System Configuration

User management

Administration manual

for system providers

9/9/2021

Product line *neo*, version 6.x

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

EVOIP*neo*

EVOLUTION*neo* / XXL / eco

INSPIRATION*neo*

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

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

Contents

1 General information

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

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

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

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

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

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

2 Introduction

The *neo* system has been designed as a potential multi-tenant system. This means several different tenants can be administered within one system. These tenants are created and administered by the system provider 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. The system provider is set up as tenant, too. However, the system provider is not another 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:	*system-admin*
neo version < 6.3	
Default password:	*1* If the default password *1* has never been changed before a software update to a *neo* version ≥ 6.3, the password must be changed upon the next login or by entering it again. If the default password has already been changed before a software update to a *neo* version ≥ 6.3, the changed password remains.
neo version ≥ 6.3	
Default password:	*A$c123*

Tab. 1: Login data - system provider

Login data for the administrator of the 1st tenant:

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

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:

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. 62.

- 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. 81.

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.

2 Introduction

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

3 LDAP

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

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

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

- Configure LDAP connection data.

  See chapter "Tab LDAP Connection Data", p. 44.
- Always activate LDAP authentication.

  See chapter "Group field Login Settings", p. 41.
- Activate LDAP authentication for individual users.

  See chapter "Authentication via LDAP", p. 72.

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.

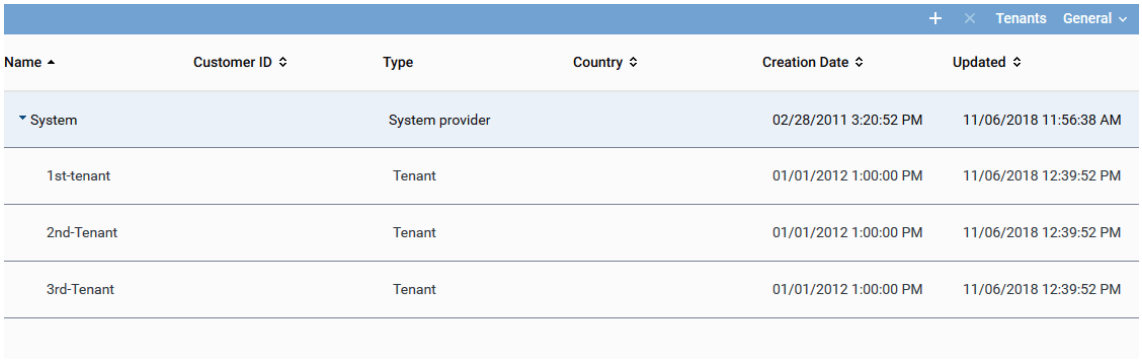

Fig. 1: Tenants module - main view

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

4.1.1 Toolbar

The toolbar offers the following functions.

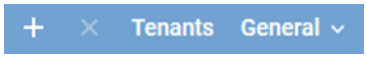

Fig. 2: Tenants module - toolbar

+	*Add*	Creates a new tenant or reseller (see chapter "Create new tenants manually", p. 57).
×	*Delete*	Deletes the selected tenant (see chapter "Delete tenant", p. 60).
Tenants		This menu is currently not available
General	*General Help*	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.

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

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

4.2 Detail view

The detail view contains additional information about and functions of 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

