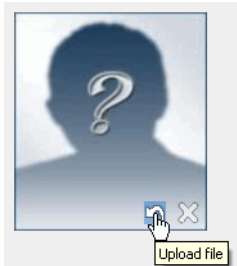


Fig. 44: Upload image

⇒ The window *Upload File* appears.

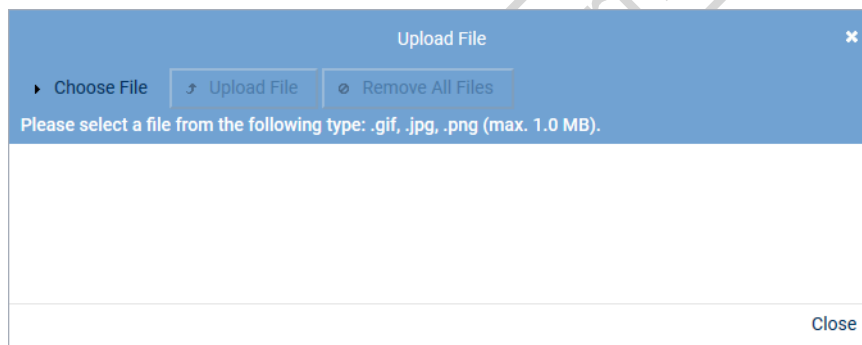



Fig. 45: Upload File

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.

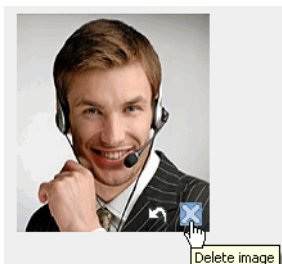


Fig. 46: Delete image (example)

⇒ 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. 47: Add address

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

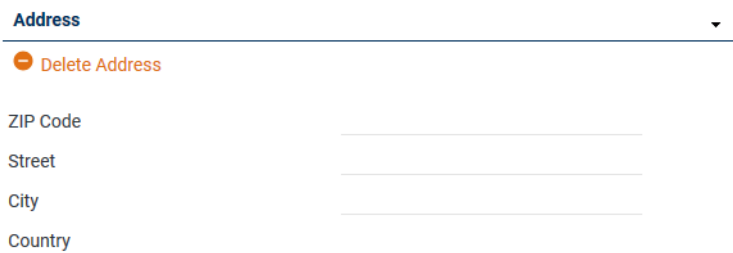


Fig. 48: Add address

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 *live streaming* for the conversations of the agent, see [chapter "Configure live streaming", p. 44](#).

To configure screen recording for agents, see [chapter "Configure screen recording", p. 48](#).

To configure the recording of the agent's, see [chapter "Configure chat recording", p. 46](#).

Entering agent data is optional.

Upon activating the option *Agent*, employees are recognized as agent by the system; however, they do neither receive any role-specific function rights yet nor access to the system. For employees to receive the required function rights, you must either assign them the default role *Agent* or an agent role you have defined yourself, see [chapter "Assign roles", p. 58](#).

Upon deactivating the option *Agent*, the system does not consider employees an agent anymore. The assignment of the role *Agent* is not removed automatically when deactivating the option. If employees are 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. 59](#).



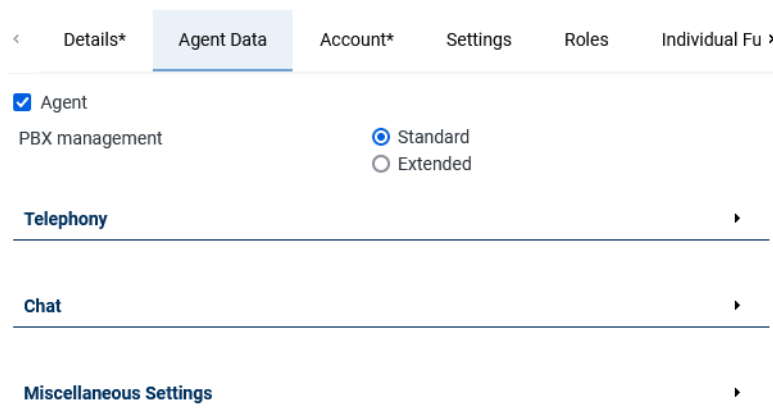


Fig. 49: Employees module - Tab Agent Data

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.

PBX management *Standard*: Select this option to assign employees extensions, PBX Agent IDs, and chat IDs of the same PBX.

Extended: Select this option to assign employees several extensions, PBX Agent IDs, and chat IDs of different PBXs.

NOTICE! If you have configured **several** PBXs in the extended option and switch back to default **all** configurations **are deleted**. If you have configured just one PBX in the extended option, the configuration continues to apply for the default.

5.2.2.1 Group field Telephony

To edit the telephony data of the agent, open the group field *Telephony*. Depending on whether you have selected the default PBX management or the extended PBX management, the view is different:

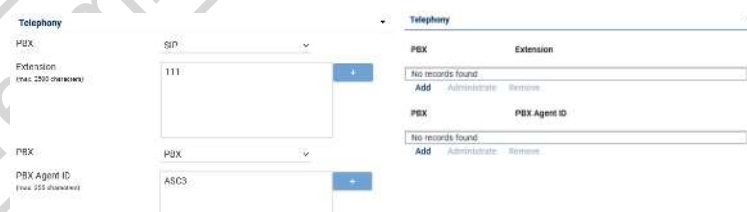


Fig. 50: Agent Data - Telephony

PBX PBX via which the agent's conversations are made.

Select the PBX from the drop-down list.

If you have selected the extended PBX management, first click on the button *Add* to open a configuration window where you proceed as described above; to save your settings click on the button *Apply*.

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 different extensions.

If you have selected the extended PBX management, first click on the button *Add* to open a configuration window where you proceed as described above; to save your settings click on the button *Apply*.

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 agents and their 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.

If you have selected the extended PBX management, first click on the button *Add* to open a configuration window where you proceed as described above; to save your settings click on the button *Apply*.

5.2.2.1.1 Configure live streaming



Precondition for this function:

The system provider has activated the function *live streaming* in the Servers module of the System Configuration.

The function *live streaming* allows users with the respective rights to listen in on a conversation which is currently recorded. If you would like to enable the function *live streaming* 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 *live streaming* 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*.

Extensions		
Extension number	Phone name	Agent name
111		Agent, 111

Rows per page 20 1 - 1 of 1

Add Cancel

Fig. 51: 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

- 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*.

PBX Agent IDs	
PBX Agent ID	Agent name
No records found	

Rows per page 20 0 - 0 of 0

Add Cancel

Fig. 52: 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*.

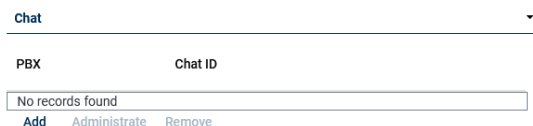



Fig. 53: Agent Data - Chat

Chat system	<p>Chat server via which the agent's chats are made.</p> <p>Select the chat server from the drop-down list.</p> <p>If you have selected the extended PBX management, first click on the button <i>Add</i> to open a configuration window where you proceed as described above; to save your settings click on the button <i>Apply</i>.</p>
Chat ID	<p>IDs which have been saved in the chat system for the agent. By means of these IDs the recording system can identify agents and their participation in a conversation.</p> <p>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.</p> <p>NOTICE! Use commas to separate the different IDs.</p> <p>If you have selected the extended PBX management, first click on the button <i>Add</i> to open a configuration window where you proceed as described above; to save your settings click on the button <i>Apply</i>.</p>

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. 42](#).
2. Open the group field *Chat* in the tab *Agent Data*, see [chapter "Group field Chat", p. 46](#).
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*.

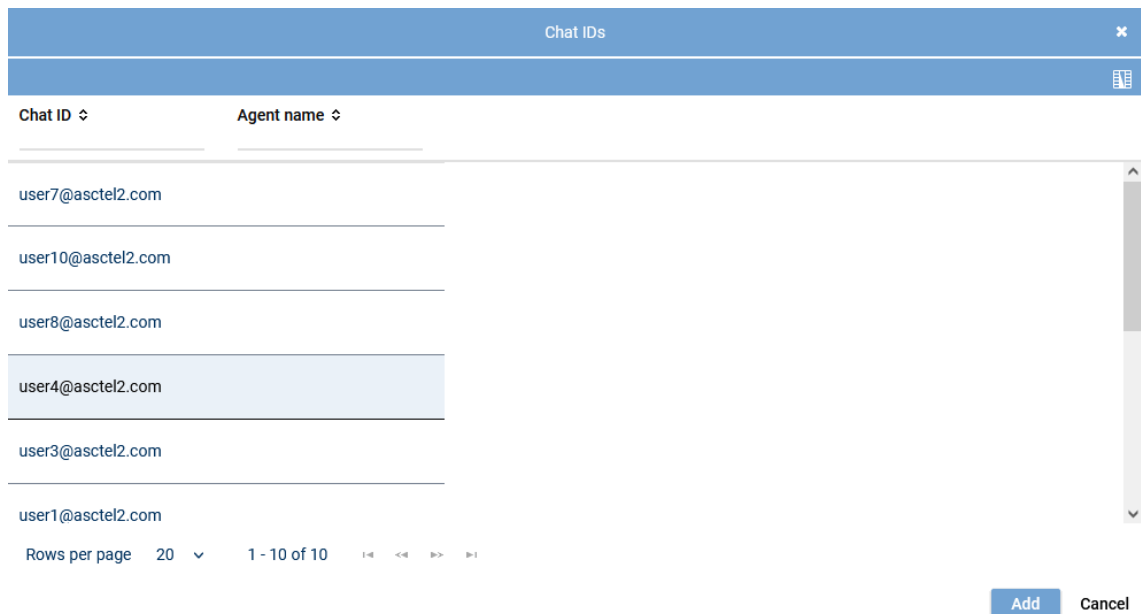


Fig. 54: Add chat ID (example)



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*.

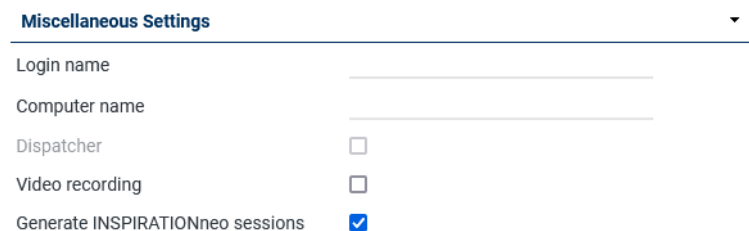


Fig. 55: Agent Data - Miscellaneous Settings

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

	This option is only displayed if there is a video recording license in the system.
<i>Generate INSPIRATION_{neo} sessions</i>	<input checked="" type="checkbox"/> = For this agent, agent sessions are recorded and a license of the type INSPIRATION _{neo} sessions is deducted. <input type="checkbox"/> = For this agent, no agent sessions are recorded. No license of the type INSPIRATION _{neo} sessions is required.

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. 47](#). 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 SCREEN_{rec}*.

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.

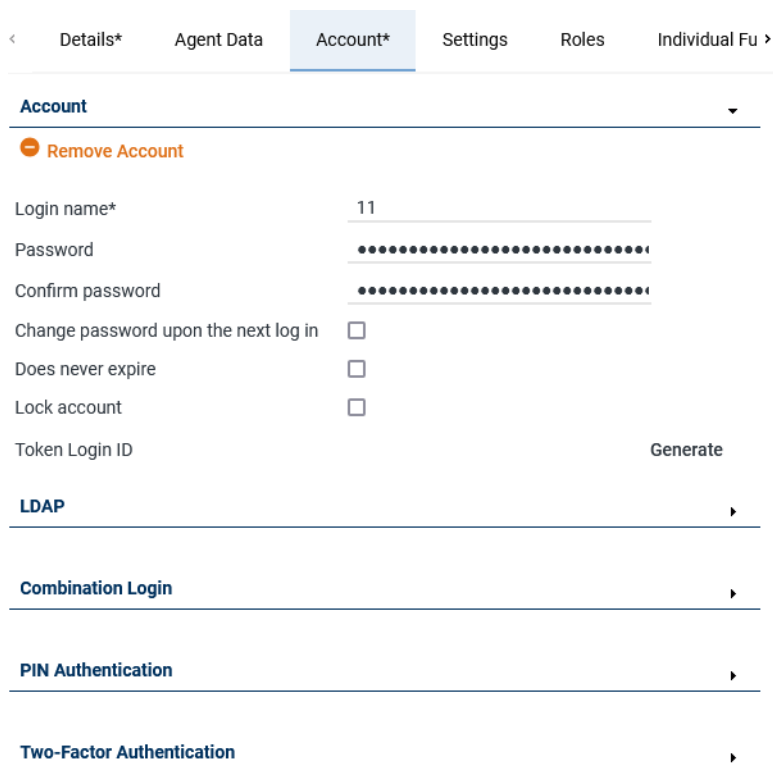



Fig. 56: Employees module - tab Account



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. 57: Add account

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

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

	NOTICE! If you use the function <i>Last Call Repeat</i> , you must use exclusively digits here.
<i>Confirm password</i>	Enter the password of the employee again.
<i>Change password upon the next login</i>	Activate this option if the employee is supposed to change the password upon logging in the next time.
<i>Does never expire</i>	Activate this option if the password is never supposed to expire.
<i>Lock account</i>	This option allows locking the employee's account. In the main view, you can filter for this criterion, see chapter "Show locked employees" , p. 36.
<i>Token login ID</i>	This function must only be configured for the replay application POWERplay Go. To generate a token login ID for employees of the tenant for replay, click on the button <i>Generate</i> . This login ID is configured to automate login for this employee. NOTICE! This option is only available for tenants.
<i>POWERplay Web for Xpert Login ID</i>	This function must only be configured for the replay application POWERplay Web for Xpert. To generate a login ID for the employees of the tenant for the replay in the Xpert client, click on the button <i>Generate</i> . This login ID is configured by the system manager of OpenScape Xpert to automate login for this employee. NOTICE! This option is only available for tenants.

