

System Configuration

User management



Administration manual

for system providers

3/17/2020

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

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

Copyright © 2019 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	10
3.1	Install certificate	10
3.2	Troubleshooting	11
4	Tenants module.....	12
4.1	Main view	12
4.1.1	Toolbar	12
4.2	Detail view.....	13
4.2.1	Detail view for the tenant account of the system provider.....	13
4.2.2	Detail view for normal tenants.....	14
4.2.3	Detail view for resellers	16
4.2.4	Tab Details	16
4.2.4.1	Add time zone	18
4.2.4.2	Group field System Availability.....	19
4.2.4.3	Group field Address	20
4.2.4.4	Group field Contact Person.....	21
4.2.5	Tab Extensions	21
4.2.5.1	Add extensions.....	22
4.2.5.2	Remove extensions.....	24
4.2.6	Tab PBX Agent IDs	25
4.2.6.1	Add PBX Agent ID.....	26
4.2.6.2	Remove PBX Agent ID.....	27
4.2.7	Tab Chat IDs	28
4.2.7.1	Add chat ID	29
4.2.7.2	Remove chat ID	30
4.2.8	Tab Passwords	31
4.2.8.1	Edit entry	36
4.2.9	Tab General Settings	36
4.2.9.1	Group field Inactivity.....	36
4.2.9.2	Group field SMTP Account.....	37
4.2.9.3	Group field SNMP Agent.....	38
4.2.9.4	Group field Login Settings.....	40
4.2.9.5	Group field Miscellaneous Settings.....	42
4.2.10	Tab LDAP Connection Data.....	42
4.2.10.1	Edit LDAP connection data	43
4.2.11	Tab Web Service.....	44
4.2.11.1	Configure web service for the system provider	44
4.2.11.2	Configure Web Service for the tenant	46
4.2.11.3	Path of the WSDL file.....	50

4.2.11.4	Configure Web Service for the reseller	50
4.2.12	Tab PBX.....	52
4.2.12.1	Assign PBX	52
4.2.12.2	Remove PBX assignment	53
4.2.13	Tab System Licenses.....	54
4.3	Create new tenants manually.....	55
4.4	Edit tenants manually	56
4.5	Delete tenant.....	57
5	Employees module	58
5.1	Main view	58
5.1.1	Toolbar	59
5.1.1.1	Show summary	60
5.1.1.2	Show locked employees	60
5.1.1.3	Make employee visible or not visible.....	61
5.1.1.4	Search.....	61
5.2	Detail view	62
5.2.1	Tab Details	62
5.2.1.1	Group field Employee Information.....	63
5.2.1.2	Group field Address	65
5.2.1.3	Group field Privacy and Terms.....	66
5.2.2	Tab Account	67
5.2.2.1	Authentication via LDAP	68
5.2.2.2	Assign combination user.....	68
5.2.2.3	Delete combination user assignment.....	69
5.2.3	Tab Settings	69
5.2.3.1	Group field Permissions	70
5.2.3.2	Group field Logging Settings.....	71
5.2.4	Tab Roles.....	71
5.2.4.1	Assign roles.....	71
5.2.4.2	Delete role assignment	72
5.2.5	Tab Individual Function Rights.....	72
5.3	Create new employee	74
5.4	Edit employee	74
5.5	Delete employee	75
6	Roles module.....	76
6.1	Main view	76
6.1.1	Toolbar	76
6.2	Detail view	77
6.2.1	Tab Details	78
6.2.2	Tab Employees	78
6.2.2.1	Assign users.....	78
6.2.2.2	Delete user assignment	79

6.2.3	Tab Function Rights	79
6.3	Create new role	81
6.4	Duplicate role	81
6.5	Edit role	82
6.6	Delete role	82
7	Predefined function packages	84
7.1	Create superuser	84
7.2	Create superadmin	84
	List of figures	86
	List of tables	89
	Glossary	90

1 General information

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

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

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

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

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

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

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

2 Introduction

The *neo* system has been designed as a potential multi-tenant system. This means several different tenants can be administered within one system. These tenants are created and administered by the system provider or by a reseller. The administrators of the particular tenants have the possibility to create users, define roles and administrate function rights (refer to administration manual *System Configuration - User management (for system providers)*).

Every *neo* system is initially installed as a 1-tenant system with one predefined tenant, the *1st tenant*. For the system provider, a tenant is created automatically, too. However, the system provider cannot be considered a tenant in the true sense of the word.

For the respective administrators of the system provider and of the predefined tenant, an account with the following login data is created during the installation of the system by default:

Login data for the administrator of the system provider:

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

Tab. 1: Login data - system provider

Login data for the administrator of the 1st tenant:

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

Tab. 2: Login data - 1st tenant

Depending on the licensing, the *neo* recording system is operated as a *1-tenant system* or as a *multi-tenant system*. In a *1-tenant system*, there is only the predefined tenant; no other tenants can be created. In a multi-tenant system, the system provider can create as many additional tenants as there are tenant licenses in the system.

System provider

The system provider is responsible for the general system configuration.

The system provider can:

- create, delete, and administrate subordinated tenants or resellers.
- create his own employees as system users and administrate and delete them.

The system provider has no access to the user data of the individual tenants. Only the tenant himself can view and edit tenant-specific data.

Reseller

A reseller has a restricted set of rights that system providers and tenants have.

A reseller can:

- create, delete, and administrate subordinated tenants and resellers.
- create his own employees as system users and administrate and delete them.

A reseller has no access to the user data of the individual tenants. Only the tenant himself can view and edit tenant-specific data.

Tenant

A tenant is the final customer.

A tenant can:

- create his own employees as system users and administrate and delete them.

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

- Create and administrate tenants and resellers
- Create and administrate own users
- Administrate function rights for your own users
- Set up LDAP authentication for your own users

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 create tenants and resellers and administrate their data.

See [chapter "Tenants module", p. 12.](#)

- Employees module

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

See [chapter "Employees module", p. 58.](#)

- 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.](#)



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.



If you change users' function rights or their assigned roles 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 or roles have been changed.



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

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

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

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

- Configure **LDAP** connection data.
See chapter "Tab LDAP Connection Data", p. 42.
- Always activate **LDAP** authentication.
See chapter "Group field Login Settings", p. 40.
- Activate **LDAP** authentication for individual users.
See chapter "Authentication via LDAP", p. 68.



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



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




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

3.1

Install certificate

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

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

3.2

Troubleshooting

LDAP SSL connection does not work

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

4 Tenants module

In the Tenants module, you can create tenants or resellers and administrate their data. Here, the contact data and the assigned extensions are administrated.

The *neo* system has been designed as a potential multi-tenant system. Every system is initially installed as a 1-tenant system with one predefined tenant, the *1st tenant*. For the system provider, a tenant is created automatically, too (tenant name = *System*). However, the system provider cannot be considered a tenant in the true sense of the word. Depending on the available licenses, you can create additional tenants or resellers here in the Tenants module. New tenants and resellers can be created automatically via the Web Service or manually.

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, all saved tenants are displayed.

+ × Tenants General ▾					
Name ▲	Customer ID ⇅	Type	Country ⇅	Creation Date ⇅	Updated ⇅
▼ System		System provider		02/28/2011 3:20:52 PM	11/06/2018 11:56:38 AM
1st-tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM
2nd-Tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM
3rd-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>	Customer ID 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>Add</i>	Creates a new tenant or reseller (see chapter "Create new tenants manually", p. 55).
	<i>Delete</i>	Deletes the selected tenant (see chapter "Delete tenant", p. 57).
<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.

Module Help

By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.



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

4.2 Detail view

The detail view contains additional information about and functions of the selected tenant or reseller. The content of the detail view depends on whether the tenant account of the system provider or of any other tenant has been selected in the main view.

The tab *Details* is the same for all tenants/resellers, regardless of whether it is the tenant account of the system provider or of a normal tenant/reseller.

4.2.1 Detail view for the tenant account of the system provider

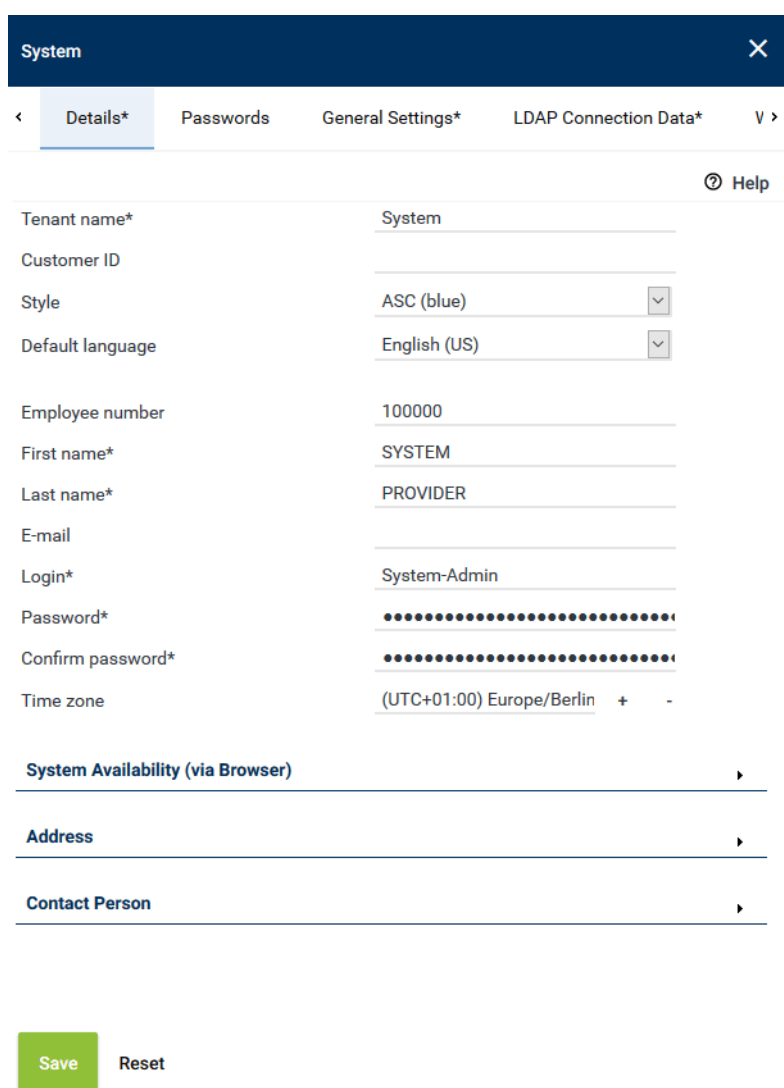


Fig. 3: Tenants module - detail view for the tenant "System"

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. 16](#).
- *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. 31](#).

- *General Settings*

Here, you can configure the general settings (inactivity, notification settings, SSO login).

See [chapter "Tab General Settings", p. 36](#).

- *LDAP Connection Data*

Here, you can configure [LDAP](#) connections.

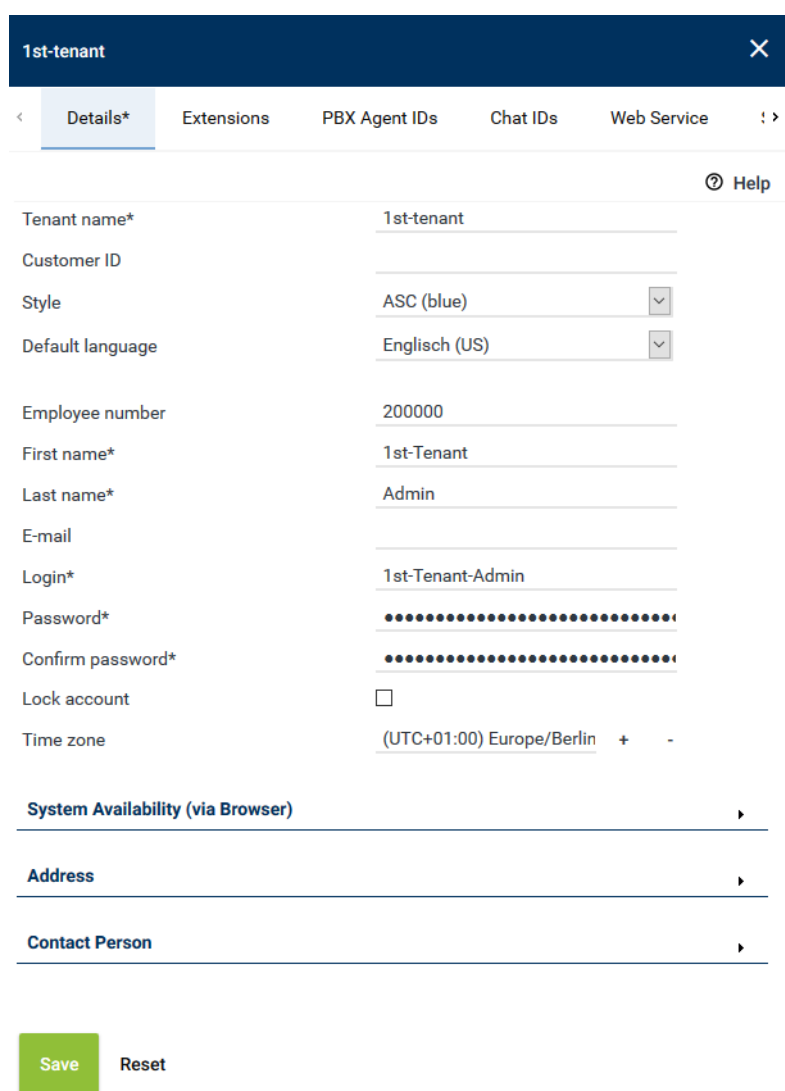
See [chapter "Tab LDAP Connection Data", p. 42](#).

- *Web Service*

Here, you can configure the usage of the Web Service.

See [chapter "Tab Web Service", p. 44](#).

4.2.2 Detail view for normal tenants



1st-tenant ✕

< **Details*** Extensions PBX Agent IDs Chat IDs Web Service >

🔗 Help

Tenant name*	1st-tenant
Customer ID	
Style	ASC (blue) ▼
Default language	Englisch (US) ▼
Employee number	200000
First name*	1st-Tenant
Last name*	Admin
E-mail	
Login*	1st-Tenant-Admin
Password*
Confirm password*
Lock account	<input type="checkbox"/>
Time zone	(UTC+01:00) Europe/Berlin + -

System Availability (via Browser) ▶

Address ▶

Contact Person ▶

Save **Reset**

Fig. 4: Tenants module - detail view for normal tenants

The detail view consists of the following tabs:

- *Details*

Here, you can display and edit the contact and the login data of the tenant.

See [chapter "Tab Details", p. 16.](#)

- *Extensions*

Here, you can display and administrate the extensions which have been assigned to the tenant.

See [chapter "Tab Extensions", p. 21.](#)

- *PBX Agent IDs*

Here, you can display and administrate the PBX Agent IDs which have been assigned to the tenant.

See [chapter "Tab PBX Agent IDs", p. 25.](#)

- *Chat IDs*

Here, you can display and administrate the chat IDs which have been assigned to the tenant.

See [chapter "Tab Chat IDs", p. 28.](#)

- *Web Service*

Here, you can activate the functions of the Web Service.

See [chapter "Tab Web Service", p. 44.](#)

- *System Licenses*

Here, you can activate modules and functionalities to be used by tenants.