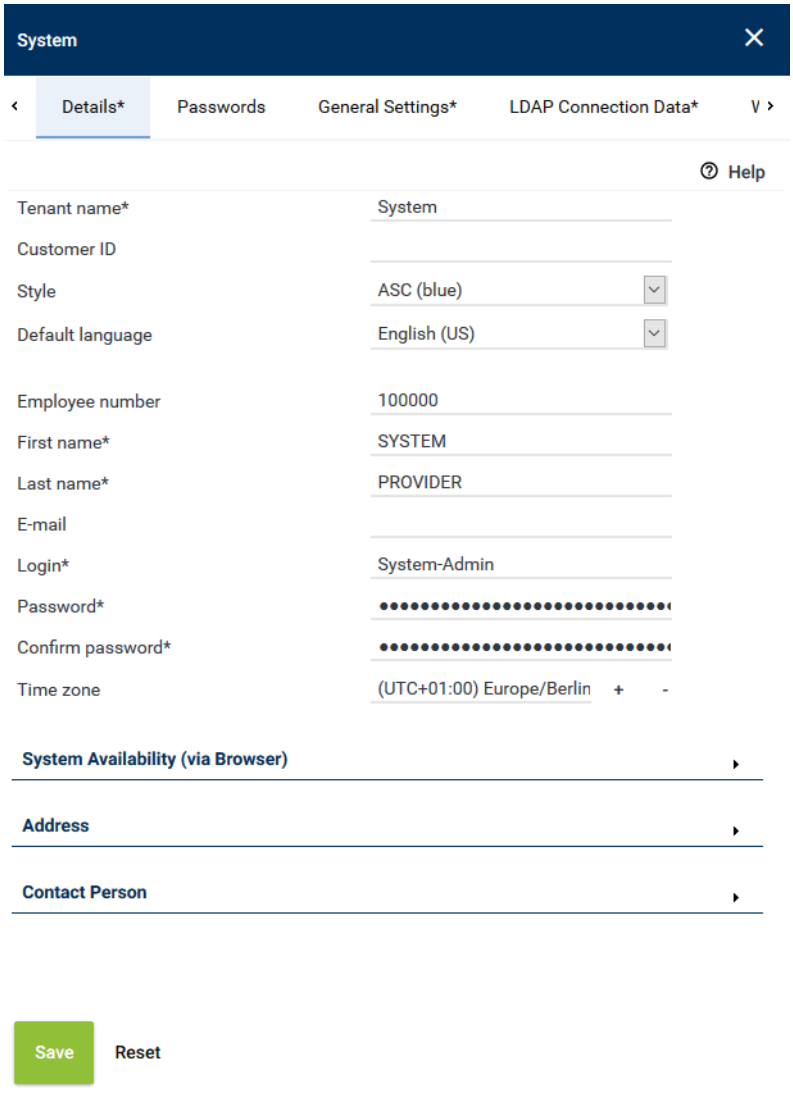

Fig. 3: Tenants module - detail view for the tenant “System”

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. 44.

- *Web Service*

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

  See chapter "Tab Web Service", p. 46.

4.2.2 Detail view for normal tenants

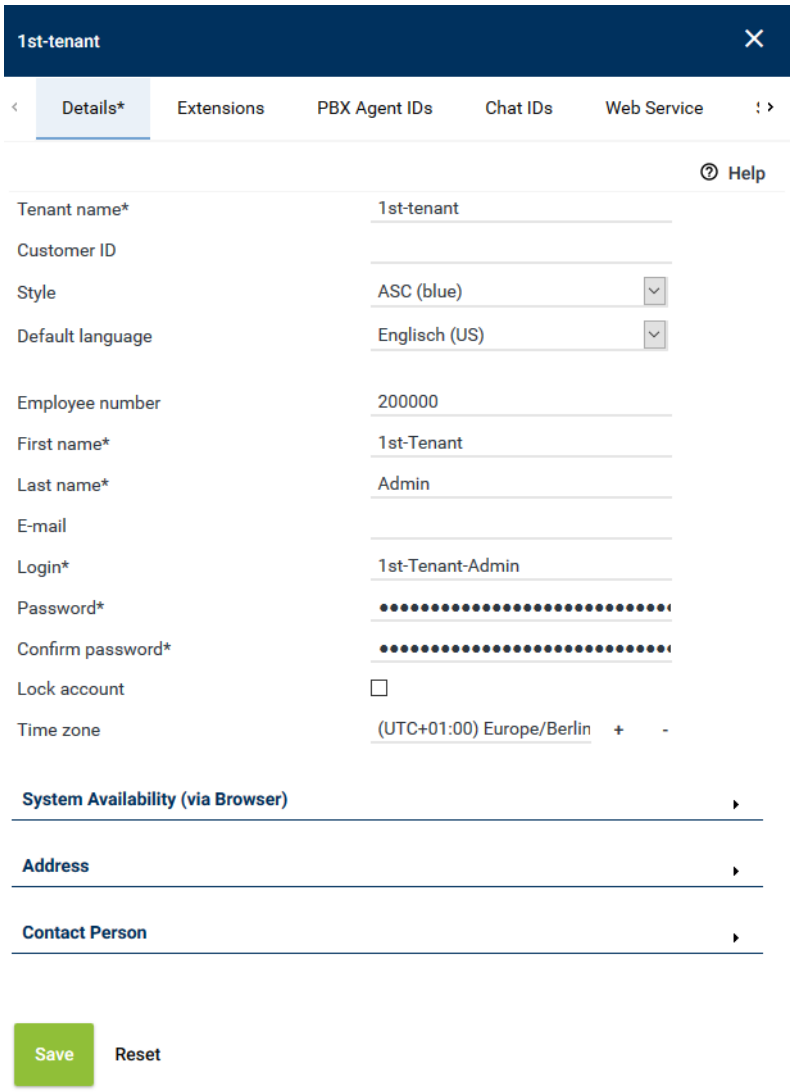

Fig. 4: Tenants module - detail view for normal tenants

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. 22.

- *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. 46.

- *Tenant Features*

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

  See chapter "Tab Tenant Features", p. 56.