- If you would like to remove the account, click on the button  *Remove account* in the title bar of the group field.
- To activate the authentication via [LDAP](#) for the employee, see [chapter "Authentication via LDAP"](#), p. 50.
- To assign the employee a combination user, see [chapter "Assign combination user"](#), p. 50.
- To activate two-factor authentication for the employee, see [chapter "Two-factor authentication"](#), p. 52.
- To activate the authentication via PIN for the employee, see [chapter "Authentication via PIN"](#), p. 52.

5.2.3.1 Authentication via LDAP

- To activate the authentication via [LDAP](#), open the group field *LDAP*.
- Activate the check box *LDAP authentication*.



Fig. 58: Activate authentication via LDAP

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

☒ = Authentication via [LDAP](#) has been activated.
☐ = Authentication via [LDAP](#) has not been activated.

5.2.3.2 Assign combination user

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



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

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

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

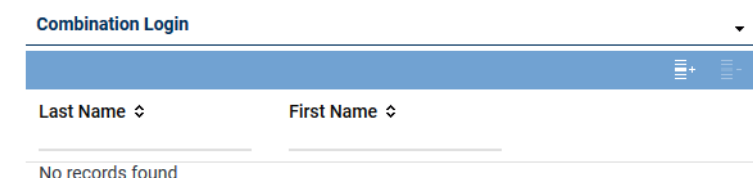
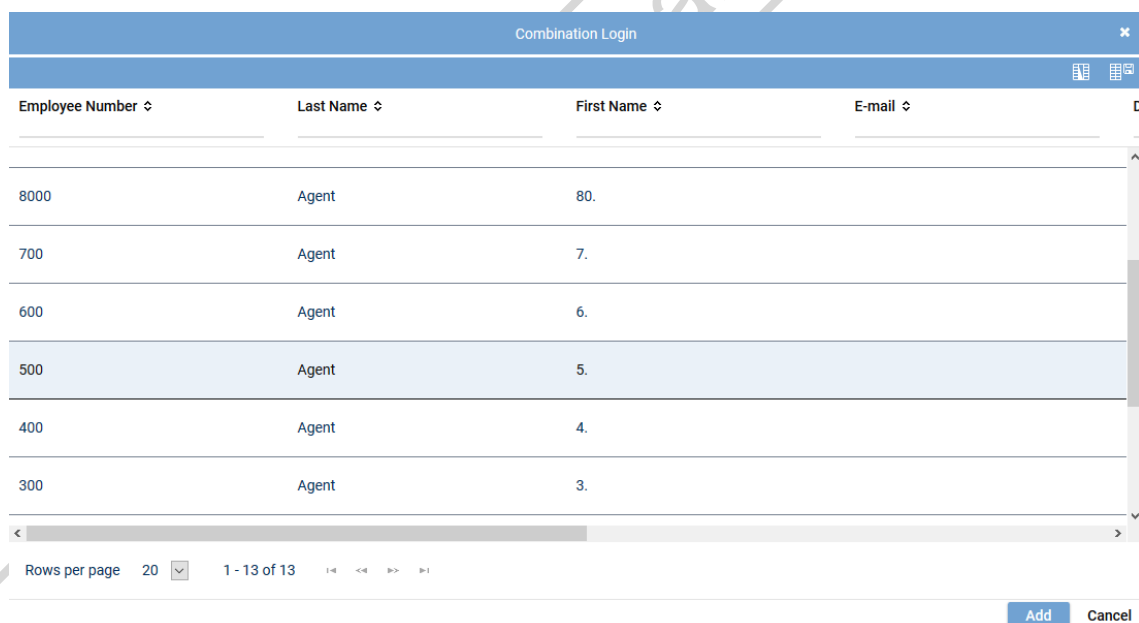


Fig. 59: Assign combination user

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




Employee Number	Last Name	First Name	E-mail
8000	Agent	80.	
700	Agent	7.	
600	Agent	6.	
500	Agent	5.	
400	Agent	4.	
300	Agent	3.	

Fig. 60: 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*).

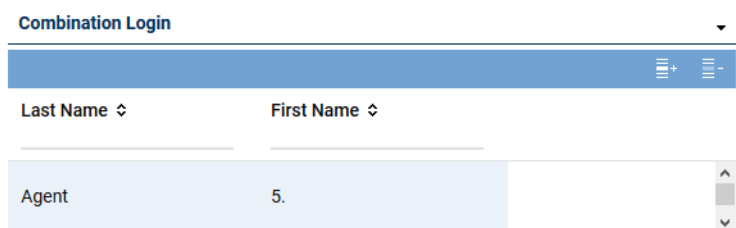


Fig. 61: Delete combination user assignment

5.2.3.4 Two-factor authentication

1. To activate two-factor authentication, open the group field *Two-Factor Authentication*.
2. Activate the check box *Two-factor authentication*.

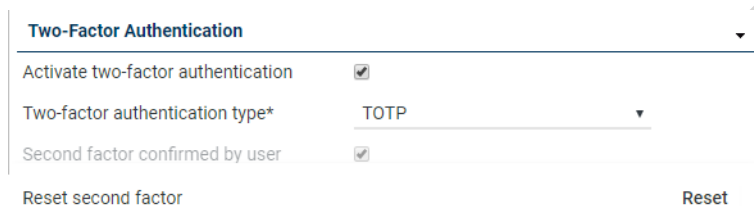


Fig. 62: Activate two-factor authentication

<i>Activate two-factor authentication</i>	Select whether two-factor authentication is supposed to be activated for the respective user. <input checked="" type="checkbox"/> = Two-factor authentication has been activated. <input type="checkbox"/> = Two-factor authentication has not been activated.
<i>Two-factor authentication type</i>	From the drop-down list, select the two-factor authentication type that you would like to use.
<i>Second factor confirmed by user</i>	Displays whether a user has already used the authenticator app to log in to one of the applications.
<i>Reset second factor</i>	If a user has already used the authenticator app to log in to one of the applications it is possible to reset the two-factor authentication data in case the end device used for authentication purposes so far is replaced. To reset the data, click on the button <i>Reset</i> and confirm your entries by clicking on the button <i>Save</i> .

5.2.3.5 Authentication via PIN

1. To activate PIN authentication, open the group field *PIN Authentication*.
2. Activate the check box *PIN authentication*.

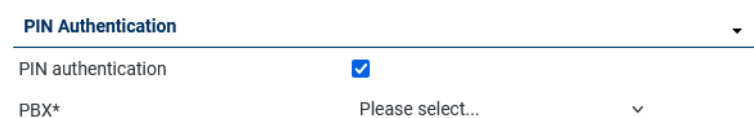


Fig. 63: Activate PIN authentication

3. In the drop-down list *PBX* select the PBX for which you would like to activate PIN authentication.
4. If you would like to deactivate PIN authentication, deactivate the check box *PIN authentication*.

☒ = PIN authentication has been activated.

☐ = PIN authentication has not been activated.

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.

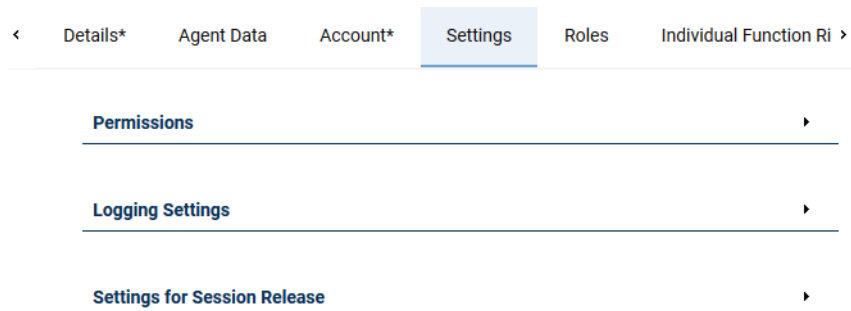


Fig. 64: Employees module - tab Settings

5.2.4.1 Group field Permissions

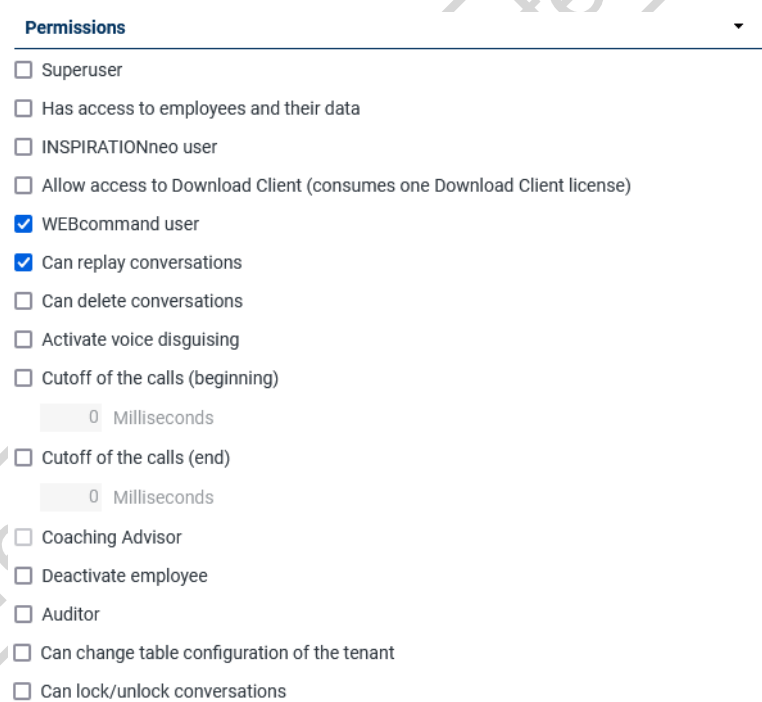


Fig. 65: Define permissions

☒ = Right has been activated.

☐ = Right has been deactivated.

Superuser	This right gives the user all licensed functions rights in the system.
Has access to employees and their data	This right gives the user access to the data of the employees. It depends on the individual function rights whether and to which degree the user can edit this data.

	Without this right, users can only see the data of other employees if they are superior of an organization unit (see chapter "Tab Organization Units", p. 64). In this case, only the data of members of this organization unit and own data is visible.
<i>INSPIRATIONneo user</i>	This right allows the user to log in to the application <u>INSPIRATIONneo</u> . NOTICE! If this right has been deactivated, it is not possible to log in to the application <u>INSPIRATIONneo</u> .
<i>Allow access to Download Client (consumes one Download Client license)</i>	This right allows users to log in to the application Download Client. NOTICE! If this right has been deactivated, it is not possible to log in to the application Download Client.
<i>WEBcommand user</i>	This right enables users to log in to the application <u>WEBcommand</u> . NOTICE! If this right has been deactivated, it is not possible to log in to the application <u>WEBcommand</u> .
<i>Can replay conversations</i>	This right allows users to replay conversations in addition to being able to see it if they have the required rights for replay in a replay application.
<i>Can delete conversations</i>	This right allows users to delete conversations in the application <u>POWERplay Web</u> . This option is license-dependent.
<i>Activate voice disguising</i>	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.
<i>Cutoff of the calls (beginning)</i>	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.
<i>Cutoff of the calls (end)</i>	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.
<i>Coaching Advisor</i>	This right allows the user to record coaching advisor sessions by means of the application <u>CLIENTcommand</u> . Coaching advisor session are simulated sessions which are recorded for training purposes. These sessions are displayed in the Coaching Advisor module of the application <u>INSPIRATIONneo</u> . 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. 59 .
<i>Deactivate employee</i>	This right allows deactivating an employee. <input checked="" type="checkbox"/> = Employee has been deactivated. <input type="checkbox"/> = 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.
<i>Auditor</i>	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.