See [chapter "Tab System Licenses", p. 54.](#)

4.2.3 Detail view for resellers

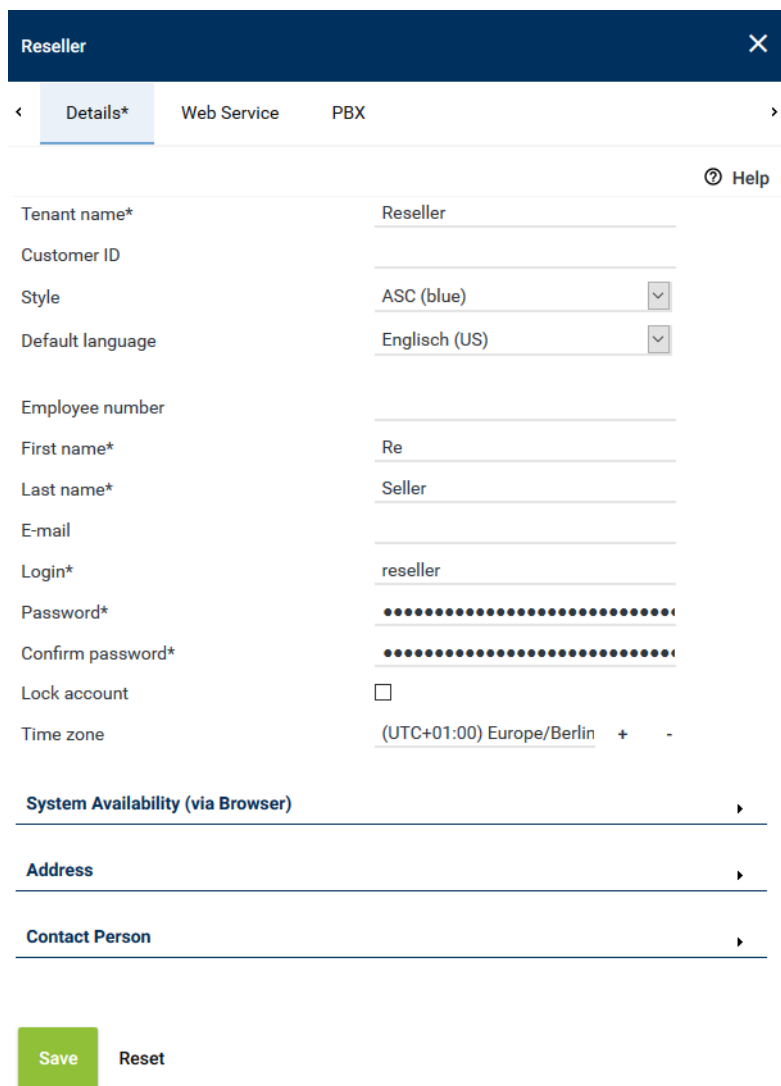


Fig. 5: Tenants module - detail view for resellers

The detail view consists of the following tabs:

- **Details**
Here, you can display and edit the contact and the login data of the reseller.
See [chapter "Tab Details", p. 16.](#)
- **Web Service**
Here, you can activate the functions of the Web Service.
See [chapter "Tab Web Service", p. 44.](#)
- **PBX**
Here, you can activate and administrate **PBX** filters which have been assigned to the selected tenant.
See [chapter "Tab PBX", p. 52.](#)

4.2.4 Tab Details

Here, you can display and edit the contact and the login data of the selected tenant or reseller.

The tab *Details* is the same for all tenants/resellers, regardless of whether it is the tenant account of the system provider or of a normal tenant/reseller.

1st-tenant

<

Details*

Extensions

PBX Agent IDs

Chat IDs

Web Service

>

Help

Tenant name*

1st-tenant

Customer ID

Style

ASC (blue)

Default language

Englisch (US)

Employee number

200000

First name*

1st-Tenant

Last name*

Admin

E-mail

Login*

1st-Tenant-Admin

Password*

Confirm password*

Lock account

☐

Time zone

(UTC+01:00) Europe/Berlin + -

System Availability (via Browser)

Address

Contact Person

Save



Reset

Fig. 6: Tenants module - detail view for normal tenants

1. Enter the following information in the general section:

- General information about the tenant profile
- Personal data of the administrator of the tenant
- Login data for the administrator of the tenant

<i>Tenant name</i>	Name which is displayed for the tenant in the system.
<i>Customer ID</i>	Enter the customer ID.
<i>Style</i>	Layout in which the tenant sees the user interface of the system. Select one of the available layouts from the drop-down list.
<i>Default language</i>	Language in which the user interface of the system is displayed for the tenant. Select the language from the drop-down list.
<i>Employee number</i>	Employee number of the administrator of the tenant.
<i>First name</i>	First name of the administrator of the tenant.
<i>Last name</i>	Last name of the administrator of the tenant.
<i>E-mail</i>	E-mail address of the administrator of the tenant.
<i>Login</i>	User name of the administrator of the tenant.


<i>Password</i>	Password which is required for the administrator of the tenant to log in to the system.
<i>Confirm password</i>	Repetition of the password for the administrator.
<i>Lock account</i>	<p>This option allows locking the tenant's account. The tenant can then no longer log in to <i>neo</i>.</p> <p>NOTICE!</p> <p>This option locks the account of exclusively this tenant. The lock does not extend to the users of the tenants. This means that the users of the tenant can continue to log in to <i>neo</i>.</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 individual employee. The configuration in the Employees module is prioritized.</p> <p>To select the time zone, click on the button . See chapter "Add time zone", p. 18.</p> <p>To delete the selection, click on the button .</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.

4.2.4.1

Add time zone

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

Fig. 7: Add time zone

2. To filter the list of entries in the table, enter the character sequence you would like to filter for in the filter field under the column headline *Continent/Region*.
 - ⇒ The table only displays entries in this column containing the character sequence.

Example:

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

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

Fig. 8: The displayed entries in the table are filtered for *ber* (example)

3. Select a time zone from the list.

Time zone	
Time Difference ↕	Continent/Region ↕
UTC-12:00	Etc/GMT+12
UTC-11:00	Pacific/Pago_Pago
UTC-11:00	Pacific/Samoa
UTC-11:00	Pacific/Niue
UTC-11:00	US/Samoa
UTC-11:00	Etc/GMT+11
UTC-11:00	Pacific/Midway
<div> Rows per page 20 ▾ 1 - 20 of 616 </div>	
<div> Add Cancel </div>	

Fig. 9: Add time zone

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

4.2.4.2 Group field System Availability

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



Fig. 10: Add system availability

2. In the title bar of the group field, click on the button  *System Availability (via Browser)*.

3. Enter the addresses you would like to use.

System Availability (via Browser) ▼

⊖ System Availability (via Browser)

Internal IP address / Internal port : 443

DNS name

External IP address / External port :

External DNS name

Fig. 11: Configure system availability

<i>Internal IP address/ Internal port</i>	Enter the destination IP address and the port of the replay server at which the Replay module can be reached internally.
<i>DNS name</i>	Enter the DNS name which can be used to reach the Replay module internally.
<i>External IP address/ External port</i>	Enter the URL or the IP address and the port at which the Replay module can be reached via the browser from outside.
<i>External DNS name</i>	Enter the external DNS name which can be used to reach the Replay module via the browser from the outside. NOTICE! If the SSL certificate has been issued for a DNS address, it is imperative to enter the DNS name! Otherwise the certificate check in the replay applications will fail.



To allow the users of the respective tenant to access the replay server via the browser, an internal IP address and/or an external IP address must be configured in the Servers module, too. The addresses 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*.

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

4.2.4.3 Group field Address

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

Address ▼

+ Add Address

Fig. 12: Add address

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

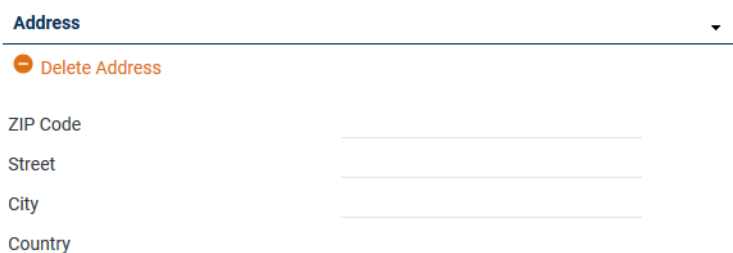



Fig. 13: Add address


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

4.2.4.4 Group field Contact Person

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



Fig. 14: Add contact person

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

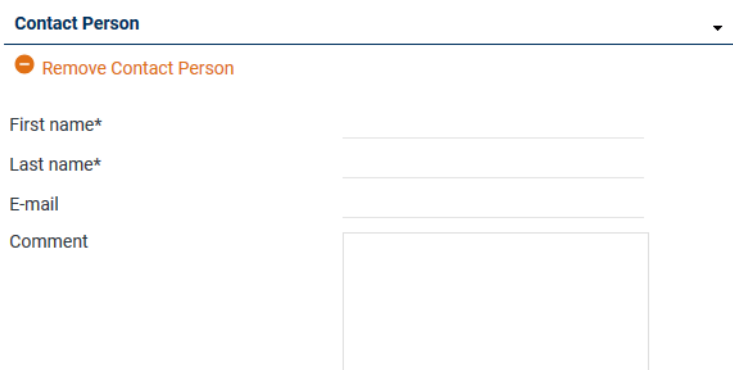



Fig. 15: Add contact person



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

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

4.2.5 Tab Extensions

Here, you can display and administrate the extensions which have been assigned to the selected tenant.



In 1-tenant systems, all extensions are automatically assigned to the tenant who has been created by the system (1st tenant). Extensions are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.



In multi-tenant systems, you have to assign the extensions manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of extensions is not possible until a PBX has been created since extensions are assigned in relation to the PBX.

<div> <div><</div> <div>Details*</div> <div>Extensions</div> <div>PBX Agent IDs</div> <div>Chat IDs</div> <div>Web Service</div> <div>></div> </div>	
PBX	Extensions
SIP	111
SIP_	user1, user10, user2, user3, user4, user5, user6,...
<div> <div>Add</div> <div>Administrate</div> </div>	

Fig. 16: Tenants module - tab Extensions

- To assign new extensions to a tenant, proceed as described in [chapter "Add extensions"](#), p. 22.
- To remove assigned extensions, proceed as described in [chapter "Remove extensions"](#), p. 24.
- To remove a [PBX](#) from the assignment, remove all assigned extensions of this [PBX](#). That way, the assignment of the [PBX](#) is deleted.

4.2.5.1 Add extensions

1. In the main view, select the tenant to whom you would like to assign extensions.
2. Click on the tab *Extensions*.
3. Click on the button *Add*.
 - ⇒ The following window appears:

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

Extension or extension range separated by
", or "; (e. g. 3434,3535; 4000-4100)

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 17: Assign extensions to tenants

4. From the drop-down list, select the PBX in which the extensions for this tenant have been configured.

<i>File import</i>	<p>Select this option to import extensions from an existing CSV file and add them to the table of extensions.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CVS file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p> <p>Enter the extension range that is reserved for this tenant using a hyphen, e. g. from 6000 to 6999. Alphanumerical entries with a hyphen are not detected as a range, they must be entered individually.</p> <p>You can separate the different extensions and extension ranges by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of extensions</i>	<p>Activate the check box to replace the list of extensions.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the extensions of the selected PBX.</p>

☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
⇒ The extensions are added in the table of extensions.
6. If errors have been detected, the window *Result* appears.
Click on the button *Display Error Report* to open the window *Error Report*.
To close the window *Error Report*, click on the button *Close*.
To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

4.2.5.2 Remove extensions

1. In the list, select the **PBX** for which you would like to remove the assigned extensions.

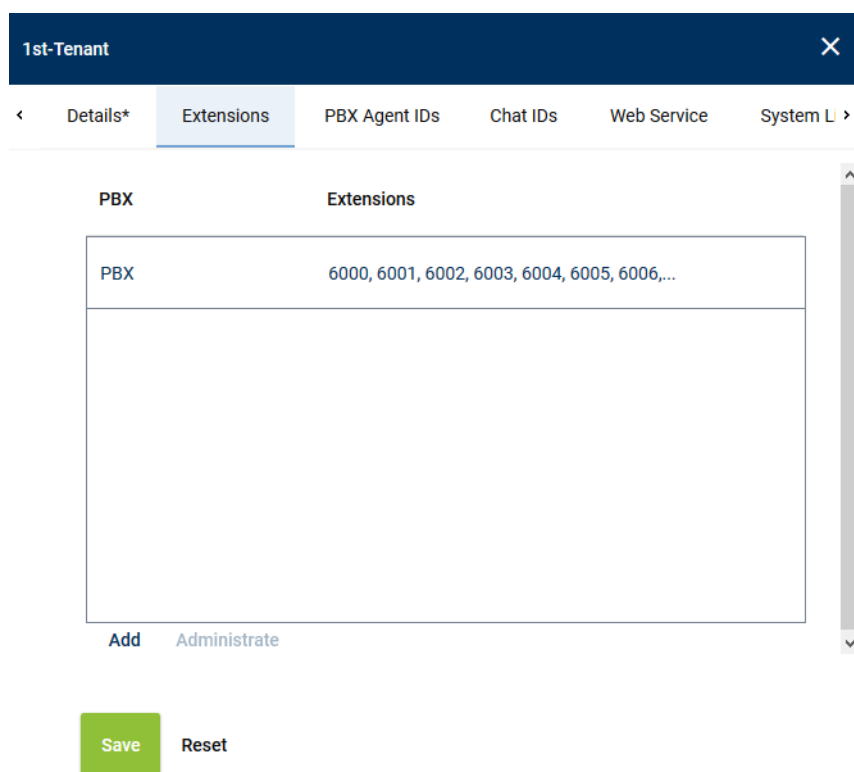


Fig. 18: Remove extensions

2. Click the button *Administrate*.
3. Select one or several extensions you would like to remove from the assignment.
To select several extensions or to revoke the selection, click on the respective line while holding the [Ctrl] key down.



Fig. 19: Select extensions

4. To remove the selected extensions, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

4.2.6 Tab PBX Agent IDs

Here, you can display and administrate the PBX Agent IDs which have been assigned to the selected tenant.



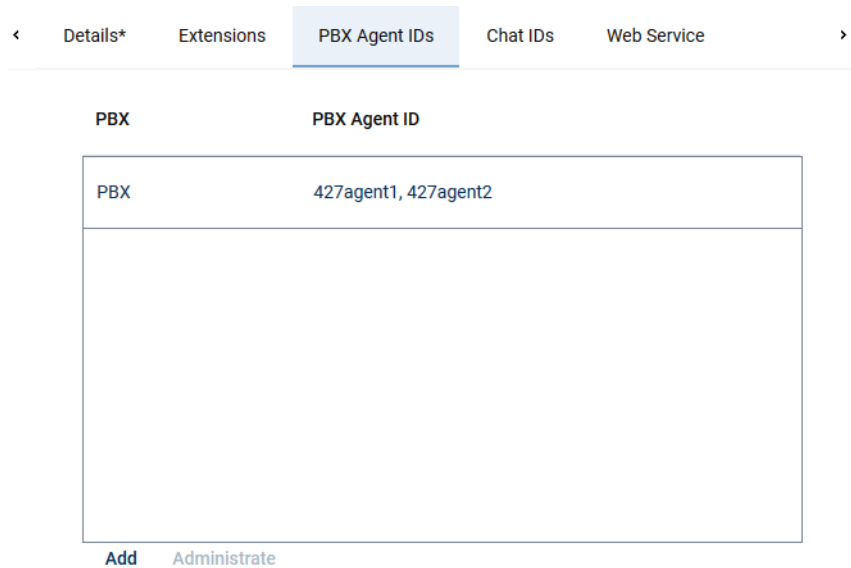
In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

When installing a 1-tenant system, you can skip this chapter.



In multi-tenant systems, you have to assign the PBX Agent IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of PBX Agent IDs is not possible until a PBX has been created since the assignment is PBX-related.



PBX	PBX Agent ID
PBX	427agent1, 427agent2

[Add](#) [Administrate](#)

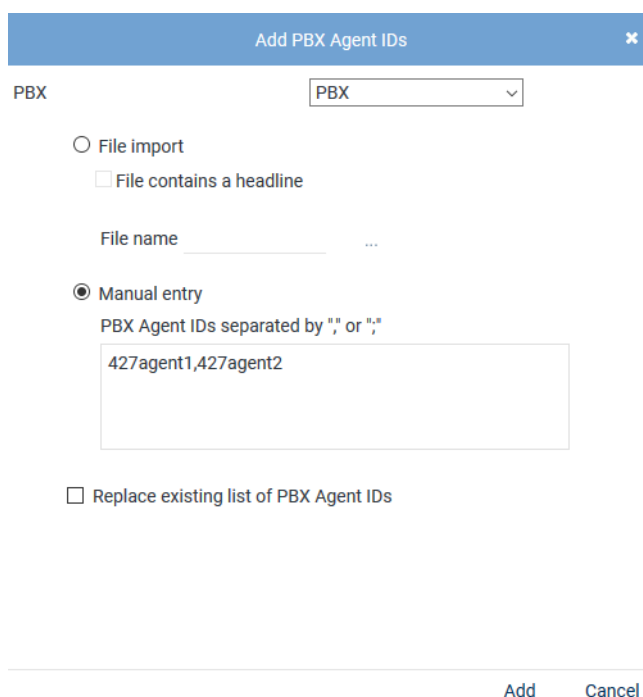
Fig. 20: Tenants module - tab PBX Agent ID

- To assign new PBX Agent IDs to a tenant, proceed as described in [chapter "Add PBX Agent ID", p. 26](#).
- To remove assigned PBX Agent IDs, proceed as described in [chapter "Remove PBX Agent ID", p. 27](#).
- To remove a [PBX](#) from the assignment, remove all assigned PBX Agent IDs of this [PBX](#). That way, the assignment of the [PBX](#) is deleted.