4.2.3 Detail view for resellers

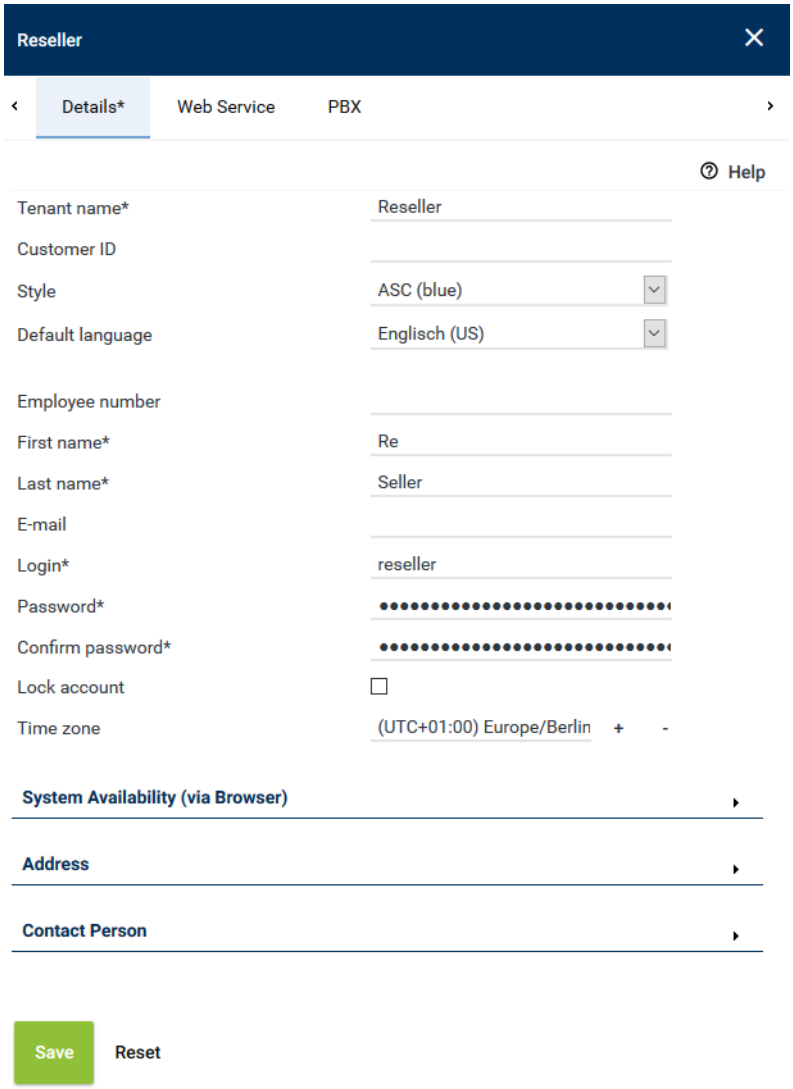

Fig. 5: Tenants module - detail view for resellers

The detail view consists of the following tabs:

- *Details*

  Here, you can display and edit the contact data 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. 46.

- *PBX*

  Here, you can activate and administrate PBX filters which have been assigned to the selected reseller.

  See chapter "Tab PBX", p. 54.

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.