	<p>Auditors have restricted agent rights and can only see their own sessions and evaluations which are required to audit the respective agent.</p> <p>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 <i>Has access to employees and their data</i> has been activated, the user has access to all agents and their data.</p> <p>To enable an auditor to use INSPIRATION_{neo}, the above function right <i>INSPIRATIONneo user</i> must have been activated.</p> <p>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.</p> <p>In the Recording Planner module, the conversation type <i>work item</i> must have been selected in the detail view of the recording plan.</p>
<i>Can change table configuration of the tenant</i>	<p>This right allows the user to change the default table configuration for the employees of the tenant.</p> <p>This applies to the main view of the respective modules as well as to dialog windows.</p>
<i>Can lock/unlock conversations</i>	<p>This right allows the user to locked conversations or to unlock locked conversations.</p>



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

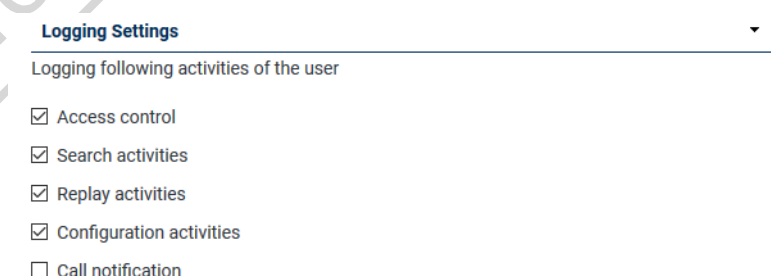


Fig. 66: Configure logging

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

- ☒ = Logging has been activated.
- ☐ = Logging has been deactivated.

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

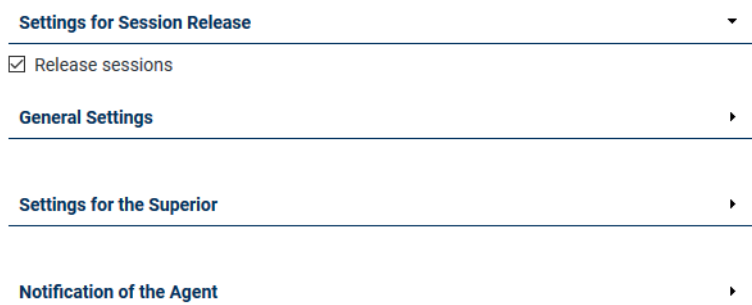
5.2.4.3 Group field Settings for Session Release



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

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

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



Settings for Session Release

- ☒ Release sessions
- General Settings**
- Settings for the Superior**
- Notification of the Agent**

Fig. 67: Set session release for agents

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

Group field General Settings

Define the conditions under which agents release sessions

General Settings ▼

Minimum number of sessions of the agent*	10
Minimum number of sessions to be released*	3
Maximum number of sessions to be released*	5
Period of time	Quarterly ▼

Fig. 68: Session release - General Settings

<i>Minimum number of sessions of the agent</i>	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.
<i>Minimum number of sessions to be re-released</i>	<p>Select how many sessions the agent has to release within the defined period time at least. If the agent has released fewer sessions at the end of the period than defined here, then the missing number of sessions is transferred to the following period of time.</p> <p>Example: An agent has to release at least 3 sessions per quarter. However, at the end of the quarter he has only released 2 sessions. As a consequence, he has to release at least 4 sessions until the end of the following quarter.</p>
<i>Maximum number of sessions to be re-released</i>	Select how many sessions the agent can release within the defined period time at the maximum.
<i>Period of time</i>	<p>Select the period of time that the settings of the session release are supposed to refer to.</p> <p>Select the period from the drop-down list.</p>

Group field Settings for the Superior

Select which sessions the superior can see and evaluate.

Settings for the Superior ▼

Access to sessions

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

Fig. 69: Session release - Settings for the Superior

<i>Access to sessions</i>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>only released ones</i> The superior can only see the sessions that the agent has released. All other sessions are not visible for the superior. • <i>all, only released ones can be evaluated</i> The superior can see all of the agent's sessions. However, he can only evaluate the sessions that the agent has released. The superior can see and replay the sessions which have not been released by the agent but he cannot evaluate them.
---------------------------	---

Group field Notification of the Agent

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

Notification of the Agent

☒ via e-mail

☐ via CLIENTcommand

Reminder

Weekly



Fig. 70: 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 CLIENTcommand.

☐ = The agent is not informed in the application CLIENTcommand.

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.

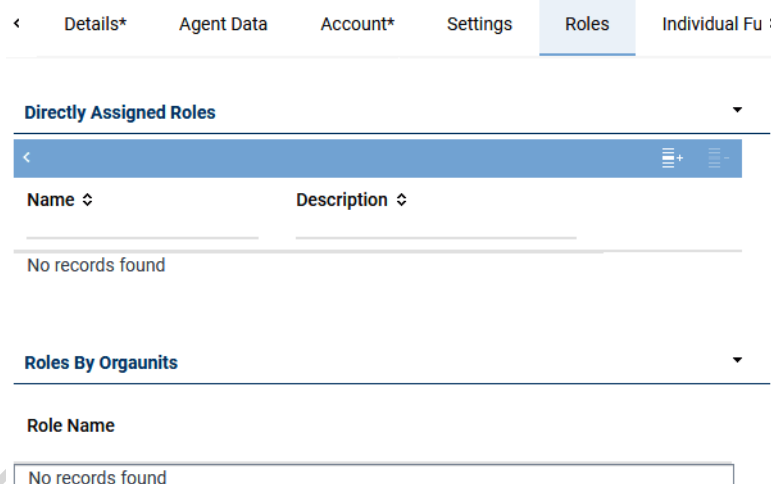


Fig. 71: Employees module - tab Roles

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).

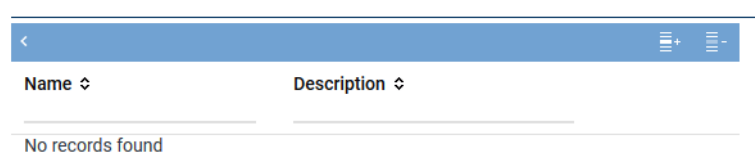
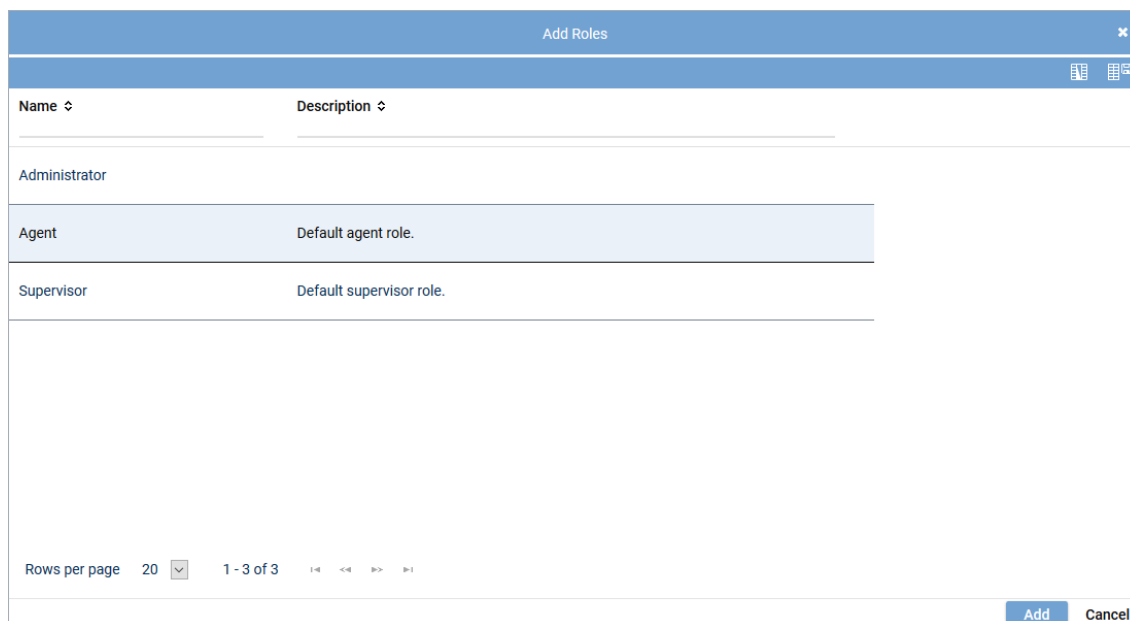


Fig. 72: Assign roles

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



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


Rows per page 20 1 - 3 of 3

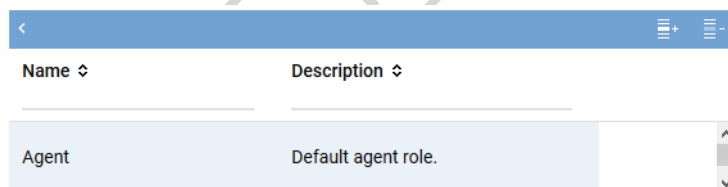
Add Cancel

Fig. 73: 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*).



Name	Description
Agent	Default agent role.

Fig. 74: Delete role assignment



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

5.2.6 Tab Individual Function Rights

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

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

Fig. 75: Employees module - tab Individual Function Rights (example)

You can assign the function rights for the different Neo applications individually.

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

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

Fig. 76: Function rights - display sections (example)

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




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

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

System Configuration ▾




☐ All function rights for System Configuration

User Configuration -

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

Tenants +

Fig. 77: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. <input checked="" type="checkbox"/> = individual function right <input type="checkbox"/> = no individual function right
Name	Description of the function right.
Type	Shows which license is required for this right.  = agent license  = supervisor license  = basic license (without agent or supervisors rights)
Role	Shows whether the function right has been assigned to the user via a role (role right). no mark = no role right <input checked="" type="checkbox"/> = role right NOTICE! In the window <i>Summary</i> , you can see via which role the function right has been assigned, see chapter "Show summary", p. 35 .

Tab. 1: Function rights

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

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

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

<i>Can remove editing locks</i>	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 function rights

The options in the group field *Player function rights* are implemented by all ASC player components offering the respective function. These are POWERplay Pro, POWERplay Web, and INSPIRATIONneo.

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

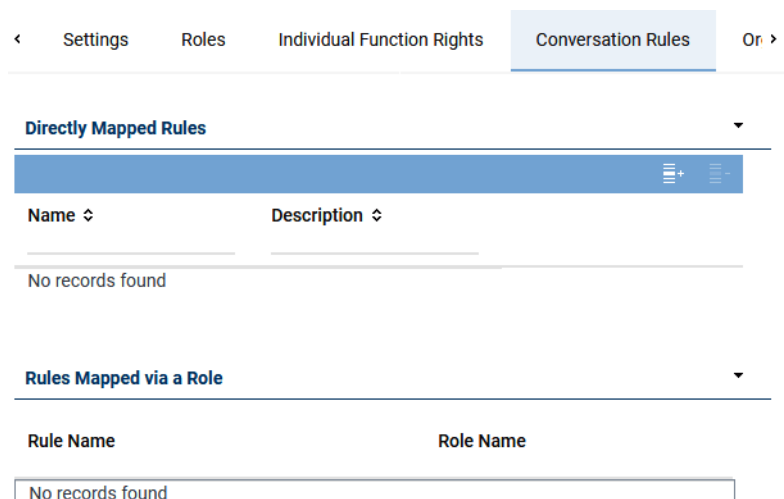


Fig. 78: Employees module - tab Conversation Rules

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
POWERplay Web	<ul style="list-style-type: none"> • Conversation module • Participant View module
POWERplay Pro	<ul style="list-style-type: none"> • Conversation module • Participant View module
INSPIRATIONneo	<ul style="list-style-type: none"> • 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. 63](#) and [chapter "Delete conversation rule assignment", p. 64](#).

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).

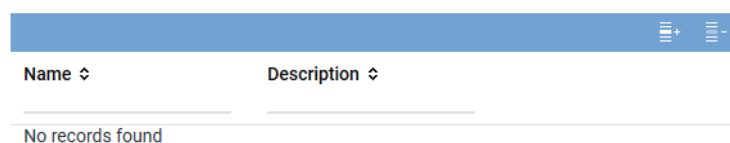


Fig. 79: Assign conversation rule


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

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

Fig. 80: Add conversation rules

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

5.2.7.2 Delete conversation rule assignment

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

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

Fig. 81: 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. 53](#)) 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. 82: Employees module - tab Organization Units

Group field Access To

Here, you see the organization units that the employee has been mapped to as superior. You can change the mapping arbitrarily. See [chapter "Assign organization units", p. 65](#) and [chapter "Delete organization unit assignment", p. 66](#).

Group field Member Of

Here, you see the organization units that the employee has been mapped to as member. You can change the mapping arbitrarily. See [chapter "Assign organization units", p. 65](#) and [chapter "Delete organization unit assignment", p. 66](#).

5.2.8.1 Assign organization units

1. Click on the icon  (Add).

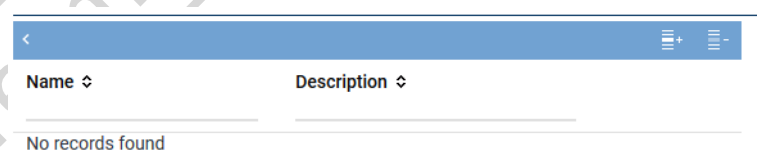


Fig. 83: Assign organization units

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.