4.2.6.1 Add PBX Agent ID

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

⇒ The following window appears:



Add PBX Agent IDs

PBX
PBX

☐ File import
☐ File contains a headline
File name ...



☒ Manual entry
PBX Agent IDs separated by ";" or ","
427agent1,427agent2

☐ Replace existing list of PBX Agent IDs

Add Cancel

Fig. 21: Assign PBX Agent IDs to tenants

4. From the drop-down list, select the PBX in which the PBX Agent IDs for this tenant have been configured.

<i>File import</i>	<p>Select this option to import the PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter PBX Agent IDs manually.</p> <p>You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of PBX Agent IDs</i>	<p>Activate the check box to replace the list of PBX Agent IDs.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX.</p> <p><input type="checkbox"/> = Function has not been activated; the configured PBX Agent IDs of all PBXs are kept and the new PBX Agent IDs are added to the selected PBX.</p>

5. Click on the button *Add*.
 - ⇒ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detected, the window *Result* appears.
 - Click on the button *Display Error Report* to open the window *Error Report*.
 - To close the window *Error Report*, click on the button *Close*.
 - To close the window *Result*, click on the button *Close*.
7. The configured PBX Agent IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

4.2.6.2 Remove PBX Agent ID

1. In the list, select the [PBX](#) for which you would like to remove the assigned PBX Agent IDs.
2. Click the button *Administrate*.
3. Select one or several PBX Agent IDs you would like to remove from the assignment.
 - To select several PBX Agent IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

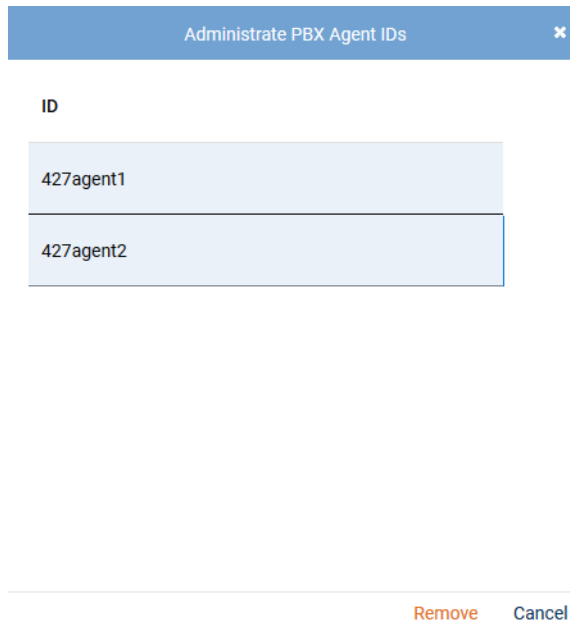


Fig. 22: Select PBX Agent IDs

4. To remove the selected PBX Agent IDs, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

4.2.7 Tab Chat IDs

Here, you can display and administrate the chat IDs which have been assigned to the selected tenant.

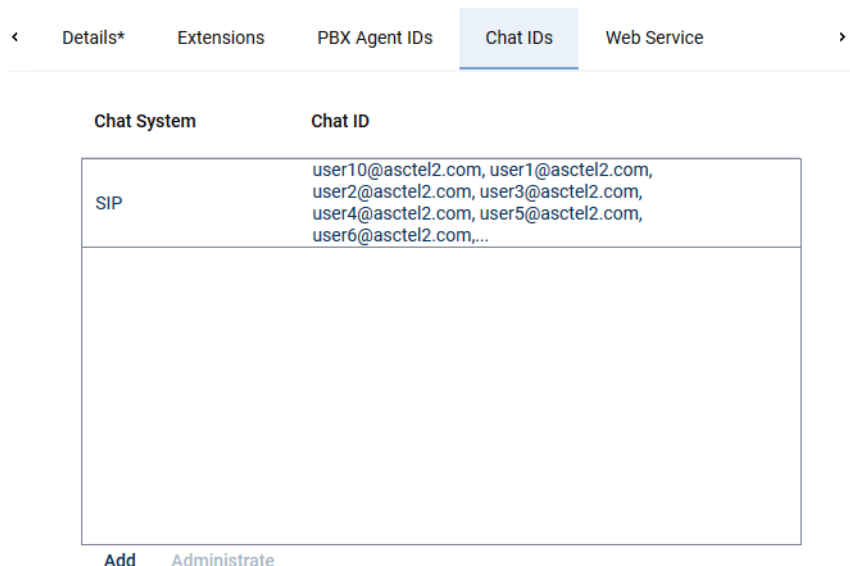


In 1-tenant systems, the chat IDs are automatically assigned to the tenant who has been created by the system (1st tenant). Chat IDs are assigned to the user in the Employees module. When installing a 1-tenant system, you can skip this chapter.



In multi-tenant systems, you have to assign the chat IDs manually to each tenant who is supposed to be able to use them. There are multi-tenant systems, too, in which only 1 tenant has been set up.

The manual assignment of chat IDs is not possible until a chat system has been created in the PBX module since the assignment is PBX-related.



Chat System	Chat ID
SIP	user10@asctel2.com, user1@asctel2.com, user2@asctel2.com, user3@asctel2.com, user4@asctel2.com, user5@asctel2.com, user6@asctel2.com,...

[Add](#) [Administrate](#)

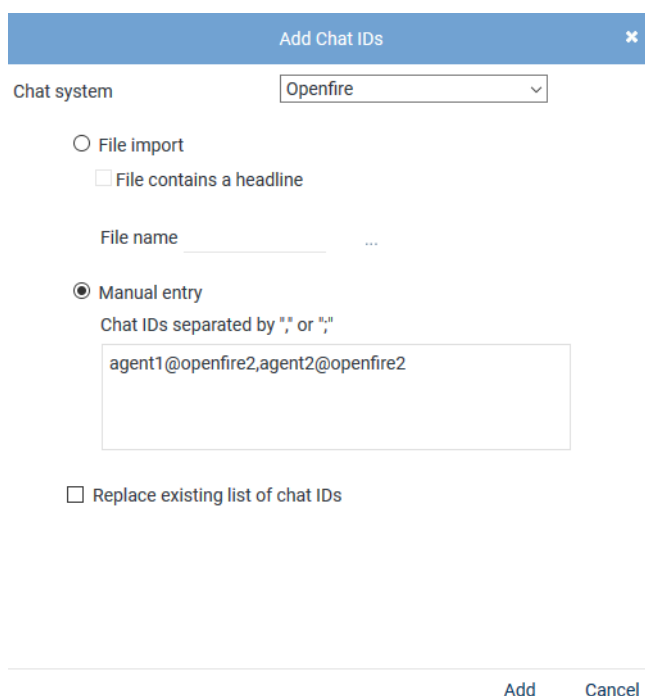
Fig. 23: Tenants module - tab Chat IDs

- To assign new chat IDs to a tenant, proceed as described in [chapter "Add chat ID", p. 29](#).
- To remove assigned chat IDs, proceed as described in [chapter "Remove chat ID", p. 30](#).
- To remove a chat system, from the assignment, remove all assigned chat IDs of this PBX. That way, the assignment of the chat system is deleted.

4.2.7.1 Add chat ID

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

⇒ The following window appears:



Add Chat IDs [X]

Chat system: Openfire

☐ File import

☐ File contains a headline

File name: _____

☒ Manual entry

Chat IDs separated by ";" or ","



agent1@openfire2,agent2@openfire2

☐ Replace existing list of chat IDs

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

Fig. 24: Assign chat IDs to tenants

4. From the drop-down list, select the chat system in which the chat IDs for this tenant have been configured.

<i>File import</i>	<p>Select this option to import the chat IDs from an existing CSV file and add them to the table of chat IDs.</p> <p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The CSV file may not contain more than 1 column. If commas or other column delimiters are found in the CSV file, then the file is not valid and an error message appears.</p> <p>Only ZIP files are supported as file format. To be able to import a CSV file, you have to pack it in a ZIP file.</p> <p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> • Click on the button  behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective ZIP file via the Explorer and click on the button <i>Open</i>. • Click on the button  <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter chat IDs manually.</p> <p>You can separate the individual chat IDs by means of the delimiters displayed in the screenshot. The chat address must be identical to the entries in the agent data in the Employees module and must contain the name of the corresponding domain.</p> <p>NOTICE! Wildcards cannot be used!</p>
<i>Replace existing list of chat IDs</i>	<p>Activate the check box to overwrite existing chat IDs. If you use several chat systems, only the list of the selected chat system will be overwritten.</p> <p><input checked="" type="checkbox"/> = Function has been activated; the entry replaces the chat IDs of the selected chat system.</p> <p><input type="checkbox"/> = Function has not been activated; the configured chat IDs are kept and the new chat IDs are added to the selected chat system.</p>

5. Click on the button *Add*.
 - ⇒ The chat IDs are added to the table of chat IDs.
6. If errors have been detected, the window *Result* appears.
 - Click on the button *Display Error Report* to open the window *Error Report*.
 - To close the window *Error Report*, click on the button *Close*.
 - To close the window *Result*, click on the button *Close*.
7. The configured chat IDs now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

4.2.7.2 Remove chat ID

1. In the list, select the chat system for which you would like to remove the assigned chat IDs.
2. Click the button *Administrate*.
3. Select one or several chat IDs you would like to remove from the assignment.
 - To select several chat IDs or to revoke the selection, click on the respective line while holding the [Ctrl] key down.

Administrare Chat IDs
✕

ID

agent1@openfire2

agent2@openfire2

Remove Cancel

Fig. 25: Select chat IDs

4. To remove the selected chat IDs, click on the button *Remove*.
To cancel the process and close the window, click on the button *Cancel*.

4.2.8 Tab Passwords

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

<
Details*
Passwords
General Settings*
LDAP Connection Data*
Web Servi >

Password Length	▸
Mandatory Characters	▸
Security	▸
Forbidden Passwords	▸
Advanced Password Settings	▸

Fig. 26: Tenants module - tab Passwords

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

Exceptions:

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

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

- Authentication takes place via [LDAP](#)
- The user is a superuser


- The following option has been activated for the user account:
Does not have to meet the password rules

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




Defining password rules is optional.



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


Group field Password Length

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




The screenshot shows the 'Password Length' group field interface. At the top, there is a title bar with the text 'Password Length' and a dropdown arrow. Below the title bar, there is a button with a minus icon and the text 'Remove password length'. Below this, there are two input fields. The first is labeled 'Minimum length' with a sub-label '(max. 3 characters)' and contains the value '1'. The second is labeled 'Maximum length' with a sub-label '(max. 3 characters)' and contains the value '256'.

Fig. 27: Define password length

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

Group field Mandatory Signs

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


Mandatory Characters

 Remove mandatory characters


Max. character repetition (max. 3 characters)	256
Min. number of Letters (max. 3 characters)	2
Digits (max. 3 characters)	2
Punctuation characters (max. 3 characters)	1
Lower-case letters (max. 3 characters)	0
Upper-case letters (max. 3 characters)	0

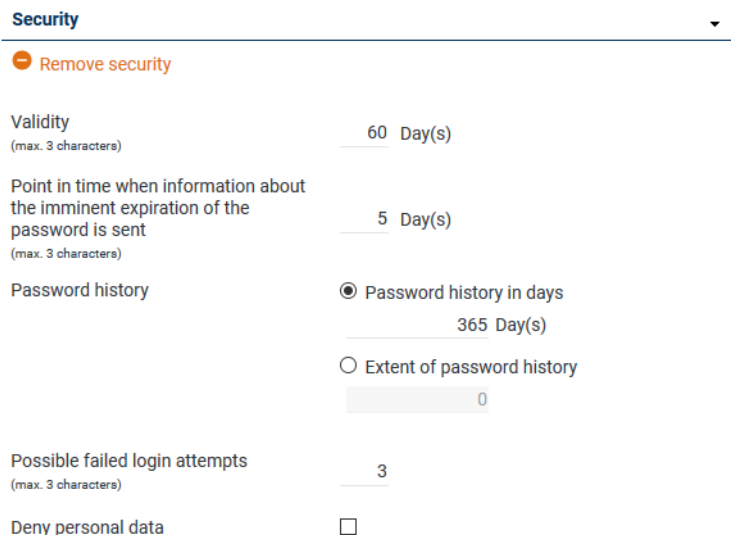
Fig. 28: Define mandatory characters

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

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.




The screenshot shows the 'Security' configuration page. At the top, there is a title bar with a dropdown arrow and a 'Remove security' button. Below this, several configuration fields are visible:

- Validity** (max. 3 characters): A text input field containing '60' followed by 'Day(s)'.
- Point in time when information about the imminent expiration of the password is sent** (max. 3 characters): A text input field containing '5' followed by 'Day(s)'.
- Password history**: Two radio button options. The first is 'Password history in days' with a value of '365 Day(s)'. The second is 'Extent of password history' with a value of '0'.
- Possible failed login attempts** (max. 3 characters): A text input field containing '3'.
- Deny personal data**: A checkbox that is currently unchecked.


Fig. 29: Configure password security

<i>Validity</i>	Enter for how long a password is supposed to remain valid. <i>Validity = 0</i> : Passwords never expire
<i>Point in time when information about the imminent expiration of the password is sent</i>	Enter how many days before the expiration of the password users are to be reminded that they will have to change their password soon. <i>Point in time ... = 0</i> : User does not receive any information 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.



☐ = 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


- To define forbidden passwords, open the group field *Forbidden Passwords*.
- In the title bar of the group field, click on the button  *Forbidden Passwords*.
- 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. 30: 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. 36).

- 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.

- 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

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

Advanced Password Settings

Password rules can be ignored ☐

Fig. 31: 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.



4.2.8.1 Edit entry

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

0002100010000	
0602150014444	
<input type="text" value="New value"/>	 

Add Delete

Fig. 32: 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*).

4.2.9 Tab General Settings

Here, you can change several general settings.

< Details* Passwords **General Settings*** LDAP Connection Data* Web Servi >

Inactivity	▶
SMTP Account	▶
SNMP Agent	▶
Login Settings	▶
Miscellaneous Settings	▶

Fig. 33: Tenants module - tab General Settings

4.2.9.1 Group field Inactivity

Inactivity ▼

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

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

Session timeout


☒ Session timeout
 Minute(s)

☐ Session never expires

Fig. 34: 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*.
The notification is sent to the e-mail address of the user.

<i>User will be deactivated</i>	Select after how many days of inactivity the account of the user is locked.
<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: The started session is never ended if the user just closes the browser instead of logging off from the application properly by using the logoff function (menu item  (Logged in as) > Logoff). Each endless session consumes storage space. This may result in the necessity to reboot the server. Upon rebooting the server, all sessions are ended.</p>




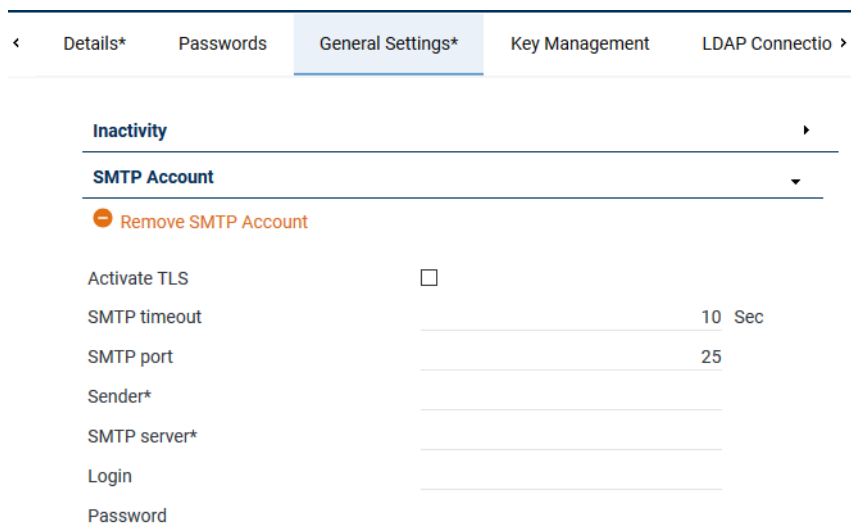
Changes in these settings come into effect only after the user has logged in to the system once again.