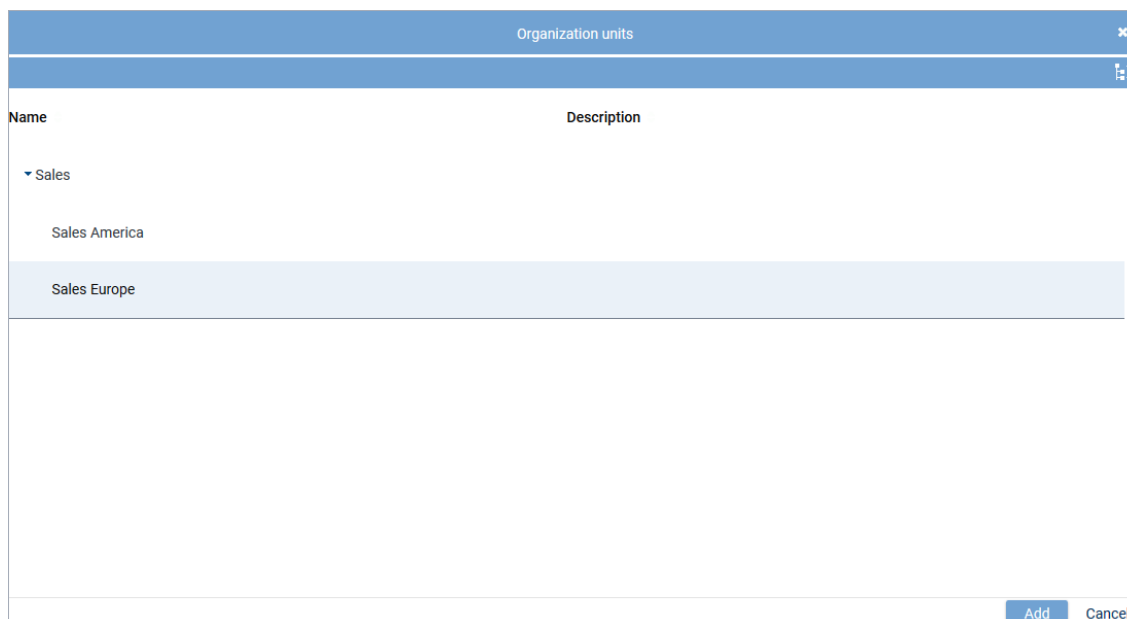





Fig. 84: Add organization units




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

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

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

5.2.8.2 Delete organization unit assignment

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

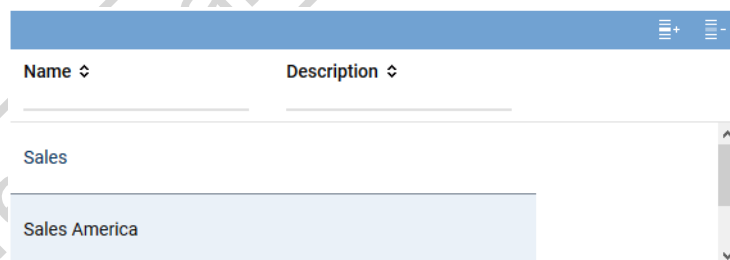



Fig. 85: Delete organization unit assignment

5.3 Create new employee

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

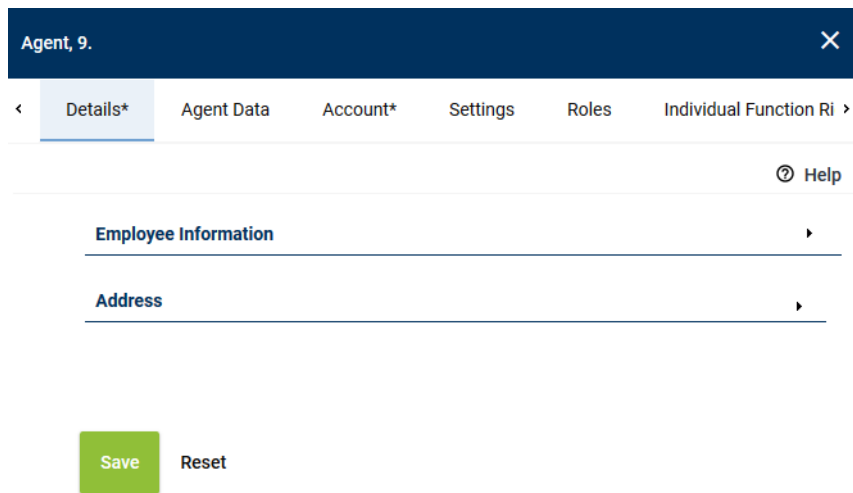


Fig. 86: Save employee

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



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


5.4

Edit employee

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

5.5

Delete employee

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



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



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

5.6


Create new employee with OAuth login

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

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



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

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

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



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



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

6 Organization Structure module

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



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

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

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



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

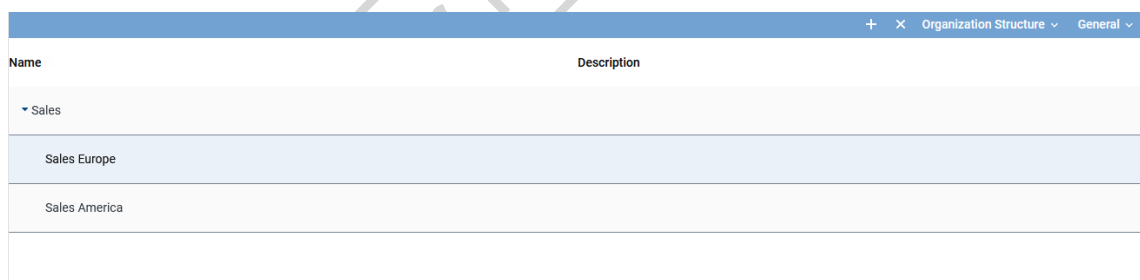


You can import configuration data from existing [LDAP](#) structures, too. The import is configured in the Configuration Import module. For further information refer to the administration manual *Import of configuration data*.

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

6.1 Main view

All saved organization units are displayed in the main view.





Name	Description
▼ Sales	
Sales Europe	
Sales America	

Fig. 87: Organization Structure module - main view

The following information is displayed in the main view:

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



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

6.1.1 Toolbar

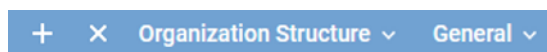




Fig. 88: Organization Structure module - toolbar

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

	<i>Create</i>	Creates a new organization unit (see chapter "Create new organization unit", p. 74).
	<i>Delete</i>	Deletes the selected organization unit (see chapter "Delete organization unit", p. 75).

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



For detailed 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.

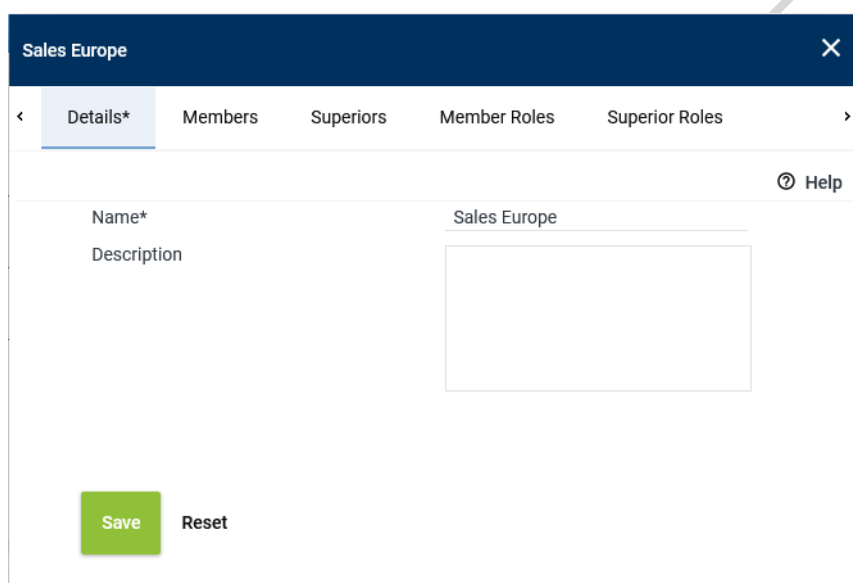


Fig. 89: Organization Structure module - detail view

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. 71](#).
- *Members*
Here, you can display the members of the organization unit and edit the member assignment.
See [chapter "Tab Members", p. 71](#).
- *Superiors*
Here, you can display the superiors of the organization unit and edit the superiors' assignment.
See [chapter "Tab Superiors", p. 72](#).
- *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. 73](#).
- *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. 74.](#)

6.2.1 Tab Details

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

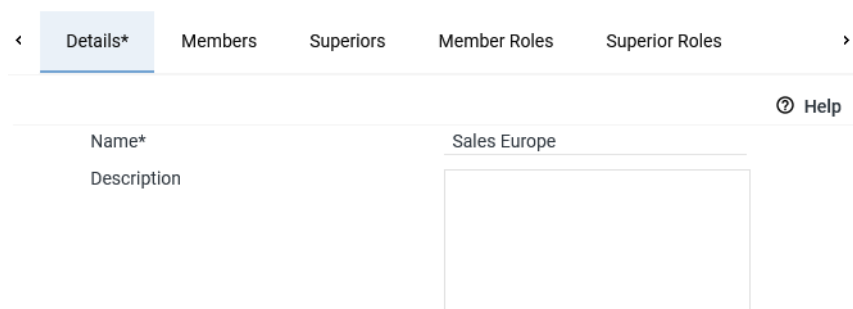
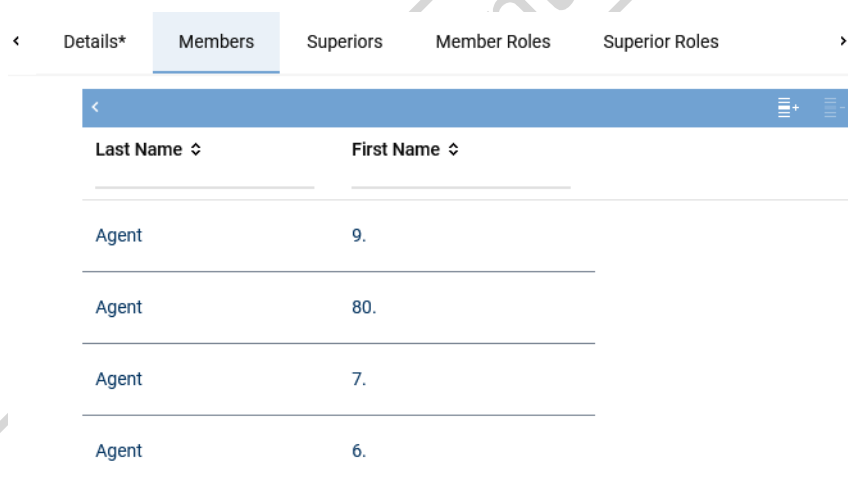


Fig. 90: Organization Structure module - tab Details

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.

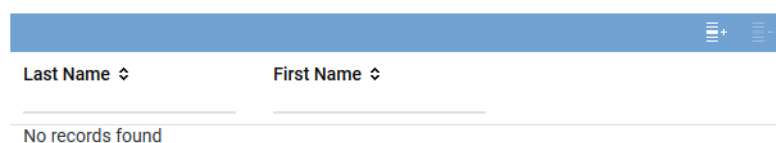


Last Name ↕	First Name ↕
Agent	9.
Agent	80.
Agent	7.
Agent	6.

Fig. 91: Organization Structure module - tab Members

6.2.2.1 Assign members

1. Click on the icon  (Add).



Last Name ↕	First Name ↕
No records found	

Fig. 92: Assign users

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

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


Rows per page 20 1 - 11 of 11

Add Cancel

Fig. 93: Add user

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

6.2.2.2 Delete member assignment

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

Last Name ↕	First Name ↕
Agent	9.