4.2.9.2

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




The screenshot shows the 'General Settings*' tab of the 'SMTP Account' configuration. At the top, there are tabs for 'Details*', 'Passwords', 'General Settings*', 'Key Management', and 'LDAP Connectio'. Below the tabs, there is a title bar with 'Inactivity' and a dropdown arrow, followed by 'SMTP Account' and another dropdown arrow. Below the title bar, there is a red minus icon and the text 'Remove SMTP Account'. The main configuration area contains the following fields:

- Activate TLS: ☐
- SMTP timeout: 10 Sec
- SMTP port: 25
- Sender*:
- SMTP server*:
- Login:
- Password:


Fig. 35: 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.

3. 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.

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

4.2.9.3 Group field SNMP Agent

To make sure that the recording system can answer the **SNMP**-GET requests of external monitoring programs, you have to configure an **SNMP** agent here.



In the **SNMP**-GET requests, the value *public* must be used as *community name*.



For **SNMP**-GET requests, the recording system uses its own **SNMP** service. The **SNMP** service of the operating system is **not** used.

Please deactivate the **SNMP** service of the operating system unless you need it for other applications!


Via **SNMP**-GET request the system status can be monitored. Possible results from a system status request are:

OK	The system runs without error.
ERROR	At least one monitored object has failed. The list in the field <i>DESCRIPTION</i> of the SNMP answer contains all failed objects. NOTICE! For detailed information about the error of an object refer to the Status module of the application System Monitoring refer to the user manual <i>System Monitoring</i> .

All **SNMP** objects of the recording system have been defined in the following **MIB** file:

- *C:\Program Files (x86)\ASC\ASC Product Suite\data\mib\ASC-SNMP-MIB-NEO.txt*

Set up SNMP agent

- To set up the function, open the group field *SNMP Agent*.
- In the title bar of the group field, click on the button  *SNMP Agent*.



Which entry fields are displayed depends on the **SNMP** version and on the security level you select.

SNMP Agent

Remove SNMP Account

SNMP version

SNMPV3

Timeout*

100 Sec

SNMP port*

161

Community*

public

User name*

SnmpUser

Security level

AUTH / PRIV

Authentication protocol

MD5

Authentication password*

.....

Privacy protocol

DES

Privacy password*

.....

SNMP Agent

Remove SNMP Account

SNMP version

SNMPV2

Timeout*

100 Sec

SNMP port*

161

Community*

public

User name*

SnmpUser

Security level


NOAUTH / NOPRIV

Fig. 36: Group field SNMP Agent (examples)


3. Complete all required fields:

SNMP version	<p>From the drop-down list, select the SNMP version you would like to use.</p> <p>The following versions are available:</p> <ul style="list-style-type: none"> • SNMPV2 • SNMPV2 / SNMPV3 • SNMPV3
Timeout	<p>Enter after how many seconds a timeout notification is supposed to be sent if no connection to the SNMP server could be established.</p>
SNMP port	<p>Enter the port via the SNMP request are supposed to come in. Default value: 161</p> <p>NOTICE! If the SNMP service of the operating system is used as well, you cannot use the default port. In this case, enter a different port.</p>
User name	<p>(Only for SNMP versions SNMPV2/SNMPV3 and SNMPV3.)</p> <p>Define the user name which has to be used for SNMP requests.</p>
Security level	<p>(Only for SNMP versions SNMPV2/SNMPV3 and SNMPV3.)</p> <p>From the drop-down list, select the security level you would like to use.</p> <p>The following security levels are available:</p> <ul style="list-style-type: none"> • NOAUTH / NOPRIV <p>The external SNMP program does not have to authenticate.</p> <p>The SNMP answer is transferred without encryption.</p> • AUTH / NOPRIV <p>Select this option if you want the external SNMP program to authenticate while the SNMP answer is transferred without encryption.</p> <p>In this case, select a protocol type in the field <i>Authentication protocol</i> and enter a corresponding password in the field <i>Authentication password</i>.</p> • AUTH / PRIV <p>Select this option if you want the external SNMP program to authenticate and the SNMP answer to be transferred with encryption.</p> <p>In this case, select a protocol type in the field <i>Authentication protocol</i> and enter a corresponding password in the field <i>Authentication password</i>.</p>

	In this case, additionally select a protocol type in the field <i>Privacy protocol</i> and enter a corresponding password in the field <i>Privacy password</i> .
<i>Authentication protocol</i>	<p>(Only for security levels <i>AUTH / NOPRIV</i> and <i>AUTH / PRIV</i>.)</p> <p>Select the protocol that you would like to use for the authentication of the external SNMP program.</p> <p>The following protocol types are available:</p> <ul style="list-style-type: none"> • <i>MD5</i> • <i>SHA</i>
<i>Authentication password</i>	<p>(Only for security levels <i>AUTH / NOPRIV</i> and <i>AUTH / PRIV</i>.)</p> <p>Enter a password for the authentication here.</p> <p>Length of the password: 8 to 15 characters</p>
<i>Privacy protocol</i>	<p>(Only for security level <i>AUTH / PRIV</i>.)</p> <p>Select the protocol that you would like to use for the encryption of the SNMP answer.</p> <p>The following protocol types are available:</p> <ul style="list-style-type: none"> • <i>DES</i> • <i>AES-128</i>
<i>Privacy password</i>	<p>(Only for security level <i>AUTH / PRIV</i>.)</p> <p>Enter a password for the encryption of the SNMP answer here.</p> <p>Length of the password: 8 to 15 characters</p>

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



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.



You can configure **SNMP** trap notifications in the Notifications module, see administration manual *System Configuration - Notifications module*.

4.2.9.4

Group field Login Settings

Login Settings	
Activate SSO login	<input type="checkbox"/>
Activate JWT login	<input type="checkbox"/>
Alternative login error page	<input type="checkbox"/>
Activate LDAP login	<input type="checkbox"/>

Fig. 37: Configure login settings

<i>Activate SSO login</i>	<p>Here, you can activate or deactivate SSO login for the users of the recording system.</p> <p>Activate or deactivate the login via Single Sign On (SSO).</p> <p><input checked="" type="checkbox"/> = SSO login has been activated.</p> <p><input type="checkbox"/> = SSO login has not been activated.</p> <p>Upon activating the function here, all users of all tenants can use SSO. The individual tenants do not have to configure any further settings.</p> <p>The only other precondition for using SSO:</p>
---------------------------	--

- For users to be able to log in to the system via [SSO](#), their login names in the recording system (see Employees module, tab *Account*) must be the same as their Windows login names and contain the domain.

Format: *Domain\Windows_login_name*

NOTICE! The login password in the recording system does **not** have to be the same as the password of the Windows account. Upon logging in via [SSO](#), only the login password is processed. The Windows password is ignored.

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

Restrictions when using [SSO](#):

- Combination login not possible
- In the address bar of the browser, it is mandatory to use the IP address of the application server. Using a DNS name is not possible.

Activate JWT login

Here, you can activate or deactivate the authentication by means of JWT login for the users of the recording system.

Activate or deactivate the authentication by means of JWT.

☒ = activated

☐ = not activated

JWT login is a special login procedure; the application receives an external token (JWT token) with certain identification attributes that it is asked to authenticate.

If the information in the token is valid, the users is logged in to the system without having to enter another password.

If the information in the token is invalid, the user is denied access.

NOTICE! To be able to check the validity of external tokens, a valid certificate of the external system must be imported in [neo](#).

Alternative login error page

Here, you can activate or deactivate whether an alternative login error page is displayed in case of an invalid JWT login.

Activate or deactivate whether an alternative login error page is displayed.

☒ = activated

☐ = not activated

Activate LDAP login

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

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

☒ = [LDAP](#) login has been activated.

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

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


NOTICE! [LDAP](#) login cannot be activated before you have configured at least 1 [LDAP](#) connection (see [chapter "Tab LDAP Connection Data"](#), p. 42).

4.2.9.5 Group field Miscellaneous Settings

Miscellaneous Settings ▼

- ☒ Display last login date
- ☒ Display logout warning
- ☒ Resource string view
- ☒ Failed login
- ☐ Deactivate logoff function
- ☐ Hide Forgot Password
- System announcement

Fig. 38: Configure miscellaneous settings

Display last login date	Select whether you would like to have the date of the last login displayed in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
Display logout warning	Select whether you would like to issue a logout warning in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
Resource string view	Select whether you would like to display the button to activate the resource string view in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
Failed login	Select whether you would like to display the information about a failed login in all applications. <input checked="" type="checkbox"/> = Displaying information has been activated. <input type="checkbox"/> = Displaying information has not been activated.
Deactivate logoff function	Select whether you would like to display the logoff function (menu item  (Logged in as) > Logoff). <input checked="" type="checkbox"/> = Logoff function is not displayed. <input type="checkbox"/> = Logoff function is displayed.
Hide Forgot Password	Select whether you would like to display the function <i>Forgot Password?</i> in the login windows. <input checked="" type="checkbox"/> = Function <i>Forgot Password?</i> is not displayed. <input type="checkbox"/> = Function <i>Forgot Password?</i> is displayed.
System announcement	Here, you can compose a message (maintenance announcement) for the tenant. The notification is displayed in the browser login screen of the <u>neo</u> application.

4.2.10 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. 40](#)).



Fig. 39: Tenants module - tab LDAP Authentication

Add	Opens a window in which you can add a new LDAP connection (see chapter "Edit LDAP connection data", p. 43).
Edit	Opens the selected entry for editing (see chapter "Edit LDAP connection data", p. 43).
Delete	Deletes the selected entry from the list.

4.2.10.1 Edit LDAP connection data

Server address	Port
159.159.159.159	46611
123.123.123.123	4711

Add **Edit** **Delete**

Fig. 40: 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*.

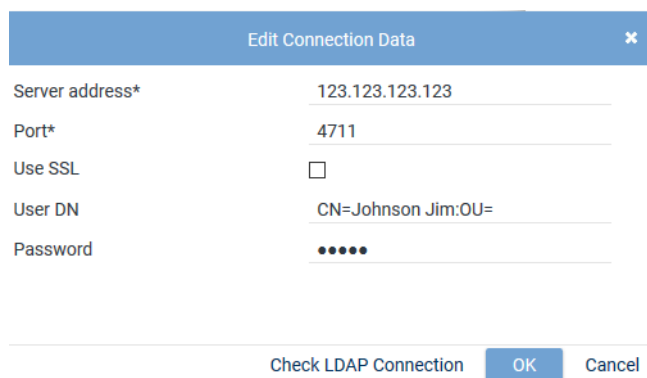


Fig. 41: Edit LDAP connection data (example)

Server address [IP](#) address of the [LDAP](#) server.

<i>Port</i>	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
<i>Use SSL</i>	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*.

4.2.11 Tab Web Service

The *neo* software provides an interface to use functionalities via Web Service.

In this tab, you can select which of the functionalities that are generally provided for Web Service are allowed to be used in your recording system. The respective functionalities are released for each tenant individually. Which functionalities are generally available and displayed in the tab depends on whether you have selected the account of a tenant or of a system provider in the main view.

4.2.11.1 Configure web service for the system provider

Here, you can activate or deactivate the functionalities of the Web Service that the system provider is supposed to be able to use.

1. Select the account of the system provider in the main view.
2. Select the tab *Web Service*.

[← Passwords](#)
[General Settings*](#)
[LDAP Connection Data*](#)
[Web Service](#)
[→](#)

General Functions ▼

☒ Checks the general Web Service functionality

Employees ▼

☐ Allows exporting function rights
☐ Allows importing roles
☐ Allows exporting roles

Tenant ▼

☒ Allows exporting tenant information
☒ Allows exporting the extension assignment
☒ Allows assigning and administrating extensions
☒ Allows deleting a tenant
☒ Allows changing an extension
☐ Allows revoking Vormetric keys.
☒ Allows importing new as well as existing tenants

Configuration ▼

☒ Allows importing monitor points
☒ Allows importing phones
☐ Allows exporting phones
☐ Allows exporting monitor points

Fig. 42: Web service functionalities for the system provider

3. Tick the check boxes of the functions which are supposed to be activated.
☒ = Function has been activated.
☐ = Function has not been activated.

Group field General Functions

In this group field, you can activate the test function.

<i>Checks the general web service functionality</i>	Activate the check box, if you would like to allow checking the general web service functionality.
---	--

Group field Employees

In this group field, you can configure the functions to administrate employees.

<i>Allows exporting function rights</i>	Activate the check box if you would like to allow the tenant to export function rights via the Web Service.
<i>Allows importing roles</i>	Activate the check box if you would like to allow the tenant to import roles via the Web Service.
<i>Allows exporting roles</i>	Activate the check box if you would like to allow the tenant to export roles via the Web Service.

Group field Tenant

In this group field, you can configure the functions to administrate tenants.

<i>Allows exporting tenant information</i>	Activate the check box if you would like to be able to export tenant information via the Web Service. Tenant information are e. g. tenant name, deployed default language, employee ID, first name, last name or the e-mail address.
--	---

<i>Allows exporting the extension assignment</i>	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
<i>Allows assigning and administering extensions</i>	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
<i>Allows deleting a tenant</i>	Activate the check box if you would like to allow the tenant to delete a tenant via the Web Service.
<i>Allows changing an extension</i>	Activate the check box if you would like to allow the tenant to change an extension via the Web Service.
<i>Allows revoking Vormetric keys</i>	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
<i>Allows importing new as well as existing tenants</i>	Activate the check box if you would like to be able to add tenants and overwrite the data of existing tenants via the Web Service.

Group field Configuration

In this group field, you can configure the functions for the configuration of the tenants.

<i>Allows importing monitor points</i>	Activate the check box if you would like to allow the tenant to import monitor points via the Web Service.
<i>Allows importing phones</i>	Activate the check box if you would like to allow the tenant to import phones via the Web Service.
<i>Allows exporting phones</i>	Activate the check box if you would like to allow the tenant to export phones via the Web Service.
<i>Allows exporting monitor points</i>	Activate the check box if you would like to allow the tenant to import monitor points via the Web Service.

4.2.11.2 Configure Web Service for the tenant

Here, you can activate or deactivate the functionalities of the Web Service that the tenant is supposed to be able to use.

1. In the main view, select the account of the tenant for which you would like to adjust the settings.
2. Select the tab *Web Service*.

<
Extensions
PBX Agent IDs
Chat IDs
Web Service
System Licenses >

General Functions
▼

☒ Checks the general Web Service functionality

Employees
▼

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

Tenant
▼

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

Conversations Export Server
▼

Export server API-01 + -

Fig. 43: Web service functionalities for the tenant

- Tick the check boxes of the functions which are supposed to be activated.
☒ = Function has been activated.
☐ = Function has not been activated.

Group field General Functions

In this group field, you can activate the test function.

<i>Checks the general web service functionality</i>	Activate the check box, if you would like to allow checking the general web service functionality.
---	--

Group field Employees

In this group field, you can configure the functions for the configuration of the employees.

<i>Allows exporting function rights</i>	Activate the check box if you would like to allow the tenant to export function rights via the Web Service.
<i>Allows importing new as well as existing employees</i>	Activate the check box if you would like to allow the tenant to add employees via the Web Service and to overwrite the data of existing employees.
<i>Allows importing roles</i>	Activate the check box if you would like to allow the tenant to import roles via the Web Service.
<i>Allows exporting roles</i>	Activate the check box if you would like to allow the tenant to export roles via the Web Service.
<i>Allows exporting employees</i>	Activate the check box if you would like to allow the tenant to export employees via the Web Service.

Group field Conversation

In this group field, you can configure the functions for searching and exporting conversations via the Web Service.

<i>Allows exporting conversations</i>	<p>Activate the check box if you would like to allow the tenant to export conversations via the Web Service.</p> <p>NOTICE! When activating this function, you have to enter an export server in the group field <i>Conversations Export Server</i>.</p>
<i>Allows searching for conversations via Web Service</i>	Activate the check box if you would like to allow the tenant to search conversations via the Web Service.
<i>Allows exporting transcriptions</i>	Activate the check box if you would like to allow the tenant to export transcriptions via the Web Service.
<i>Set delete time for conversations</i>	Activate the check box if you would like to allow the tenant to set a deletion time for conversations via the Web Service.
<i>Set deletion time for packages</i>	Activate the check box if you would like to allow the tenant to set a deletion time for packages via the Web Service.

Group field Tenant

In this group field, you can configure the functions for the administration of the tenants.

<i>Allows exporting organization units</i>	Activate the check box if you would like to allow the tenant to export organization units via the Web Service.
<i>Allows revoking Vormetric keys</i>	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
<i>Allows importing organization units</i>	Activate the check box if you would like to allow the tenant to import organization units via the Web Service.

Group field Conversations export server

In this group field, you can configure the export server on which the conversations which are supposed to be exported via the Web Service are stored.

<i>Export server</i>	Click on the button  next to the field <i>Export server</i> .
----------------------	--



Fig. 44: Select export server

NOTICE! For export servers, the property *Replay* is mandatory. Therefore, this list only contains servers which have been configured as replay servers.

1. Select the server from the list from which the conversations are supposed to be exported.
2. Click on the button *Add*.
 - ⇒ The name of the export server appears in the detail view.



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

4.2.11.2.1 Assign server

1. Click on the button **+** behind the entry field *Export server*.

_____ + -

Fig. 45: Assign server

2. Select the appropriate server from the list.

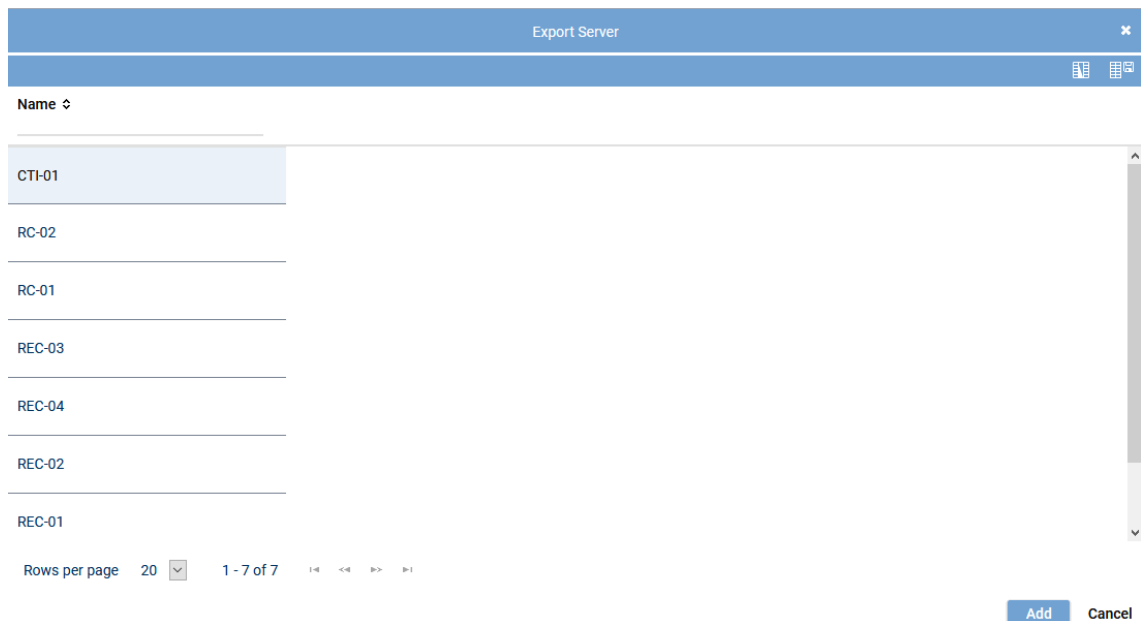


Fig. 46: Select server (example)

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

4.2.11.3 Path of the WSDL file

The provided [WSDL](#) file lists the functions which can be used with the Web Service.

Enter the URL <http://<Recorder-IP>/ASCWebService/ASCWebServiceService?wsdl> in the browser to call up the [WSDL](#) file.

Return value

- Import:
If an import is executed, an entry about its success or about its failure appears in the System Monitoring in the Jobs module in the column *Job Status*.
- Export:
The export can be checked on basis of the read-out data, the Boolean value indicating a success or a failure as well as on basis of the error description in case of a failure.

4.2.11.4 Configure Web Service for the reseller

Here, you can activate or deactivate the functionalities of the Web Service that the reseller is supposed to be able to use.

- Select the account of the reseller in the main view.
- Select the tab *Web Service*.

<
Details*
Web Service
PBX
>

General Functions
▼

☐ Checks the general Web Service functionality

Employees
▼

☐ Allows exporting function rights
☐ Allows importing roles
☐ Allows exporting roles

Tenant
▼

☐ Allows exporting tenant information
☐ Allows exporting the extension assignment
☐ Allows assigning and administrating extensions
☐ Allows deleting a tenant
☐ Allows changing an extension
☐ Allows revoking Vormetric keys.
☐ Allows importing new as well as existing tenants

Configuration
▼

☐ Allows importing monitor points
☐ Allows importing phones
☐ Allows exporting phones
☐ Allows exporting monitor points

Fig. 47: Web service functionalities for the reseller

3. Tick the check boxes of the functions which are supposed to be activated.
☒ = Function has been activated.
☐ = Function has not been activated.

Group field General Functions

In this group field, you can activate the test function.

<i>Checks the general web service functionality</i>	Activate the check box, if you would like to allow checking the general web service functionality.
---	--

Group field Employees

In this group field, you can configure the functions to administrate employees.

<i>Allows exporting function rights</i>	Activate the check box if you would like to allow the tenant to export function rights via the Web Service.
<i>Allows importing roles</i>	Activate the check box if you would like to allow the tenant to import roles via the Web Service.
<i>Allows exporting roles</i>	Activate the check box if you would like to allow the tenant to export roles via the Web Service.

Group field Tenant

In this group field, you can configure the functions for the administration of the tenants.

<i>Allows exporting tenant information</i>	Activate the check box if you would like to be able to export tenant information via the Web Service. Tenant information are e. g. tenant name, the used default language, employee ID, first name, last name or the e-mail address.
--	---

<i>Allows exporting the extension assignment</i>	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
<i>Allows assigning and administering extensions</i>	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
<i>Allows deleting a tenant</i>	Activate the check box if you would like to be able to delete the tenant via the Web Service.
<i>Allows changing an extension</i>	Activate the check box if you would like to be able to change the extension via the Web Service.
<i>Allows revoking Vormetric keys</i>	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
<i>Allows importing new as well as existing tenants</i>	Activate the check box if you would like to be able to add tenants and overwrite the data of existing tenants via the Web Service.

Group field Configuration

In this group field, you can configure the functions for the configuration of the tenants.

<i>Allows importing monitor points</i>	Activate the check box if you would like to allow the tenant to import monitor points via the Web Service.
<i>Allows importing phones</i>	Activate the check box if you would like to allow the tenant to import phones via the Web Service.
<i>Allows exporting phones</i>	Activate the check box if you would like to allow the tenant to export phones via the Web Service.
<i>Allows exporting monitor points</i>	Activate the check box if you would like to allow the tenant to import monitor points via the Web Service.

4.2.12

Tab PBX

Here, you can activate and administrate [PBX](#) filters which have been assigned to the selected tenant.

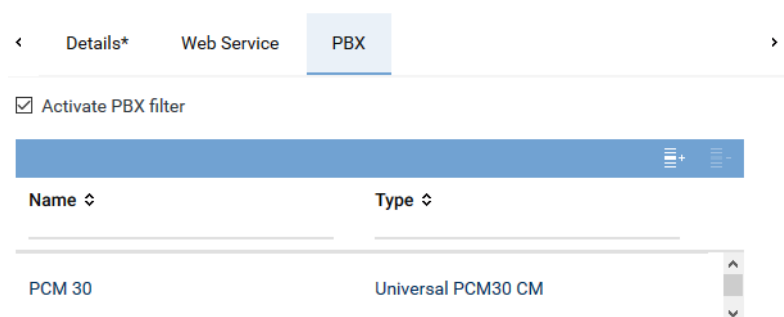


Fig. 48: Tenants module - tab PBX

<i>Activate PBX filter</i>	Activate the check box if you would like to restrict the access of the reseller to assigned PBXs .
----------------------------	--

- To assign a [PBX](#) to a reseller, proceed as described in [chapter "Assign PBX", p. 52](#).
- To remove the assignment of a [PBX](#) to a reseller, proceed as described in [chapter "Remove PBX assignment", p. 53](#).

4.2.12.1

Assign PBX

1. Click on the icon  (Add).

< Details* Web Service **PBX** >

☒ Activate PBX filter

Name ↕	Type ↕
No records found	

Fig. 49: Assign PBX

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

PBX	
Name ↕	Type ↕
AL	ALCATEL OmniPCX
Universal Import	Universal import
Alcatel OmniPCX	ALCATEL OmniPCX
PCM 30	Universal PCM30 CM
PRI passive DP	Universal PRI passive DP
MVTC	Universal MVTC

Rows per page 20 1 - 20 of 54

Add Cancel

Fig. 50: Add PBX

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

4.2.12.2 Remove PBX assignment


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

< Details* Web Service **PBX** >

☒ Activate PBX filter

Name ↕	Type ↕
PCM 30	Universal PCM30 CM

Fig. 51: Remove PBX assignment

- Click on the icon  (*Remove*).

4.2.13

Tab System Licenses



This tab is only displayed if there is a license of the type *Cloud Recording* in the system.

Here, you can activate modules and functionalities to be used by tenants.

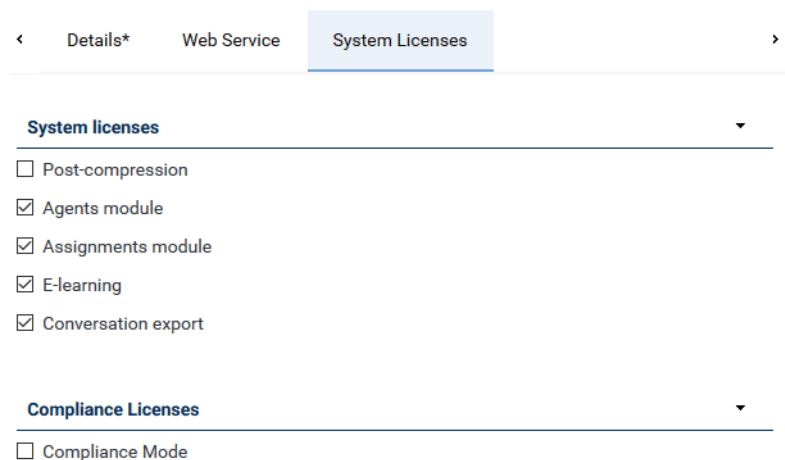


Fig. 52: Tab System Licenses

Group field System Licenses

Post-compression

Select whether the recorded conversations are supposed to be compressed.

☒ = Recordings are compressed.

☐ = Recordings are not compressed.

NOTICE! To be able to use post-compression, you need one license of the type *Data Compression* for each channel which is supposed to be compressed.

Compressing the saved conversations allows increasing the number of recordings which can be saved. In addition, the network bandwidth necessary for a possible transfer of recording data is decreased.

The standardized algorithm [G.729A](#) is used to compress the recordings. [G.729A](#) compresses audio data in stereo and in mono calls from 128 kbit/s to a data rate of 16 kbit/s and from 64 kbit/s to 8 kbit/s respectively. The precondition for using post-compression is that the conversations are available in G.711 or G.722 format (A-law or μ -law).

NOTICE! If the compression has been activated, data is only transferred to the storage expansion once it has been compressed. A compression delay thus delays the transfer to the storage expansion, too.

NOTICE! Data which has already been compressed is not decompressed in the event of a data transfer even if no compression has been selected for the target drive. This means that compressed data is not decompressed neither when transferred between different system storages nor from one system storage to a storage expansion.

NOTICE! Recordings are compressed from the moment on that post-compression is activated. Recordings which have already been transferred to the storage expansion are **not** compressed retroactively.

	NOTICE! The drives must be configured for post-compression. For further information refer to the administration manual <i>System Configuration - Configuration drives</i> . Post-compression applies for all drives for which post-compression has been activated.
<i>Agents module</i>	Select whether the Agents module is supposed to be activated. <input checked="" type="checkbox"/> = Agents module has been activated. <input type="checkbox"/> = Agents module has not been activated.
<i>Assignments module</i>	Select whether the Assignments module is supposed to be activated. <input checked="" type="checkbox"/> = Assignments module has been activated. <input type="checkbox"/> = Assignments module has not been activated.
<i>E-learning</i>	Select whether the E-Learning module is supposed to be activated. <input checked="" type="checkbox"/> = E-Learning module has been activated. <input type="checkbox"/> = E-Learning module has not been activated.
<i>Conversation export</i>	Select whether the export of conversations is supposed to be activated. <input checked="" type="checkbox"/> = Export of conversations has been activated. <input type="checkbox"/> = Export of conversations has not been activated.

Group field Compliance Licenses



This group field is only displayed if the license *INSPIRATION for Compliance* has been installed in the system.

<i>Compliance mode</i>	Select whether the compliance mode for INSPIRATION ^{neo} is supposed to be activated. <input checked="" type="checkbox"/> = Compliance mode has been activated. <input type="checkbox"/> = Compliance mode has not been activated.
------------------------	---


4.3

Create new tenants manually

1. In the main view, select the system provider or the reseller under which you would like to create a tenant or a reseller.

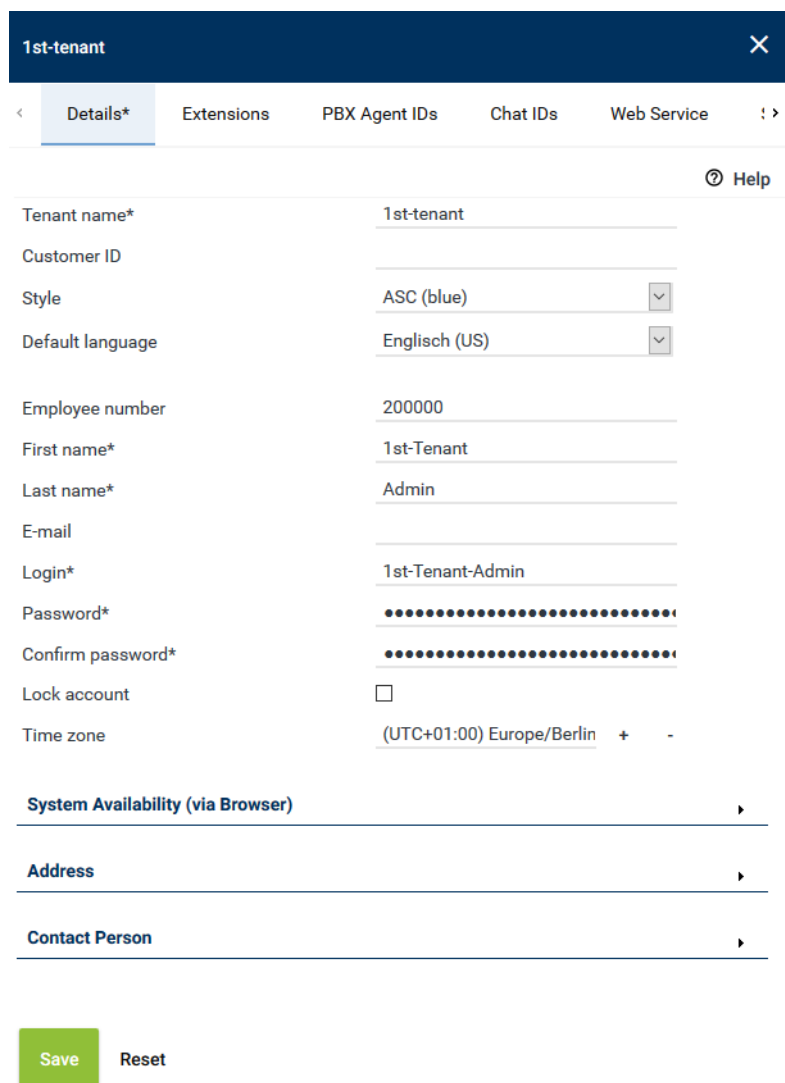
+ × Tenants General ▾	
Name	Type
▼ System	System provider
1st-tenant	Tenant
2nd-Tenant	Tenant
3rd-Tenant	Tenant

Fig. 53: Tenants module - main view (example)

2. Click on the icon  (Add) in the toolbar.
3. Select one of the following options:

<i>Create Tenant</i>	A new tenant is created.
<i>Create Reseller</i>	A new reseller is created.