Fig. 94: Delete user assignment

6.2.3 Tab Superiors

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

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

Fig. 95: Organization Structure module - tab Superiors

6.2.3.1 Assign superiors

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

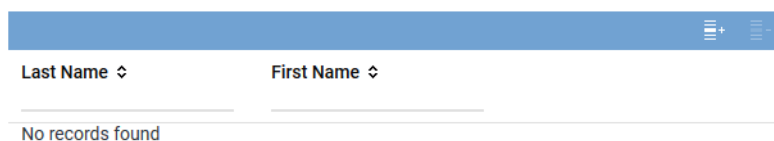
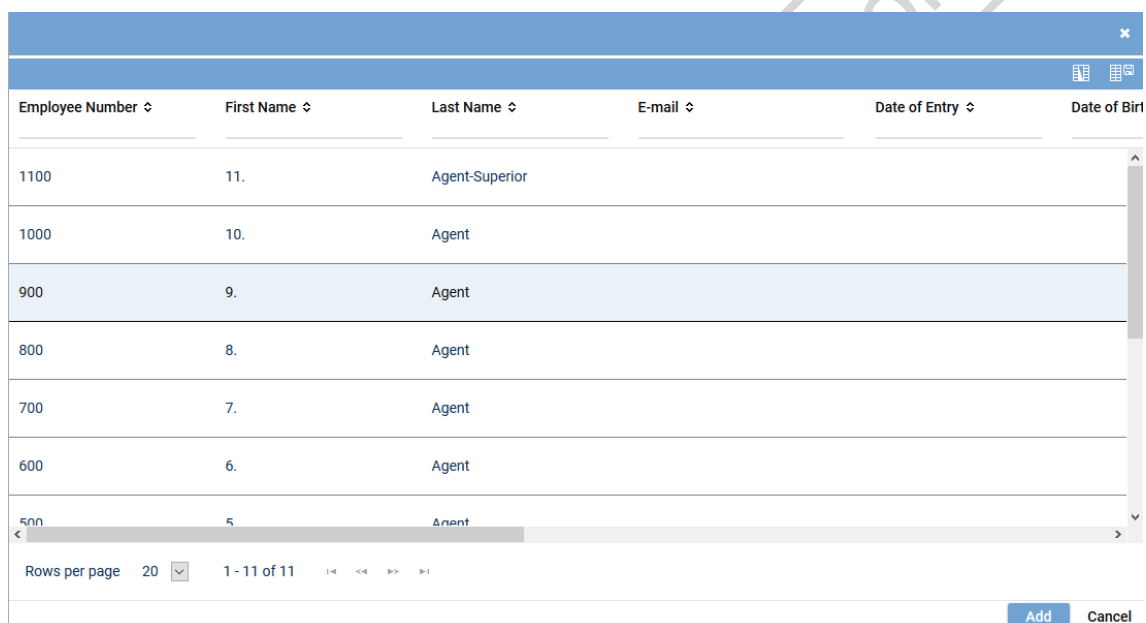


Fig. 96: Assign users

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




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

Fig. 97: 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*).

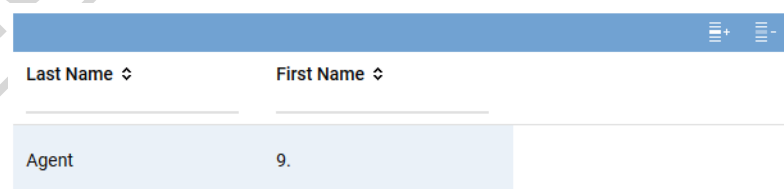


Fig. 98: Delete user assignment

6.2.4 Tab Member Roles

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

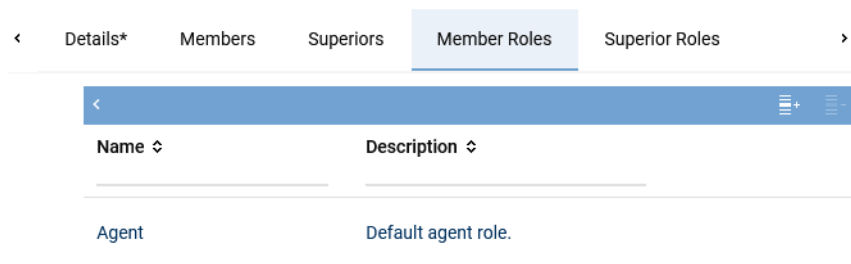


Fig. 99: Organization Structure module - tab Member Roles

For a description of how to add roles, see [chapter "Assign roles", p. 58](#).

For a description of how to remove roles, see [chapter "Delete role assignment", p. 59](#).

6.2.5 Tab Superior Roles

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

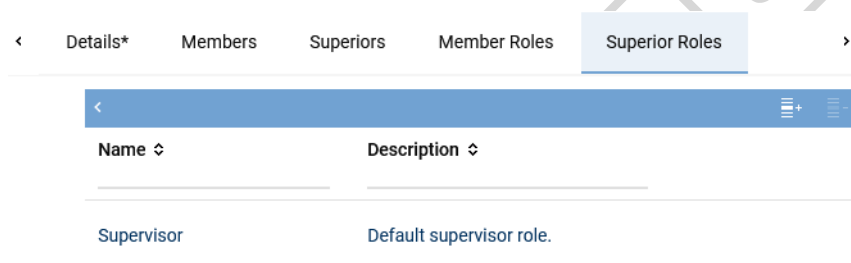


Fig. 100: Organization Structure module - tab Superior Roles

For a description of how to add roles, see [chapter "Assign roles", p. 58](#).


For a description of how to remove roles, see [chapter "Delete role assignment", p. 59](#).

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. 70](#)).
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.

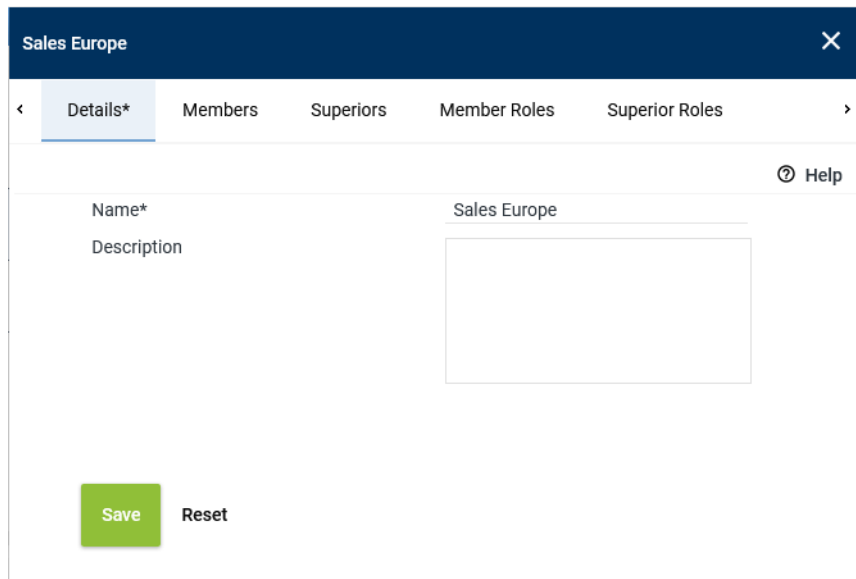


Fig. 101: Save organization unit

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. 70](#). 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*.

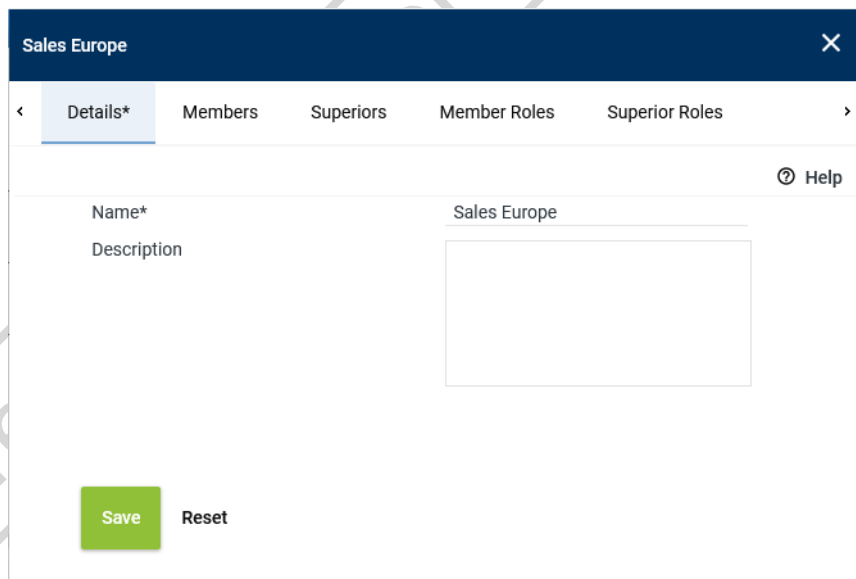



Fig. 102: Save changes

6.5

Delete organization unit

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



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

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

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

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

- Role *Agent*

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

- Evaluations module
- Sessions module
- E-Learning module

- Role *Supervisor*

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

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



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

The default roles *Agent* and *Supervisor* cannot be changed. To deactivate individual function right which are not wanted in a default role, duplicate the role and make the respective changes in the duplicate (see [chapter "Duplicate role", p. 84](#)). 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.

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

Rows per page 50 1 - 3 of 3

Fig. 103: Roles module - main view

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

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






7.1.1

Toolbar

The toolbar offers the following functions.



Fig. 104: Roles module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 36 . The icon  (<i>Search</i>) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new role (see chapter "Create new role", p. 83).
	<i>Delete</i>	Deletes the selected role (see chapter "Delete role", p. 85).
<i>Roles</i>	<i>Duplicate with Employees</i>	Creates a copy of the selected role (see chapter "Duplicate role", p. 84).
	<i>Duplicate Without Employees</i>	Creates a copy of the selected role (see chapter "Duplicate role", p. 84).
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • Displayed information • Order of the displayed columns • Number of rows per page
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



For detailed 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.

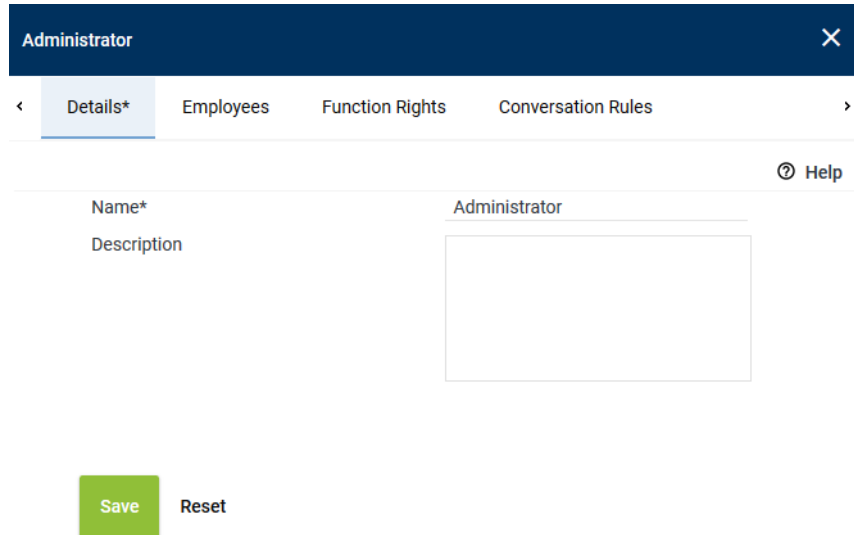


Fig. 105: Roles module - detail view

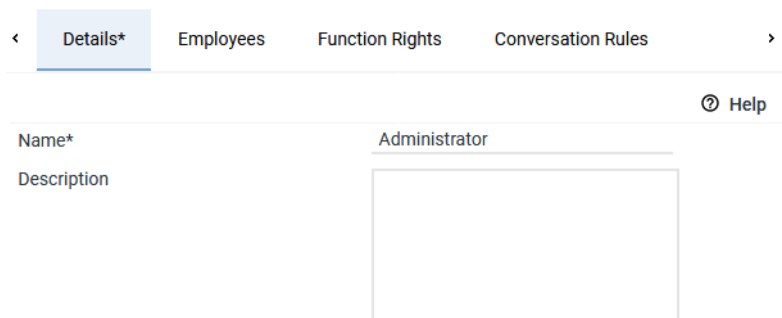
The detail view consists of the following tabs:

- *Details*
Here, you can display and edit the name and the description of the role.
See [chapter "Tab Details", p. 78](#).
- *Employees*
Here, you can display the users who have been assigned the role and edit the user assignment.
See [chapter "Tab Employees", p. 79](#).
- *Function Rights*
Here, you can display and assign the function rights of the role.
See [chapter "Tab Function Rights", p. 80](#)
- *Conversation Rules*
Here, you can display and assign the conversation rules of the role.
See [chapter "Tab Conversation Rules", p. 82](#).

7.2.1

Tab Details

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



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

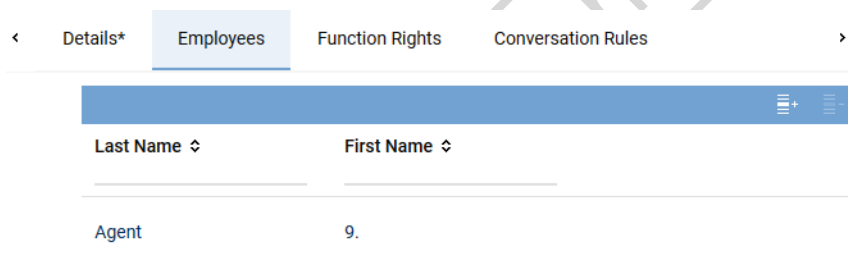
Fig. 106: Roles module - tab Details

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.