4. In the detail view, make all necessary settings within the tabs.
You can change tabs without buffering without risking the loss of your settings.
5. 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**.



1st-tenant ✕

< **Details*** Extensions PBX Agent IDs Chat IDs Web Service >

ⓘ Help

Tenant name* 1st-tenant

Customer ID

Style ASC (blue) ▼

Default language Englisch (US) ▼

Employee number 200000

First name* 1st-Tenant

Last name* Admin

E-mail

Login* 1st-Tenant-Admin

Password*

Confirm password*

Lock account ☐

Time zone (UTC+01:00) Europe/Berlin + -

System Availability (via Browser) ▶

Address ▶

Contact Person ▶

Save **Reset**

Fig. 54: Save tenant

4.4

Edit tenants manually

1. In the main view, select the tenant or reseller whose data you would like to edit.
2. In the detail view, make all necessary changes within the tabs.
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**.

1st-tenant

<

Details*

Extensions

PBX Agent IDs

Chat IDs

Web Service

>

Help

Tenant name*

1st-tenant

Customer ID

Style

ASC (blue)

Default language

Englisch (US)

Employee number

200000

First name*

1st-Tenant

Last name*

Admin

E-mail

Login*

1st-Tenant-Admin

Password*

.....

Confirm password*

.....

Lock account

☐

Time zone

(UTC+01:00) Europe/Berlin + -

System Availability (via Browser)

Address

Contact Person


Save

Reset

Fig. 55: Save changes

4.5

Delete tenant

1. In the main view, select the tenant or reseller you would like to delete.
A reseller can only be deleted if no tenant and no other reseller has been subordinated to it.
2. Click on the icon  (*Delete*) in the toolbar.
3. To really delete the selected tenant, confirm the security prompt.

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 which can be defined in the Roles module. In addition or optionally, you can assign the user individual function rights.



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.



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. 56: 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>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.

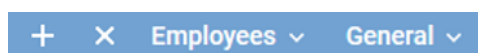




Fig. 57: Employees module - toolbar

	<i>Create</i>	Creates a new employee (see chapter "Create new employee", p. 74).
	<i>Delete</i>	Deletes the selected employee (see chapter "Delete employee", p. 75).
<i>Employees</i>	<i>Summary</i>	Lists all function rights of the selected employee (see chapter "Show summary", p. 60).
	<i>Show Locked Employees/Show All Employees</i>	Lists only the locked employees in the main view (see chapter "Show locked employees", p. 60).
	<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. 61).
	<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>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. 61 .

	When opening the module, a search filter is set automatically so that only data sets of the current day are displayed. The function by means of the menu item <i>General > Reset Search</i> does not deactivate this filter.
<i>Reset Search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



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

5.1.1.1 Show summary

This function allows displaying the function rights of the employee.

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

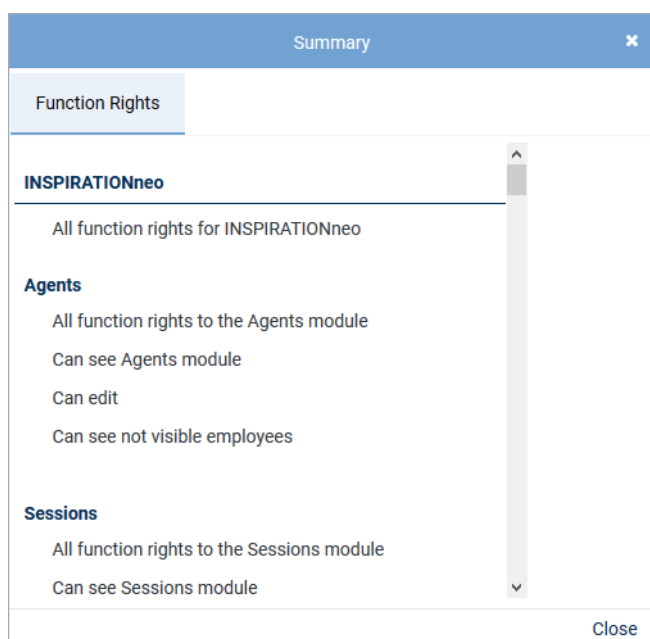




Fig. 58: Summary of the function rights

	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 [chapter "Tab Account", p. 67](#).

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. Click on the menu item *General > Search* in the toolbar.
 - ⇒ The window *Search Criteria* appears.

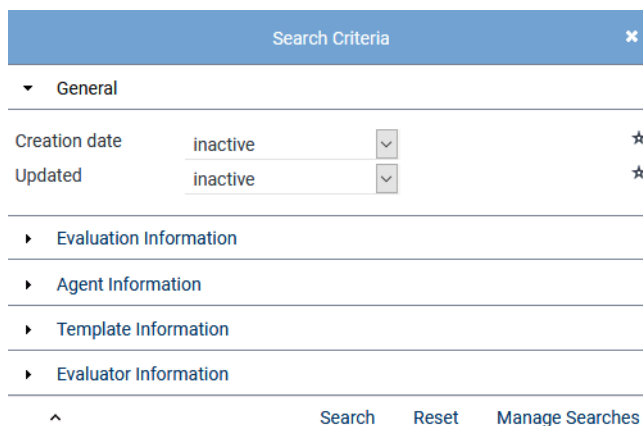




Fig. 59: Window Search Criteria (example)

2. Set the respective search criteria.

NOTICE! It depends on the respective module which search criteria are available.
3. To start the search, click on the button *Search*.
To reset all manually entered search criteria, click on the button *Reset*.
 - ⇒ After running the search, only those sets of data are displayed in the main view which meet the set search criteria.
4. To display all original sets of data in the main view again, i. e. to reset the manually entered search criteria, click on the menu item *General > Reset Search* in the toolbar.

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

Via 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.

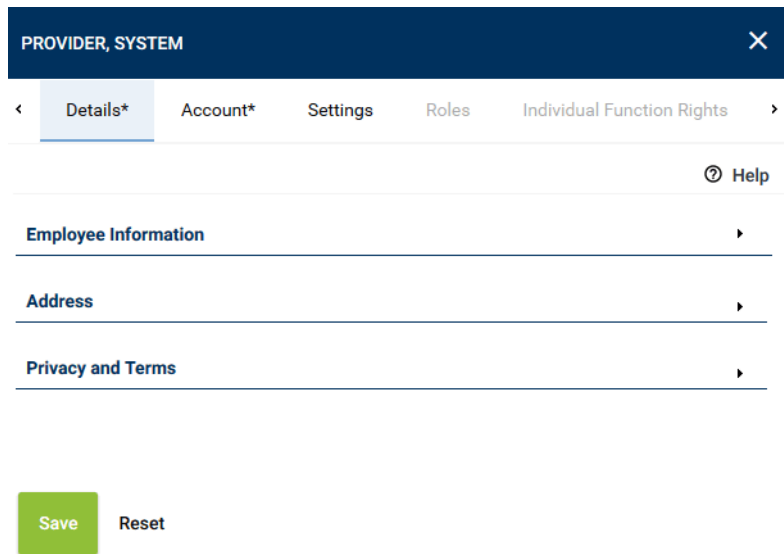


Fig. 60: Employees module - detail view

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. 62.](#)
- *Account*
Here, you can display and edit the employee's login data.
See [chapter "Tab Account", p. 67.](#)
- *Settings*
Here, you can display and edit the employee's rights and logging settings.
See [chapter "Tab Settings", p. 69.](#)
- *Roles*
Here, you can display the roles which have been assigned to the employee and edit the role assignment.
See [chapter "Tab Roles", p. 71.](#)
- *Individual Function Rights*
Here, you can display and assign the employee's individual function rights.
See [chapter "Tab Individual Function Rights", p. 72.](#)

5.2.1

Tab Details

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

< **Details*** Account* Settings Roles Individual Function Rights >

? Help

Employee Information ▶

Address ▶


Privacy and Terms ▶

Fig. 61: 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

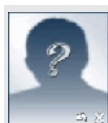
- To edit personal data of the employee, open the group field *Employee Information*.

Employee Information ▼



Employee number	100000
First name*	SYSTEM
Last name*	PROVIDER
Date of birth	<input type="text"/>
E-mail	<input type="text"/>
Date of entry	<input type="text"/>
Comment	<div></div>
Address for replay via phone	<input type="text"/>
Import key	<input type="text"/>
Time zone	UNKNOWN + -



Fig. 62: Edit employee information



Placeholder for the employee's photo.

See [chapter "Upload or delete image"](#), p. 64.

<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>Date of birth</i>	Date of birth of the employee. You can enter the date directly via the keyboard or via the icon.
<i>E-mail</i>	E-mail address of the employee.
<i>Date of entry</i>	Day on which the employee was hired. You can enter the date directly via the keyboard or via the icon.
<i>Comment</i>	Comment on the employee information.
<i>Address for replay via phone</i>	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. • MAC address if it has been configured. • SIP address, e. g. <i>Extension@IP-Address</i>.
<i>Import key</i>	Key to unambiguously identify an employee imported from an external source. When importing the employee information for the first time, the import key is entered here automatically. Upon each new import, this import key is checked to determine whether the employee has already been imported before. In addition, the import key is used when transferring (export/import) recordings from a <i>neo</i> system to another <i>neo</i> system to map the recordings to the agents. If the employee does not have an automatically created import key, you can enter an import key manually for this mapping. 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.
<i>Time zone</i>	Shows the time zone in which the conversations are supposed to be displayed in the replay applications. The settings which have been configured for the respective employee prevail over the default settings in the Tenants module To select the time zone, click on the button  . See chapter "Add time zone", p. 18 . To delete the selection, click on the button  .

5.2.1.1.1 Upload or delete image

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

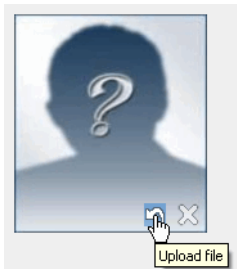


Fig. 63: Upload image

⇒ The window *Upload File* appears.

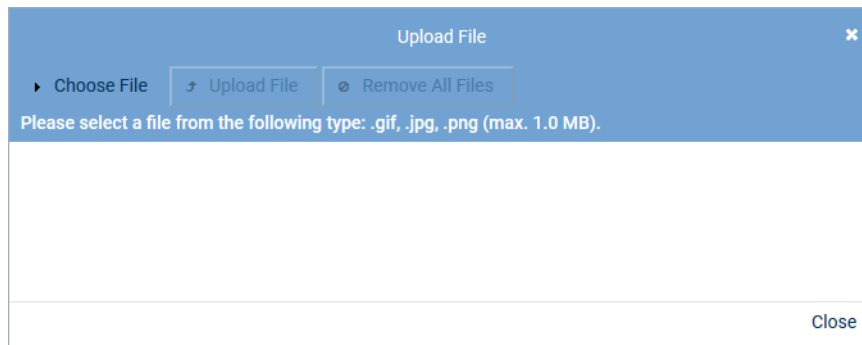


Fig. 64: Upload File


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.

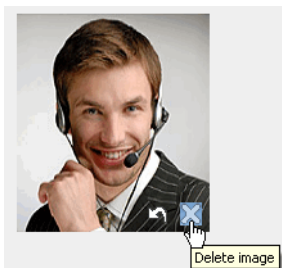


Fig. 65: Delete image (example)

⇒ 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*.

Address ▼

+ Add Address

Fig. 66: 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. 67: Add address

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

5.2.1.3 Group field Privacy and Terms

- If you would like to add a privacy statement and other terms of usage, open the group field *Privacy and Terms*.

Privacy and Terms ▼

+ Add Link

Fig. 68: Add privacy statement and terms

- In the title bar of the group field, click on the button + Add Link.
- Enter the respective links.

Privacy and Terms ▼

– Remove

Official privacy

Substitute privacy

Official legal notice

Substitute legal notice

Fig. 69: Add privacy statement and terms

<i>Official privacy</i>	Enter the link to the official privacy statement.
<i>Substitute privacy</i>	Enter the link to the substitute privacy statement.
<i>Official legal notice</i>	Enter the link to the official legal notice.
<i>Substitute legal notice</i>	Enter the link to the substitute legal notice.

- If you would like to remove the privacy statement and terms, click on the button – Remove in the title bar of the group field.

5.2.2 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.

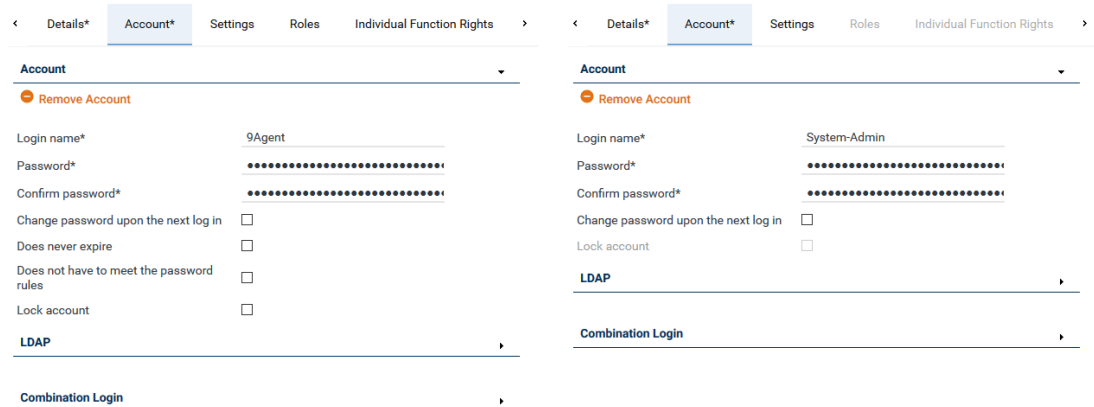


Fig. 70: Employees module - tab Account




For employees with superuser rights, some options are hidden.



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. 71: Add account

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

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

Does not have to meet the password rules

Activate this option if the password does not necessarily have to be consistent with the password rules.

NOTICE! Password rules can be defined in the Tenants module in the tab *Passwords*.


NOTICE! This option is not available for superusers.

Lock account

This option allows locking the employee's account.

In the main view, you can filter for this criterion, see [chapter "Show locked employees"](#), p. 60.

NOTICE! This option is not available for superusers.

4. If you would like to remove the account, click on the button  *Remove account* in the title bar of the group field.
5. To activate the authentication via [LDAP](#) for the employee, see [chapter "Authentication via LDAP"](#), p. 68.
6. To assign the employee a combination user, see [chapter "Assign combination user"](#), p. 68.

5.2.2.1 Authentication via LDAP

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



Fig. 72: Activate authentication via LDAP

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

☒ = Authentication via [LDAP](#) has been activated.

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


5.2.2.2 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*).

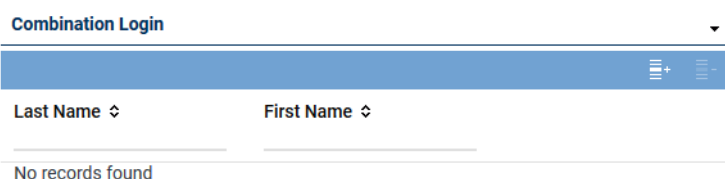


Fig. 73: Assign combination user

- 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.

Combination Login				
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.		

Rows per page 20 1 - 13 of 13


Add Cancel

Fig. 74: Add combination user

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

5.2.2.3

Delete combination user assignment

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

Combination Login	
Last Name	First Name
Agent	5.

Fig. 75: Delete combination user assignment

5.2.3

Tab Settings

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

<	Details*	Account*	Settings	Roles	Individual Function Rights	>
Permissions						
Logging Settings						

Fig. 76: Employees module - tab Settings

5.2.3.1 Group field Permissions

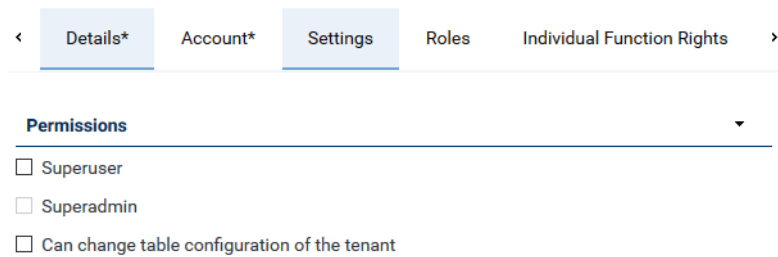


Fig. 77: Configure permissions

Superuser	<p>This right assigns all function rights in the system to the user if their licenses are available.</p> <p><input checked="" type="checkbox"/> = Right has been activated. <input type="checkbox"/> = Right has been deactivated.</p>
Superadmin	<p>This right assigns the user limited superuser function rights in the system.</p> <p>Employees of the system provider who have been configured as superadmins can log in to the accounts of any tenant in the system with the rights of a superuser of this tenant in the following applications:</p> <ul style="list-style-type: none"> • System Configuration • System Monitoring • Portal <p>Information about the login for superadmins can be found in the respective user manuals <i>System Configuration - General information</i>, <i>System Monitoring</i>, and <i>Portal</i>.</p> <p>A superadmin does not have access to recordings.</p> <p>A superadmin cannot be assigned to an organization unit.</p> <p><input checked="" type="checkbox"/> = Right has been activated. <input type="checkbox"/> = Right has been deactivated.</p> <p>NOTICE! Superadmin rights are only available in a Cloud environment and have to be activated when needed. The option <i>Superadmin</i> is only displayed if there is the respective license in the system. In a 1-tenant system, the option <i>Superadmin</i> is activated automatically. No extra license is required For the default superuser created by the system, the option <i>Superadmin</i> is not available.</p>
Can change table configuration of the tenant	<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>



As soon as you assign superuser rights to the user, only the tabs *Details*, *Account* and *Settings* are active. In this case, no further adjustments are have to be made in any of the other tabs.

5.2.3.2 Group field Logging Settings

Logging Settings ▼

Logging following activities of the user

☐ Access control

☐ Configuration activities

Fig. 78: Configure logging

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

☒ = Logging has been activated.

☐ = Logging has been deactivated.

Access control	If this option has been activated, the system logs when the user has signed in to and off from the system.
Configuration activities	If this option has been activated, all adjustments of the configuration on behalf of the user are logged.

5.2.4 Tab Roles



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



You can define roles in the Roles module.

< Details* Account* Settings **Roles** Individual Function Rights >

Directly Assigned Roles ▼

<  

Name ↕	Description ↕
No records found	

Roles By Orgaunits ▼

Role Name

No records found


Fig. 79: 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.

5.2.4.1 Assign roles

1. Click on the icon  (Add).

Name ↕	Description ↕
No records found	

Fig. 80: 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.

Add Roles	
Name ↕	Description ↕
Administrator	
Agent	Default agent role.
Supervisor	Default supervisor role.
Rows per page 20 ▾ 1 - 3 of 3 < << >> >	
<div>Add Cancel</div>	

Fig. 81: 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*.

5.2.4.2 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. 82: 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.

5.2.5 Tab Individual Function Rights

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

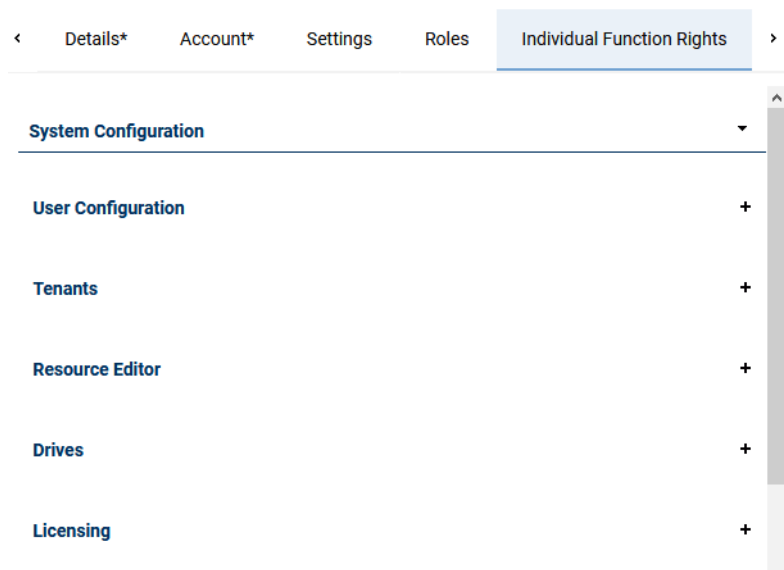


Fig. 83: Employees module - tab Individual Function Rights (example)

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

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

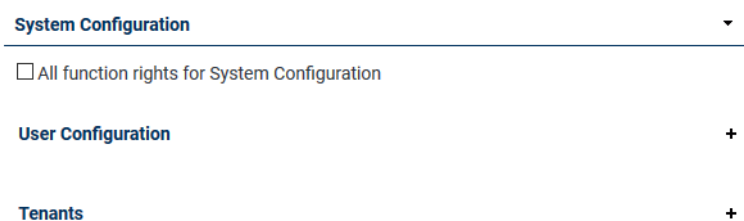


Fig. 84: Function rights - display sections (example)

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



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

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

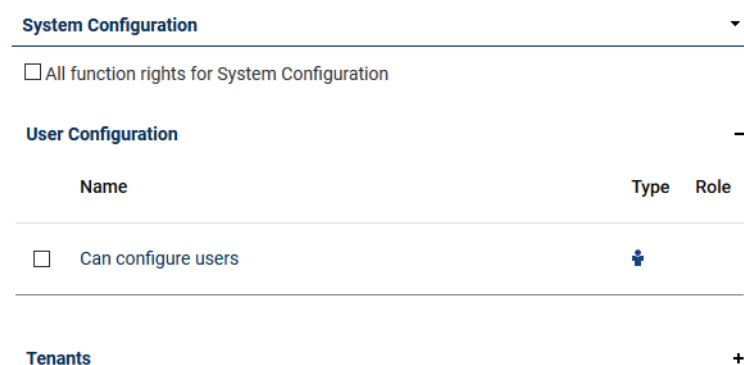





Fig. 85: Function rights - Display function rights


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)
<i>Role</i>	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. 60 .

Tab. 3: 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.

5.3

Create new employee

- 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*.

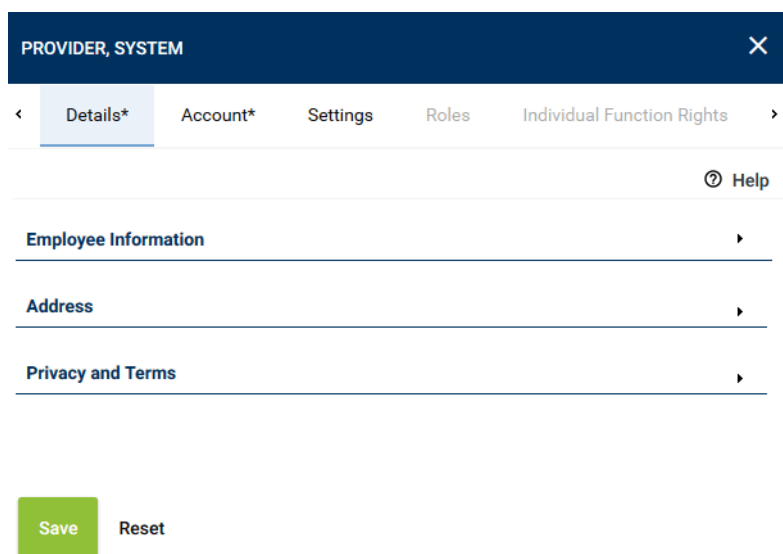


Fig. 86: Save employee

5.4

Edit employee

- 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*.

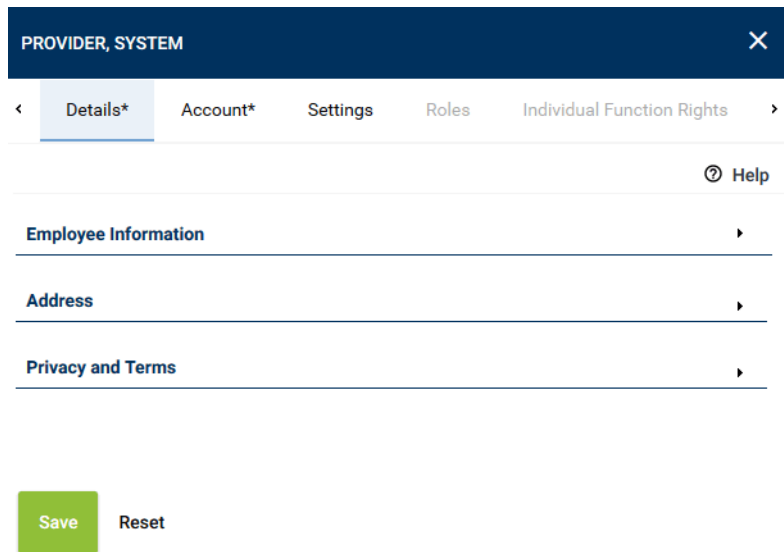



Fig. 87: Save changes

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.

6

Roles module

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

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



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



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.

6.1

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. 88: 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.

6.1.1

Toolbar

The toolbar offers the following functions.

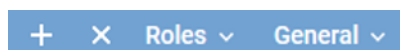



Fig. 89: Roles module - toolbar

+	Create	Creates a new role (see chapter "Create new role", p. 81).
---	--------	---

	<i>Delete</i>	Deletes the selected role (see chapter "Delete role", p. 82).
<i>Roles</i>	<i>Duplicate with Employees</i>	Creates a copy of the selected role with the assigned employee, see chapter "Duplicate role", p. 81 .
	<i>Duplicate Without Employees</i>	Creates a copy of the selected role without the assigned employee, see chapter "Duplicate role", p. 81 .
<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>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. 61 . When opening the module, a search filter is set automatically so that only data sets of the current day are displayed. The function by means of the menu item <i>General > Reset Search</i> does not deactivate this filter.
	<i>Reset Search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.

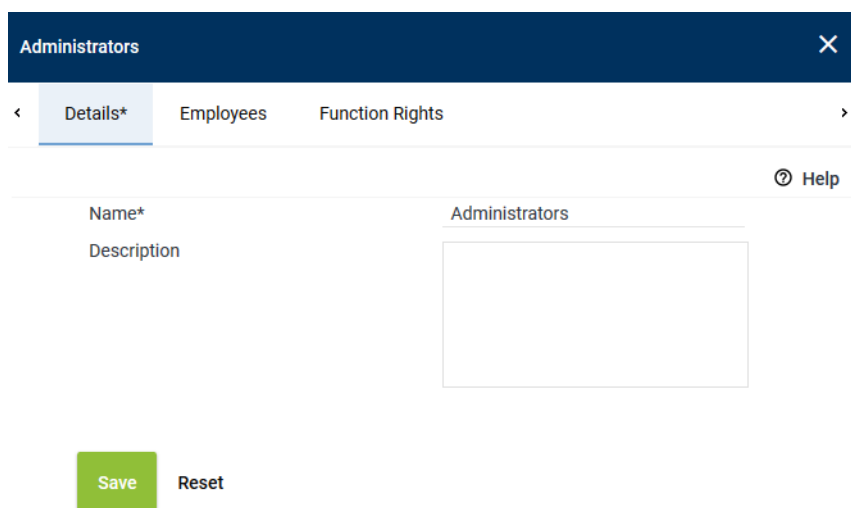


For detailed information on default functions such as *Print*, *Adjust table*, or *Help* refer to the user manual for administrators *System Configuration - General Information*.

6.2

Detail view

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



The screenshot shows the 'Administrators' detail view. At the top is a dark blue header with the title 'Administrators' and a close icon. Below the header is a tab bar with three tabs: 'Details*' (selected), 'Employees', and 'Function Rights'. To the right of the tabs is a 'Help' icon. The main content area is divided into two sections. The left section has a label 'Name*' and a text input field containing 'Administrators'. Below this is a label 'Description' and a large empty text area. At the bottom left are two buttons: a green 'Save' button and a grey 'Reset' button.

Fig. 90: 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. 78](#).

- *Function Rights*

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

See [chapter "Tab Function Rights", p. 79](#)

6.2.1 Tab Details

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

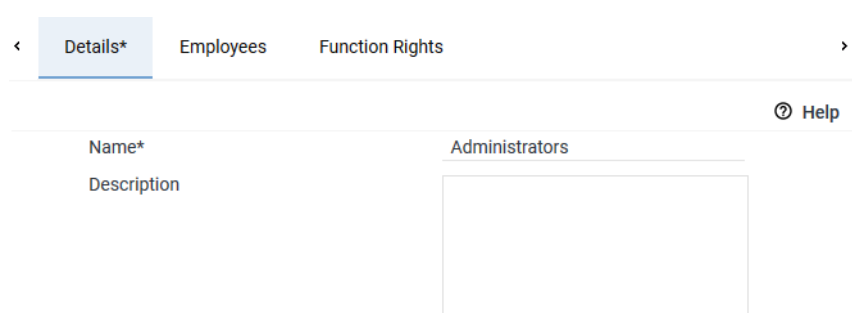


Fig. 91: Roles module - tab Details

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

6.2.2 Tab Employees

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

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

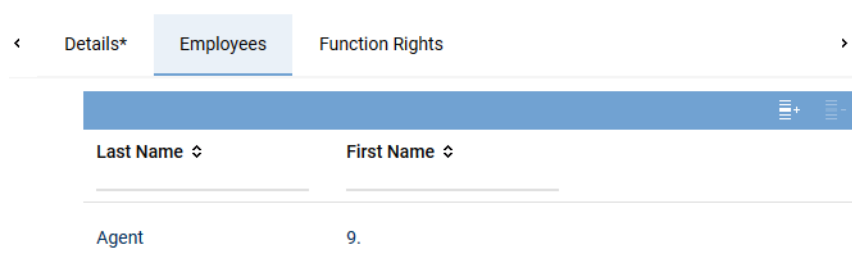



Fig. 92: Roles module - tab Employees



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

6.2.2.1 Assign users

1. Click on the icon  (Add).

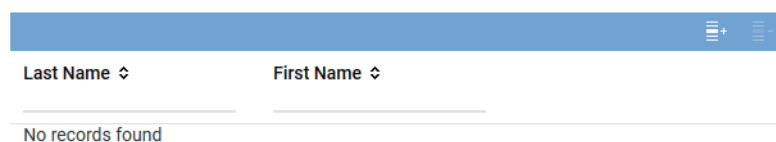
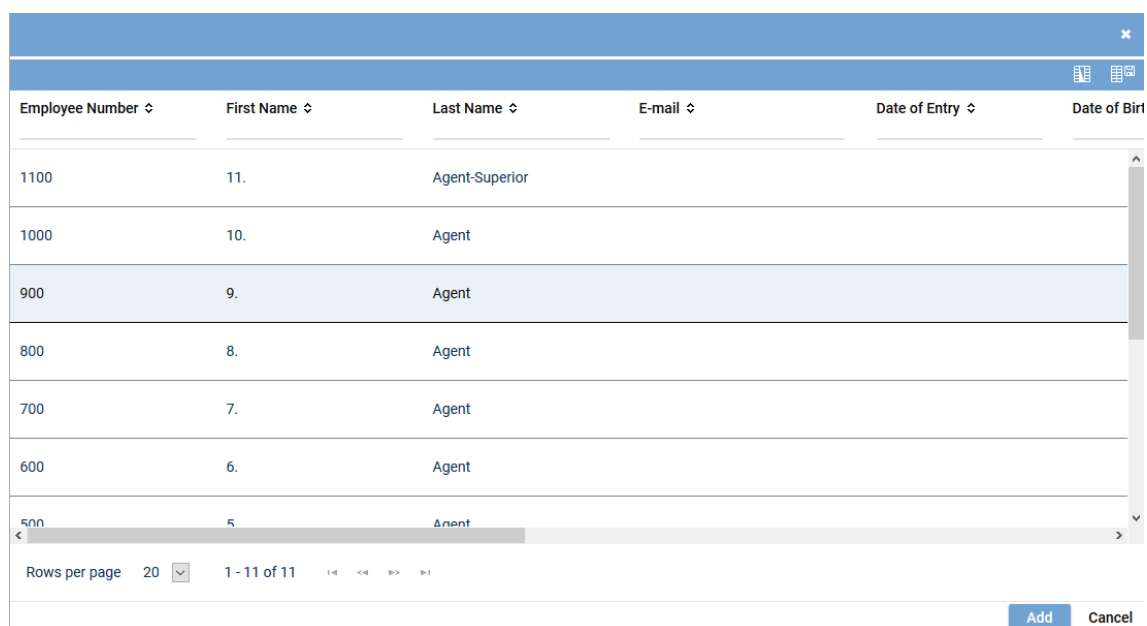


Fig. 93: Assign users

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




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. 94: Add user

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

6.2.2.2 Delete user assignment

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

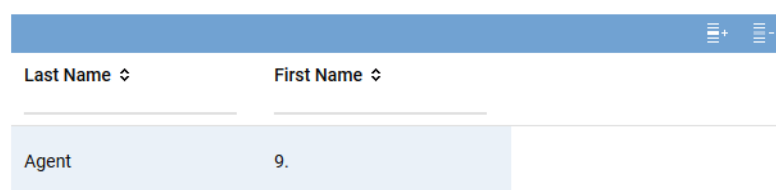


Fig. 95: Delete user assignment

6.2.3 Tab Function Rights

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



Fig. 96: 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.