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

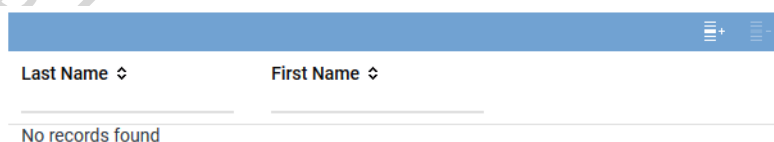
Fig. 107: Roles module - tab Employees



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

7.2.2.1 Assign users

1. Click on the icon  (Add).



The screenshot shows the 'Assign users' step. It displays a table with two columns: 'Last Name' and 'First Name'. Below the table, it says 'No records found'. There is a blue header bar with a '+' icon and a search bar.

Fig. 108: Assign users

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

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

Fig. 109: Add user

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

7.2.2.2 Delete user assignment

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

Last Name ↕		First Name ↕	
Agent		9.	

Fig. 110: Delete user assignment

7.2.3 Tab Function Rights

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

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

Fig. 111: Roles module - tab Function Rights (example)

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

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

Fig. 112: Function rights - display sections (example)

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




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

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

System Configuration




☐ All function rights for System Configuration

User Configuration

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

Tenants

Fig. 113: Function rights - Display function rights

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

Tab. 4: Function rights

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

7.2.4 Tab Conversation Rules

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



Conversation rules can be defined in the Conversation Rules module.

<	Details*	Employees	Function Rights	Conversation Rules	>
---	----------	-----------	-----------------	--------------------	---

Fig. 114: 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).

Name ↕	Description ↕
No records found	

Fig. 115: Assign conversation rule


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

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

Fig. 116: Add conversation rules

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


7.2.4.2 Delete conversation rule assignment

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

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

Fig. 117: Delete conversation rule assignment

7.3 Create new role

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

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

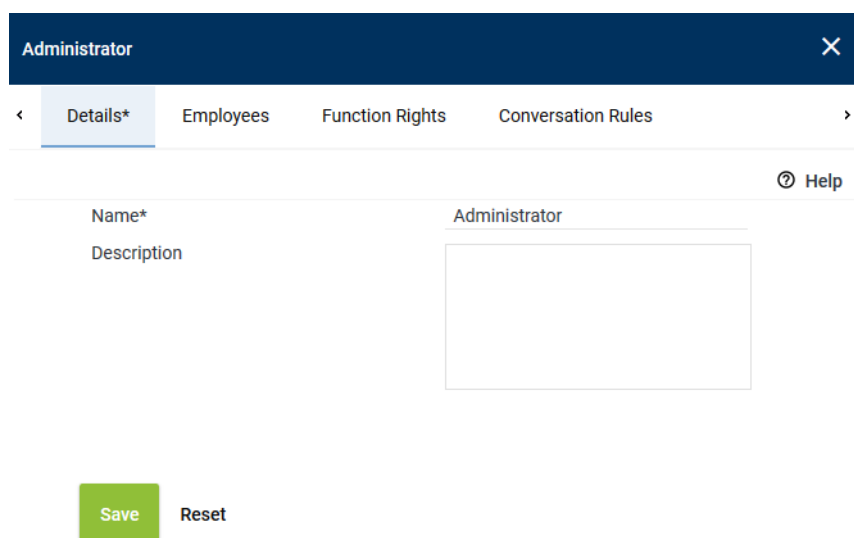


Fig. 118: Save role

7.4

Duplicate role

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

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

- A copy of the role is created in the detail view.
- Enter a new name for the copied role.
- Adjust all settings in the tabs of the detail view as described in the respective chapters (see [chapter "Detail view", p. 78](#)).
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button *Save* to save the settings. To discard the entries, click on the button *Reset*.

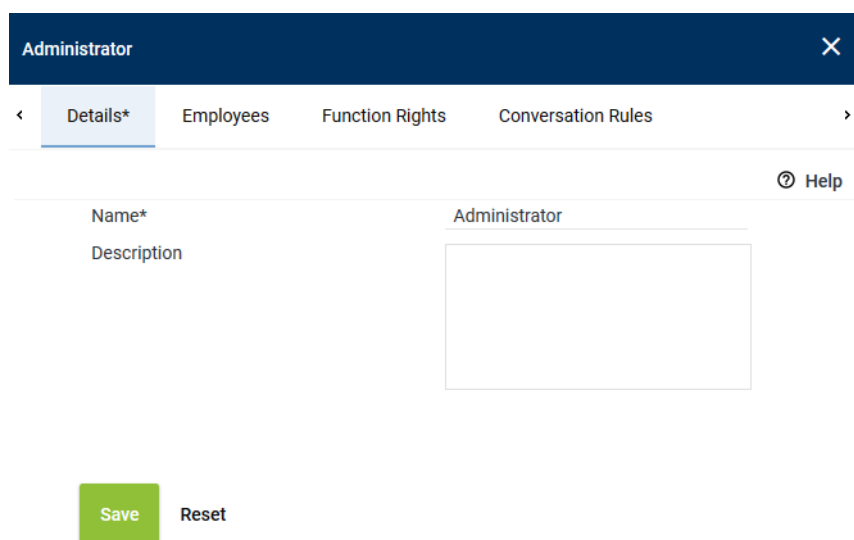


Fig. 119: Save role

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. 78](#). 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**.

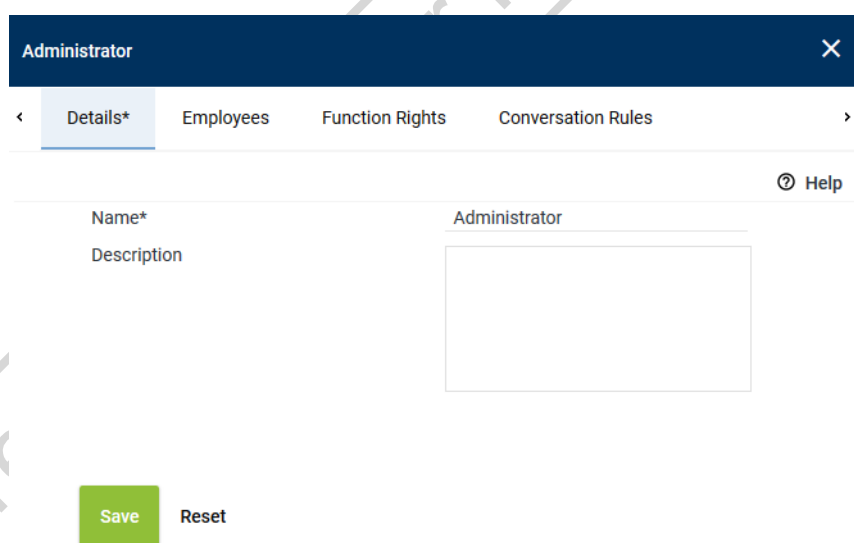



Fig. 120: Save changes

7.6

Delete role

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



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

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

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

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

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

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

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

Example 1:

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

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

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

Example 2:

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

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

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

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

Conversation rules take effect in the following applications and modules:

Application	Module
POWERplay Web	<ul style="list-style-type: none"> • Conversation module • Participant View module
POWERplay Pro	<ul style="list-style-type: none"> • Conversation module • Participant View module
INSPIRATIONneo	<ul style="list-style-type: none"> • 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 INSPIRATIONneo;
- the settings in the tab *Participant View Criteria* affect the participant view in POWERplay Web and in POWERplay Pro;
- the settings in the tab *Conversation Criteria* affect the conversation view in POWERplay Web, in POWERplay Pro as well as in the Sessions module in INSPIRATIONneo.

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

8.1

Main view

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

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

Fig. 121: 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. 122: Conversation Rules module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 36 . The icon  (<i>Search</i>) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new conversation rule (see chapter "Create new conversation rule", p. 100).
	<i>Delete</i>	Deletes the selected conversation rule (see chapter "Delete conversation rule", p. 102).
<i>Conversation Rules</i>		This menu is currently not available
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> • Displayed information • Order of the displayed columns • Number of rows per page
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.

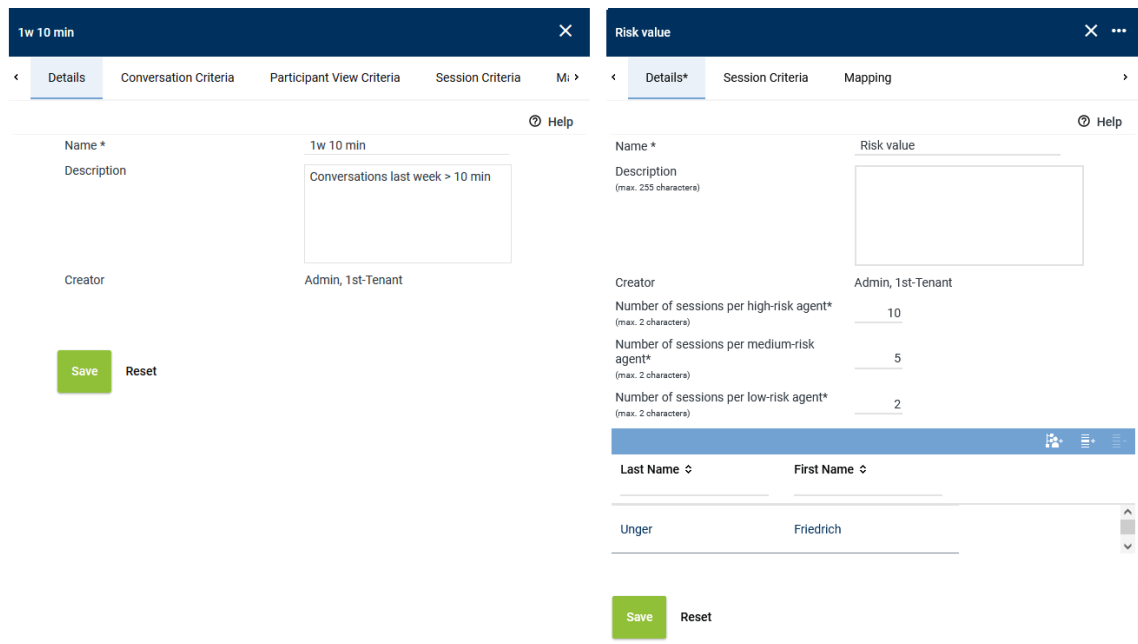


For detailed descriptions of the default functions such as *Search*, *Print*, *Adjust table* or *Help* refer to the user manual for system providers *General information - System Configuration*.

8.2

Detail view

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



The screenshot displays two side-by-side panels of the Conversation Rules module. The left panel is titled '1w 10 min' and the right panel is titled 'Risk value'. Both panels have a 'Details' tab selected. The left panel shows fields for Name (1w 10 min), Description (Conversations last week > 10 min), and Creator (Admin, 1st-Tenant). The right panel shows fields for Name (Risk value), Description, Creator (Admin, 1st-Tenant), and three session criteria: Number of sessions per high-risk agent* (10), Number of sessions per medium-risk agent* (5), and Number of sessions per low-risk agent* (2). Both panels have 'Save' and 'Reset' buttons at the bottom.

Fig. 123: 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. 90](#).
- **Conversation Criteria**
Here, you can define filter criteria based on the conversation data.
See [chapter "Tab Conversation Criteria", p. 93](#).
- **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. 96](#).
- **Session Criteria**
Here, you can define filter criteria based on the session data.
See [chapter "Tab Session Criteria", p. 98](#).
- **Assignment**
Here, you can see the roles and employees that the conversation rule has been mapped to.
See [chapter "Tab Mapping", p. 100](#).

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.

Time and Duration 1

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

2 3 4

Fig. 124: Filter criteria

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

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

<i>inactive</i>	The filter criterion is ignored.
<i>equal</i>	<p>All conversations which exactly meet the entered value are displayed as filter result.</p> <p>Enter the value directly into the entry field via the keyboard.</p>
<i>in</i>	<p>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.</p> <p>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.</p> <p>To remove a value from the list, click on the icon x on the right of the value.</p>
<i>greater or equal</i>	<p>All conversations which meet the entered value or a larger value are displayed as filter result.</p> <p>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.</p>
<i>Period of time</i>	<p>All conversations which meet the entered value are displayed as filter result.</p> <p>Select the value from the drop-down list.</p>

8.2.2 Tab Details

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

Details

Conversation Criteria

Participant View Criteria

Session Criteria

Mi >

Name *

1w 10 min

Description

Conversations last week > 10 min

Creator

Admin, 1st-Tenant

Details*

Session Criteria

Mapping

Name *

Risk value

Description

(max. 255 characters)

Creator

Admin, 1st-Tenant

Number of sessions per high-risk agent*

(max. 2 characters)

10

Number of sessions per medium-risk agent*

(max. 2 characters)

5

Number of sessions per low-risk agent*

(max. 2 characters)

2

Last Name ↕


First Name ↕

Unger

Friedrich

Fig. 125: 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.
Number of sessions per high-risk agent	Number of sessions which are supposed to be evaluated for agents with a high risk profile. (Only available for risk value rule.)
Number of sessions per medium-risk agent	Number of sessions which are supposed to be evaluated for agents with a medium risk profile. (Only available for risk value rule.)
Number of sessions per low-risk agent	Number of sessions which are supposed to be evaluated for agents with a low risk profile. (Only available for risk value rule.)