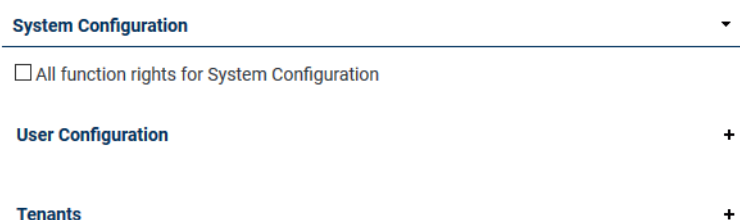


Fig. 97: Function rights - display sections (example)

- 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.

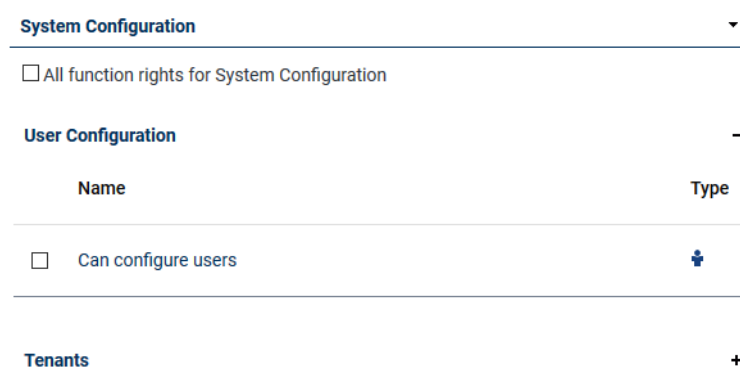





Fig. 98: Function rights - Display function rights

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)

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.

6.3

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 (see [chapter "Detail view", p. 77](#)).
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*.

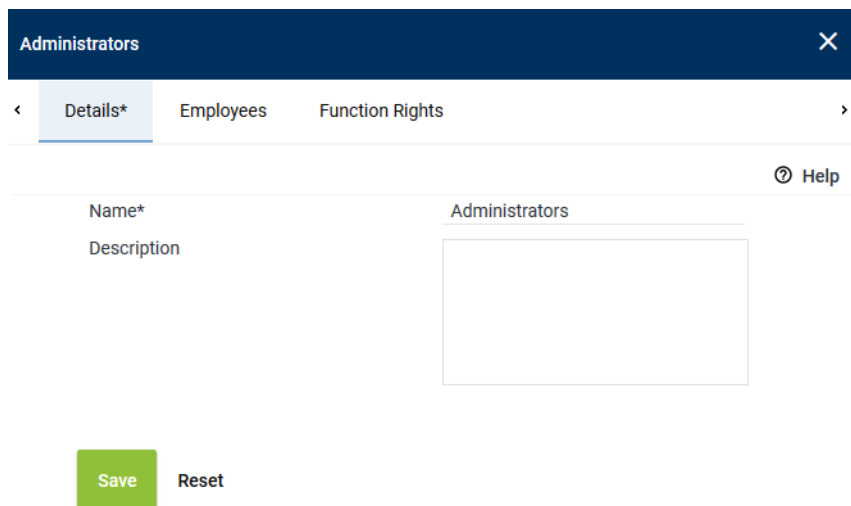


Fig. 99: Save role

6.4

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. 77](#)).
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**.

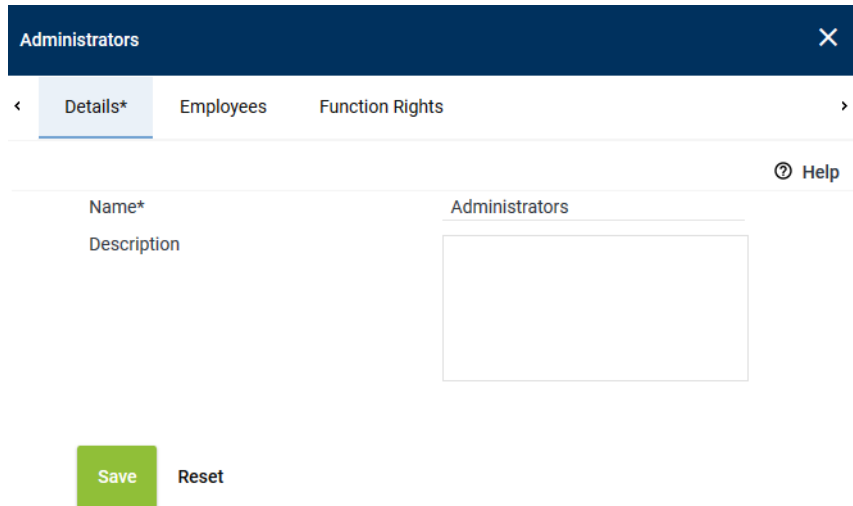


Fig. 100: Save role

6.5

Edit role

- In the main view, select the role you would like to edit.
- Make all necessary changes in the tabs of the detail view, see [chapter "Detail view", p. 77](#).
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**.

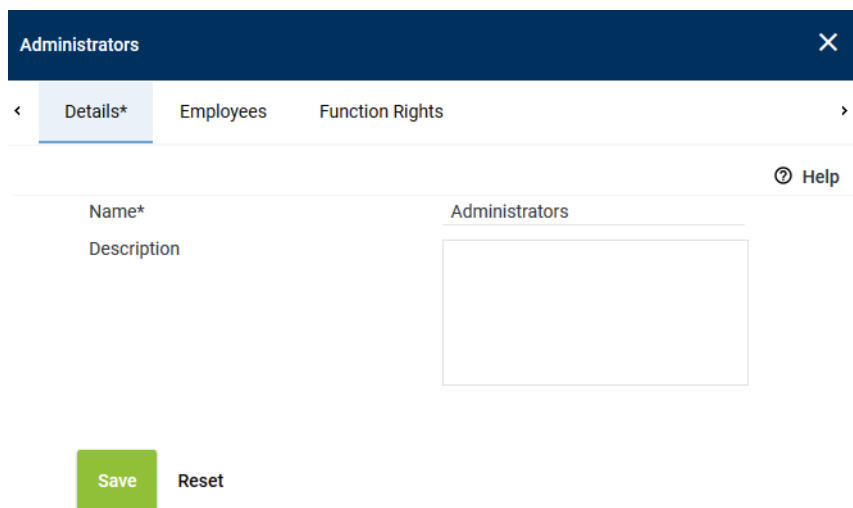



Fig. 101: Save changes

6.6

Delete role

- In the main view, select the role you would like to delete.
- Click on the icon  (**Delete**) in the toolbar.
- 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.

7

Predefined function packages

The *neo* system offers the following predefined function packages for the users of the system provider which provide them with selected function rights:

- **Superuser**

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

- **Superadmin**

Superadmin rights are only available in a Cloud environment and have to be activated when needed.

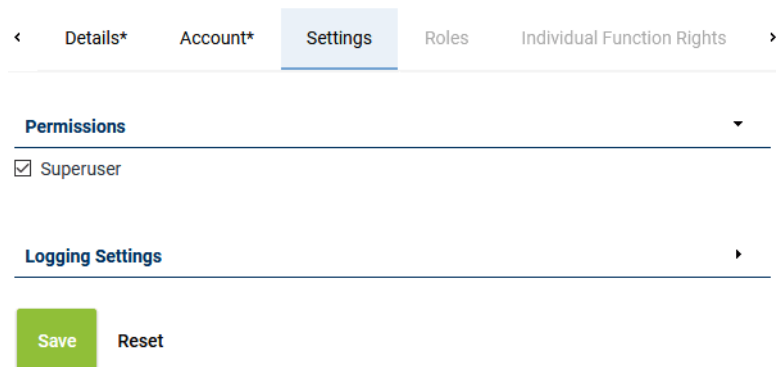
A superadmin has limited superuser function rights in the system.

Employees of the system provider who have been configured as superadmins can log in to the accounts of any tenant in the system with the rights of a superuser of this tenant.

7.1

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*.



Navigation tabs: Details*, Account*, **Settings**, Roles, Individual Function Rights

Permissions: ☒ Superuser

Logging Settings

Buttons: Save, Reset

Fig. 102: Create superuser

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

7.2

Create superadmin

1. Open the Employees module.
2. In the main view, select the user whom you would like to assign superadmin 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*.
6. Activate the check box in front of *Superadmin*.
NOTICE! The option *Superadmin* is only displayed if there is the respective license in the system.

[Details*](#) [Account*](#) [Settings](#) [Roles](#) [Individual Function Rights](#)

Permissions ▼
☒ Superuser
☒ Superadmin

Logging Settings ►

Fig. 103: Create superadmin

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

List of figures

Fig. 1	Tenants module - main view	12
Fig. 2	Tenants module - toolbar	12
Fig. 3	Tenants module - detail view for the tenant "System"	13
Fig. 4	Tenants module - detail view for normal tenants	14
Fig. 5	Tenants module - detail view for resellers.....	16
Fig. 6	Tenants module - detail view for normal tenants	17
Fig. 7	Add time zone	18
Fig. 8	The displayed entries in the table are filtered for ber (example).....	19
Fig. 9	Add time zone	19
Fig. 10	Add system availability.....	19
Fig. 11	Configure system availability.....	20
Fig. 12	Add address	20
Fig. 13	Add address	21
Fig. 14	Add contact person	21
Fig. 15	Add contact person	21
Fig. 16	Tenants module - tab Extensions.....	22
Fig. 17	Assign extensions to tenants	23
Fig. 18	Remove extensions.....	24
Fig. 19	Select extensions	25
Fig. 20	Tenants module - tab PBX Agent ID	26
Fig. 21	Assign PBX Agent IDs to tenants.....	26
Fig. 22	Select PBX Agent IDs	28
Fig. 23	Tenants module - tab Chat IDs	29
Fig. 24	Assign chat IDs to tenants	29
Fig. 25	Select chat IDs	31
Fig. 26	Tenants module - tab Passwords.....	31
Fig. 27	Define password length.....	32
Fig. 28	Define mandatory characters.....	33
Fig. 29	Configure password security.....	34
Fig. 30	Define forbidden passwords.....	35
Fig. 31	Define advanced password settings	35
Fig. 32	Edit entry in the list.....	36
Fig. 33	Tenants module - tab General Settings	36
Fig. 34	Configure user activity.....	36
Fig. 35	Add SMTP account	37
Fig. 36	Group field SNMP Agent (examples).....	39
Fig. 37	Configure login settings.....	40
Fig. 38	Configure miscellaneous settings	42
Fig. 39	Tenants module - tab LDAP Authentication	43
Fig. 40	LDAP Connection Data	43
Fig. 41	Edit LDAP connection data (example)	43

Fig. 42	Web service functionalities for the system provider	45
Fig. 43	Web service functionalities for the tenant	47
Fig. 44	Select export server	49
Fig. 45	Assign server	49
Fig. 46	Select server (example)	50
Fig. 47	Web service functionalities for the reseller.....	51
Fig. 48	Tenants module - tab PBX	52
Fig. 49	Assign PBX	53
Fig. 50	Add PBX.....	53
Fig. 51	Remove PBX assignment	53
Fig. 52	Tab System Licenses	54
Fig. 53	Tenants module - main view (example)	55
Fig. 54	Save tenant	56
Fig. 55	Save changes	57
Fig. 56	Employees module - main view	58
Fig. 57	Employees module - toolbar	59
Fig. 58	Summary of the function rights	60
Fig. 59	Window Search Criteria (example)	61
Fig. 60	Employees module - detail view	62
Fig. 61	Employees module - tab Details	63
Fig. 62	Edit employee information.....	63
Fig. 63	Upload image	65
Fig. 64	Upload File	65
Fig. 65	Delete image (example).....	65
Fig. 66	Add address	66
Fig. 67	Add address	66
Fig. 68	Add privacy statement and terms.....	66
Fig. 69	Add privacy statement and terms.....	66
Fig. 70	Employees module - tab Account	67
Fig. 71	Add account	67
Fig. 72	Activate authentication via LDAP	68
Fig. 73	Assign combination user	68
Fig. 74	Add combination user	69
Fig. 75	Delete combination user assignment.....	69
Fig. 76	Employees module - tab Settings	69
Fig. 77	Configure permissions	70
Fig. 78	Configure logging	71
Fig. 79	Employees module - tab Roles	71
Fig. 80	Assign roles.....	72
Fig. 81	Add role.....	72
Fig. 82	Delete role assignment	72
Fig. 83	Employees module - tab Individual Function Rights (example)	73

Fig. 84	Function rights - display sections (example)	73
Fig. 85	Function rights - Display function rights	73
Fig. 86	Save employee	74
Fig. 87	Save changes	75
Fig. 88	Roles module - main view	76
Fig. 89	Roles module - toolbar	76
Fig. 90	Roles module - detail view	77
Fig. 91	Roles module - tab Details	78
Fig. 92	Roles module - tab Employees	78
Fig. 93	Assign users.....	79
Fig. 94	Add user.....	79
Fig. 95	Delete user assignment	79
Fig. 96	Roles module - tab Function Rights (example).....	80
Fig. 97	Function rights - display sections (example)	80
Fig. 98	Function rights - Display function rights	80
Fig. 99	Save role	81
Fig. 100	Save role	82
Fig. 101	Save changes	82
Fig. 102	Create superuser	84
Fig. 103	Create superadmin.....	85

List of tables

Tab. 1	Login data - system provider	7
Tab. 2	Login data - 1st tenant	7
Tab. 3	Function rights.....	74
Tab. 4	Function rights.....	80

Glossary

CSV

Comma-separated values is a file format which stores tabular data in plain text form.

G.729A

G.729 Annex A is a codec for the compressing of audio into digital signals with low complexity, fixed point arithmetic and a data rate of 8 kbit/s.

IP

Internet Protocol, basic protocol for Internet communication

LDAP

Lightweight Directory Access Protocol

MIB

Management Information Base; file which defines the provided SNMP objects.

PBX

Private Branch Exchange

SMTP

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

SNMP

Simple Network Management Protocol is a network protocol and serves to monitor and manage network components. The protocol does not depend on the IP network protocol for the transport. It sends notifications (traps) about the activities on the network components on its own accord.

SSL

Secure Socket Layer

SSO

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

TLS

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

URL

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)

WSDL

Web Service Description Language; meta language which allows describing the offered functions, data, data types, and exchange protocols of a web service. (Source: Wikipedia 12th December 2014)

XML

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