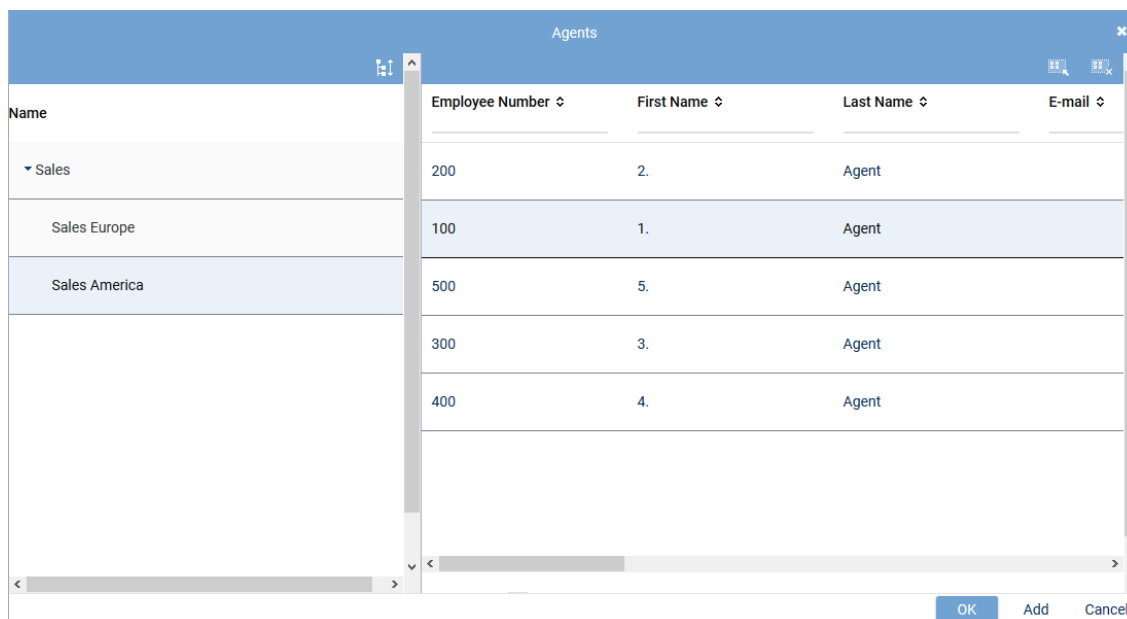
1. To assign agents from the organization structure, click on the icon  (Add from organization structure).

Last Name ↕First Name ↕

No records found



Fig. 126: Agents

2. Click on the organization unit on the left of the window.



Name	Employee Number	First Name	Last Name	E-mail
▼ Sales	200	2.	Agent	
Sales Europe	100	1.	Agent	
Sales America	500	5.	Agent	
	300	3.	Agent	
	400	4.	Agent	


Fig. 127: Add agents from organization structure

3. Select one or several agents from the list in the right window.
To select several agents or to revoke a selection, click on the respective line while holding the [Ctrl] key down.
To select all agents, click on the icon  (*Select all*).
To deselect all selected agents, click on the icon  (*Deselect all*).
4. To add the selected agents and leave the window open for further adjustments, such as adding more agents from other organization structures, click on the button *Add*.
To add selected agents and close the window, click on the button *OK*.
To discard the selection and close the window, click on the button *Cancel*.



You can only add agents to whose data you have access.

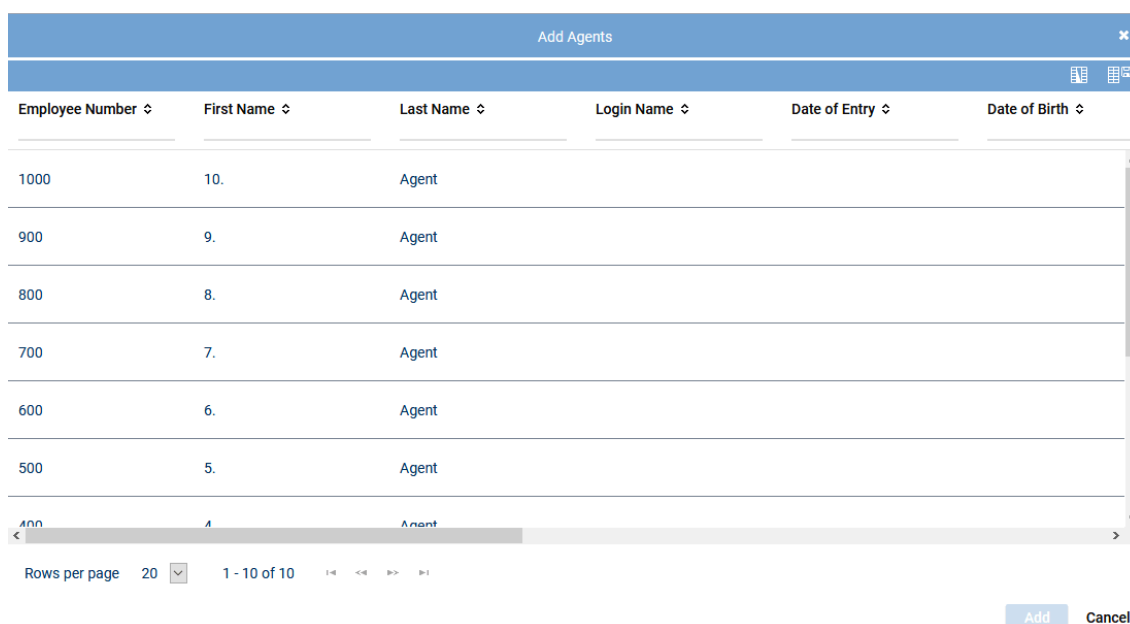
5. To assign an agent, click on the icon  (*Add*).



Last Name	First Name
No records found	

Fig. 128: Agents (example)

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




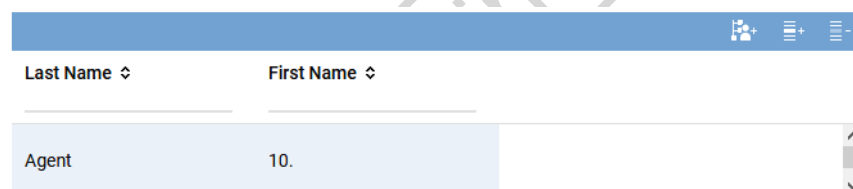
Employee Number	First Name	Last Name	Login Name	Date of Entry	Date of Birth
1000	10.	Agent			
900	9.	Agent			
800	8.	Agent			
700	7.	Agent			
600	6.	Agent			
500	5.	Agent			
400	4.	Agent			

Rows per page: 20 1 - 10 of 10

Add Cancel

Fig. 129: Add own agents

- To add the selected agents, click on the button **Add**.
To discard the selection and close the window, click on the button **Cancel**.
- To remove the assignment of an agent, select the respective agent in the list and click on the icon  (**Remove**).



Last Name	First Name
Agent	10.

Remove

Fig. 130: Remove agent assignment

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. 89](#).

<
Details
Conversation Criteria
Participant View Criteria
Session Criteria
Mi >

Conversation Information

Statistics of the Conversation

Calling Party Information

Called Party Information

1st-Connected Participant Information

Additional Data

General

Fig. 131: Conversation Rules module - tab Conversation Criteria

Group field Conversation Information

Conversation Information

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

Fig. 132: 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

Statistics of the Conversation

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

Fig. 133: Conversation criteria - Statistics of the Conversation (example)

Duration of Ringing Sections	Duration of ringing sections
-------------------------------------	------------------------------

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

Group field Calling Party Information

Calling Party Information ▼

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

Fig. 134: Conversation Criteria - Calling Party Information (example)



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

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

Group field Called Party Information

Called Party Information ▼

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

Fig. 135: Conversation Criteria - Called Party Information (example)

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

Group field 1st-Connected Participant Information

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

Fig. 136: Conversation Criteria - 1st-Connected Participant Information (example)

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

Group field Additional Data

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

Fig. 137: Conversation Criteria - Additional Data (example)

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

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

Group field General

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

Fig. 138: Conversation Criteria - General (example)

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

8.2.4 Tab Participant View Criteria

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

For information about how to define the different filter criteria see [chapter "Define filter criteria", p. 89](#).

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

Participant View Information ▶

Participant Information ▶

General ▶

Fig. 139: Conversation Rules module - tab Participant View Criteria

Group field Participant View Information

Participant View Information ▼

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

Fig. 140: Participant View Criteria - Participant View Information

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

Group field Participant Information

Participant Information ▼

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

Fig. 141: Participant View Criteria - Participant Information (example)

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

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

Group field General

General

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

Fig. 142: Participant View Criteria - General (example)

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

8.2.5

Tab Session Criteria

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

For information about how to define the different filter criteria see [chapter "Define filter criteria", p. 89](#).

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

Agent Information	▶
Time and Duration	▶
CTI Information	▶
Categories	▶
General	▶
Organization Units	▶

Fig. 143: Conversation Rules module - tab Session Criteria

Group field Agent Information

Agent Information

First name	equal	▼	9.
Last name	equal	▼	Agent

Fig. 144: Session Criteria - Agent Information (example)

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

Group field Time and Duration

Time and Duration

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

Fig. 145: Session Criteria - Time and Duration (example)

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

Group field CTI Information

CTI Information

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

Fig. 146: Session Criteria - CTI Information (example)

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

Group field Categories

Categories

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

Fig. 147: Session Criteria - Categories (example)

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

Group field General

General

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

Fig. 148: Session Criteria - General (example)

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

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

Group field Organization Units

Organization Units		
Of the agent	inactive	<input type="button" value="v"/>
Of the calling party	inactive	<input type="button" value="v"/>
Of the called party	inactive	<input type="button" value="v"/>
Of the 1st-connected	inactive	<input type="button" value="v"/>

Fig. 149: Session Criteria - Organization Units (example)

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

8.2.6

Tab Mapping

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

[Conversation Criteria](#)
[Participant View Criteria](#)
[Session Criteria](#)
[Mapping](#)

Mapping to Employees

First Name	Last Name
No records found	

Mapping to Roles

Name	Description
No records found	

Fig. 150: Conversation Rules module - tab Mapping

8.3

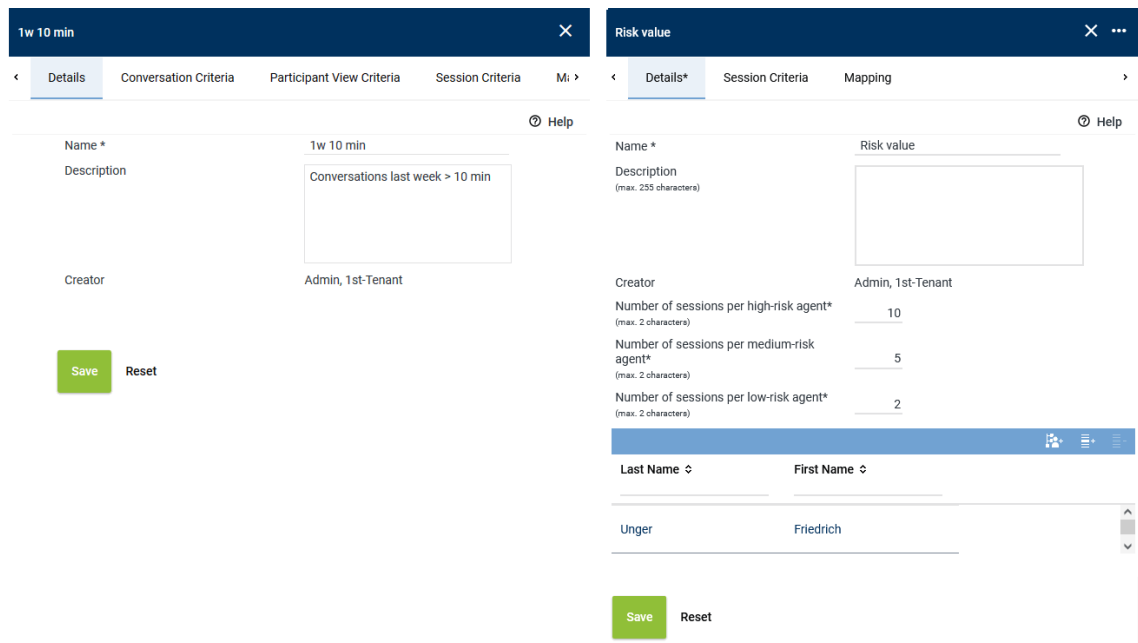
Create new conversation rule

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

<i>Create New</i>	Creates a new conversation rule.
<i>Create New Risk Value Rule</i>	A new conversation rule to evaluated conversations of agents with certain risk profiles is created.
<i>Create Clone</i>	<i>This function is currently not available.</i>

- Adjust the required settings in the tabs of the detail view, see [chapter "Detail view", p. 88](#). You can change tabs without buffering without risking to lose already entered data.

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



The image shows two side-by-side screenshots of the conversation rule configuration interface. The left window is titled '1w 10 min' and the right window is titled 'Risk value'. Both windows have a 'Details' tab selected. The '1w 10 min' window shows a 'Name' field with '1w 10 min', a 'Description' field with 'Conversations last week > 10 min', and a 'Creator' field with 'Admin, 1st-Tenant'. The 'Risk value' window shows a 'Name' field with 'Risk value', a 'Description' field, and a 'Creator' field with 'Admin, 1st-Tenant'. Below the 'Description' field in the 'Risk value' window, there are three input fields for session counts: 'Number of sessions per high-risk agent*' (10), 'Number of sessions per medium-risk agent*' (5), and 'Number of sessions per low-risk agent*' (2). At the bottom of each window are 'Save' and 'Reset' buttons.

Fig. 151: Save conversation rule

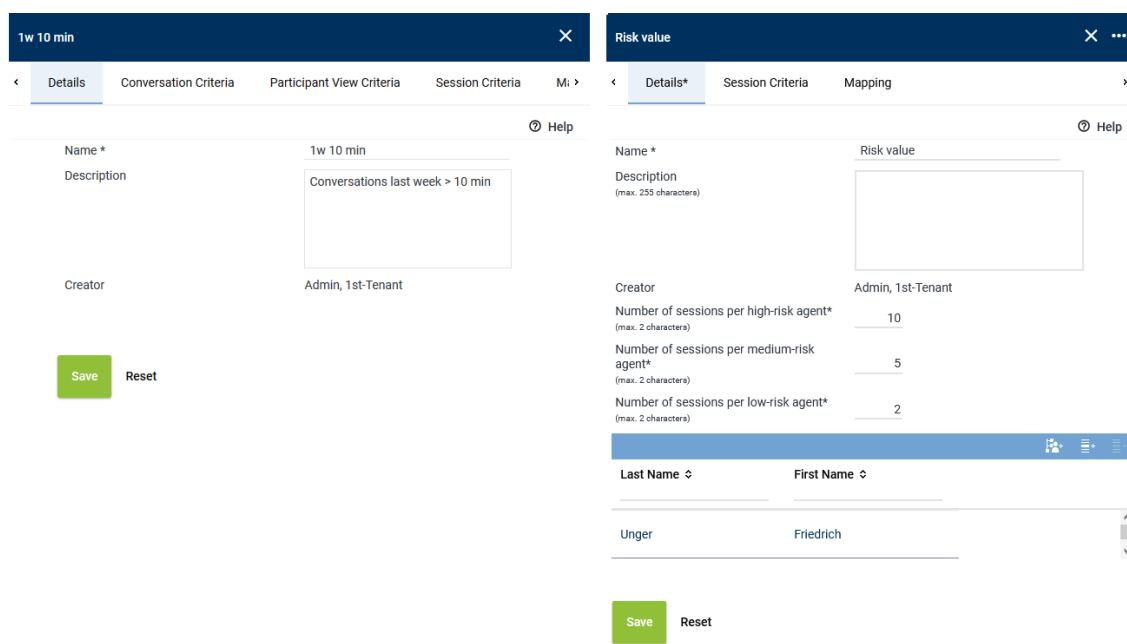
8.4

Edit conversation rule



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

- In the main view, select the conversation rule you would like to edit.
- Adjust the respective settings in the tabs of the detail view (see [chapter "Detail view", p. 88](#)).
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button **Save** to save the settings.
To discard the entries, click on the button **Reset**.



The figure displays two side-by-side screenshots of the 'Conversation Rules' configuration interface. Both windows have a dark blue header with a close button (X) and a help icon (i).

Left Screenshot (1w 10 min):

- Header:** 1w 10 min, X, Help
- Tabs:** Details (selected), Conversation Criteria, Participant View Criteria, Session Criteria, Mapping
- Form Fields:**
 - Name *: 1w 10 min
 - Description: Conversations last week > 10 min
 - Creator: Admin, 1st-Tenant
- Buttons:** Save (green), Reset


Right Screenshot (Risk value):

- Header:** Risk value, X, ...
- Tabs:** Details* (selected), Session Criteria, Mapping
- Form Fields:**
 - Name *: Risk value
 - Description: (max. 255 characters)
 - Creator: Admin, 1st-Tenant
 - Number of sessions per high-risk agent*: 10 (max. 2 characters)
 - Number of sessions per medium-risk agent*: 5 (max. 2 characters)
 - Number of sessions per low-risk agent*: 2 (max. 2 characters)
- User Selection:** A table with columns 'Last Name' and 'First Name'. The first row shows 'Unger' and 'Friedrich'.
- Buttons:** Save (green), Reset

Fig. 152: 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 rule 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. 103](#).

- **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. 104](#).

- **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. 104](#).

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. 104](#).

- **Superuser**

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

See [chapter "Create superuser", p. 105](#).

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. 42](#).
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. 58](#).
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. 59](#).



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. 59](#).

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. 58](#).
- 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. 53](#).
- 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. 73](#).
- 5. Click on the button *Save* to save the setting.

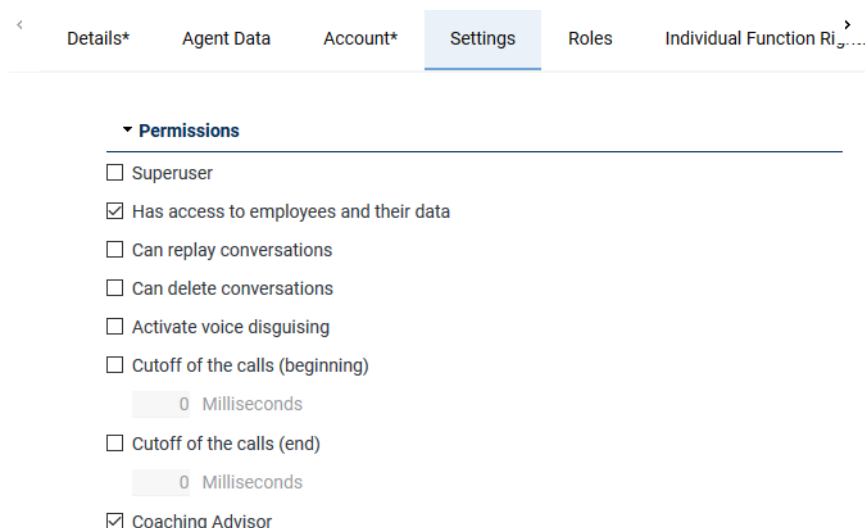


Alternatively, you can define a user as superior in the Employees module, see [chapter "Tab Organization Units", p. 64](#).

9.4

Create Coaching Advisor

- ✓ The user has the right *Has access to agents and their data*, see [chapter "Tab Settings", p. 53](#).
- 1. Open the Employees module.
- 2. In the main view, select the agent you would like to assign coaching advisor rights.
- 3. Click on the tab *Settings* in the detail view.
- 4. Open the group field *Permissions*.
- 5. Activate the check box in front of *Coaching Advisor*.



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

▼ Permissions

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

0 Milliseconds
- ☐ Cutoff of the calls (end)

0 Milliseconds
- ☒ Coaching Advisor

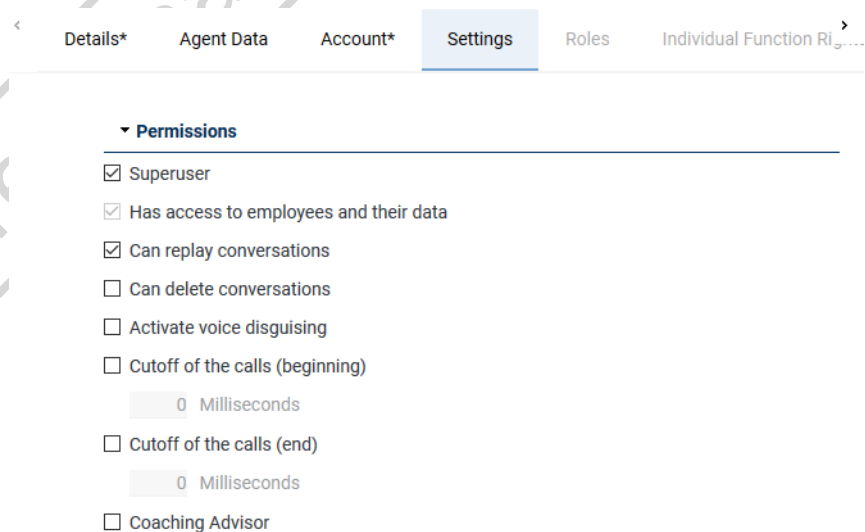
Fig. 153: Create Coaching Advisor

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*.



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

▼ Permissions

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

0 Milliseconds
- ☐ Cutoff of the calls (end)

0 Milliseconds
- ☐ Coaching Advisor

Fig. 154: 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.

Preliminary - For internal use only

List of figures

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

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

Fig. 84	Add organization units	66
Fig. 85	Delete organization unit assignment.....	66
Fig. 86	Save employee	67
Fig. 87	Organization Structure module - main view	69
Fig. 88	Organization Structure module - toolbar.....	69
Fig. 89	Organization Structure module - detail view	70
Fig. 90	Organization Structure module - tab Details.....	71
Fig. 91	Organization Structure module - tab Members.....	71
Fig. 92	Assign users	71
Fig. 93	Add user	72
Fig. 94	Delete user assignment	72
Fig. 95	Organization Structure module - tab Superiors	72
Fig. 96	Assign users	73
Fig. 97	Add user	73
Fig. 98	Delete user assignment	73
Fig. 99	Organization Structure module - tab Member Roles	74
Fig. 100	Organization Structure module - tab Superior Roles	74
Fig. 101	Save organization unit	75
Fig. 102	Save changes	75
Fig. 103	Roles module - main view.....	77
Fig. 104	Roles module - toolbar.....	77
Fig. 105	Roles module - detail view	78
Fig. 106	Roles module - tab Details.....	79
Fig. 107	Roles module - tab Employees.....	79
Fig. 108	Assign users	79
Fig. 109	Add user	80
Fig. 110	Delete user assignment	80
Fig. 111	Roles module - tab Function Rights (example).....	81
Fig. 112	Function rights - display sections (example)	81
Fig. 113	Function rights - Display function rights.....	82
Fig. 114	Roles module - tab Conversation Rules Object Rules.....	82
Fig. 115	Assign conversation rule.....	83
Fig. 116	Add conversation rules	83
Fig. 117	Delete conversation rule assignment.....	83
Fig. 118	Save role.....	84
Fig. 119	Save role.....	85
Fig. 120	Save changes	85
Fig. 121	Conversation Rules module - main view	87
Fig. 122	Conversation Rules module - toolbar	88
Fig. 123	Conversation Rules module - detail view	89
Fig. 124	Filter criteria	90
Fig. 125	Conversation Rules module - Tab Details	91

Fig. 126 Agents.....	91
Fig. 127 Add agents from organization structure.....	92
Fig. 128 Agents (example).....	92
Fig. 129 Add own agents.....	93
Fig. 130 Remove agent assignment.....	93
Fig. 131 Conversation Rules module - tab Conversation Criteria.....	94
Fig. 132 Conversation Criteria - Conversation Information (example).....	94
Fig. 133 Conversation criteria - Statistics of the Conversation (example).....	94
Fig. 134 Conversation Criteria - Calling Party Information (example)	95
Fig. 135 Conversation Criteria - Called Party Information (example).....	95
Fig. 136 Conversation Criteria - 1st-Connected Participant Information (example)	96
Fig. 137 Conversation Criteria - Additional Data (example)	96
Fig. 138 Conversation Criteria - General (example).....	96
Fig. 139 Conversation Rules module - tab Participant View Criteria.....	97
Fig. 140 Participant View Criteria - Participant View Information	97
Fig. 141 Participant View Criteria - Participant Information (example)	97
Fig. 142 Participant View Criteria - General (example)	98
Fig. 143 Conversation Rules module - tab Session Criteria	98
Fig. 144 Session Criteria - Agent Information (example).....	98
Fig. 145 Session Criteria - Time and Duration (example).....	99
Fig. 146 Session Criteria - CTI Information (example)	99
Fig. 147 Session Criteria - Categories (example).....	99
Fig. 148 Session Criteria - General (example)	99
Fig. 149 Session Criteria - Organization Units (example).....	100
Fig. 150 Conversation Rules module - tab Mapping.....	100
Fig. 151 Save conversation rule	101
Fig. 152 Save changes	102
Fig. 153 Create Coaching Advisor.....	105
Fig. 154 Create superuser	105

List of tables

Tab. 1	Function rights	61
Tab. 2	Function rights INSPIRATIONneo > Evaluation templates.....	61
Tab. 3	Function rights player	62
Tab. 4	Function rights	82

Preliminary - For internal use only

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 Socket 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.