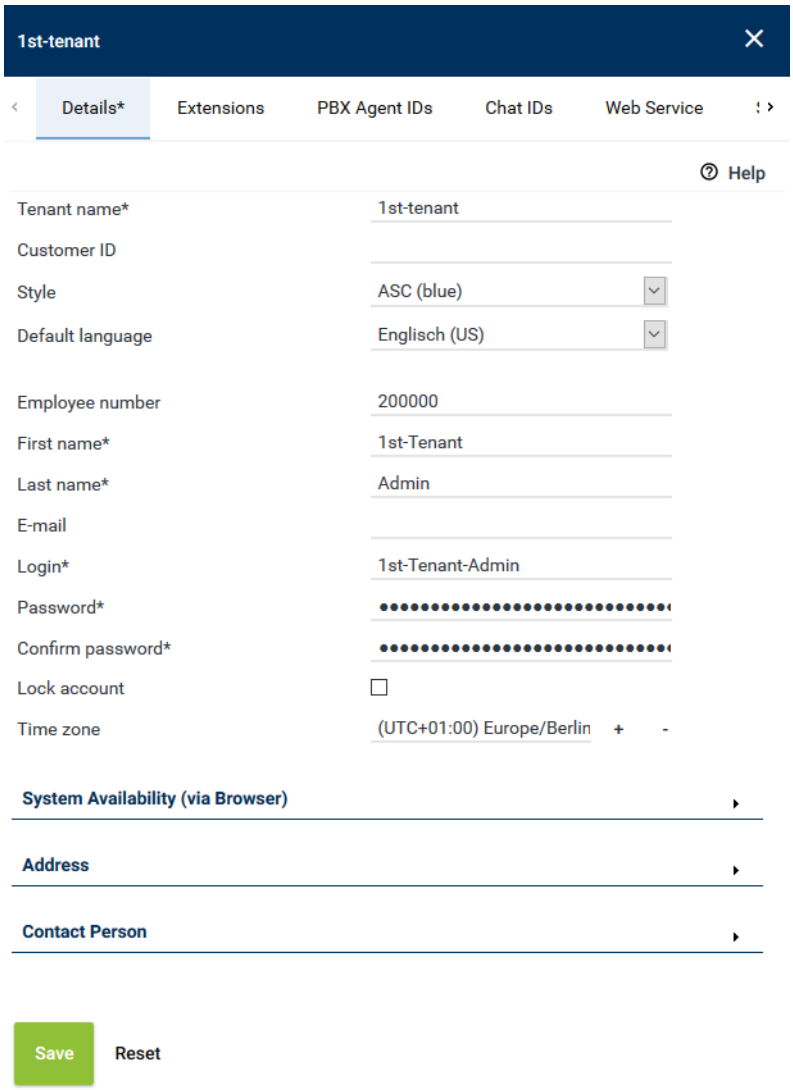

Fig. 6: Tenants module - detail view for normal tenants

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

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

Password	Password which is required for the administrator of the tenant to log in to the system.
Confirm password	Repetition of the password for the administrator.
Lock account	This option allows locking the tenant's account. The tenant can then no longer log in to *neo*. **NOTICE!** 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 *neo*.
Time zone	Shows the time zone in which the conversations are supposed to be displayed in the replay applications. This time zone is defined as a pre-setting for all other, newly created employees. If required, you can edit the time zone for each individual employee. The configuration in the Employees module is prioritized. To select the time zone, click on the button + . See chapter "Add time zone", p. 18. To delete the selection, click on the button - .

The information in the following group fields is optional:

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

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

4.2.4.1 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*:

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

3. Select a time zone from the list.

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

Fig. 10: System Availability (via Browser)

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

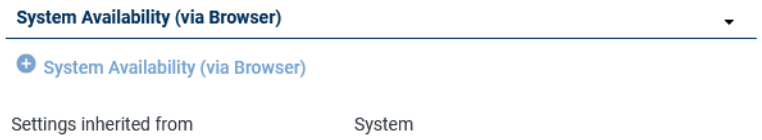

Fig. 11: System Availability (via Browser)

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

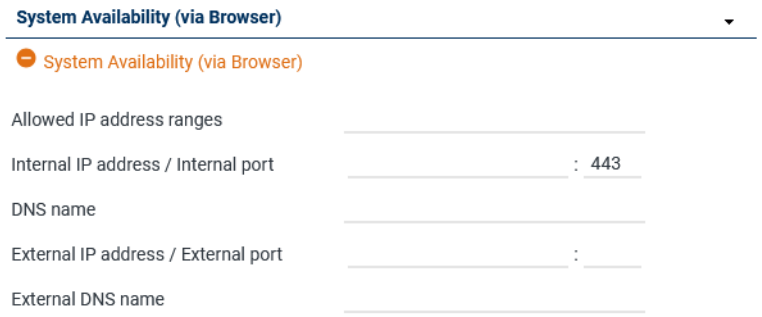

Fig. 12: Configure system availability

Allowed UP address ranges	Enter the IP address ranges under which the Replay module can be reached via the browser.
Internal IP address / Internal port	Enter the target IP address and the port of the replay server under which the Replay module can be reached internally.
DNS name	Enter the DNS name under which the Replay module can be reached internally.
External IP address / External port	Enter the URL or the IP address and the port under which the Replay module can be reached via the browser from outside the local network.
External DNS name	Enter the external DNS name under which the Replay module can be reached via the browser from outside the local network. **NOTICE!** If the SSL certificate has been issued for a DNS address, it is mandatory to enter the DNS name, otherwise the certificate check in the replay applications will fail.

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

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

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

4.2.4.3 Group field Address

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

Fig. 13: Add address

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

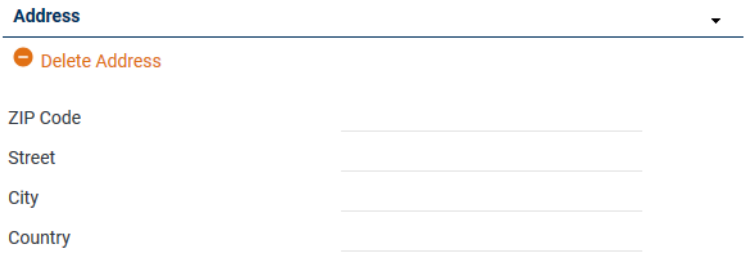

Fig. 14: Add address

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. 15: Add contact person

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

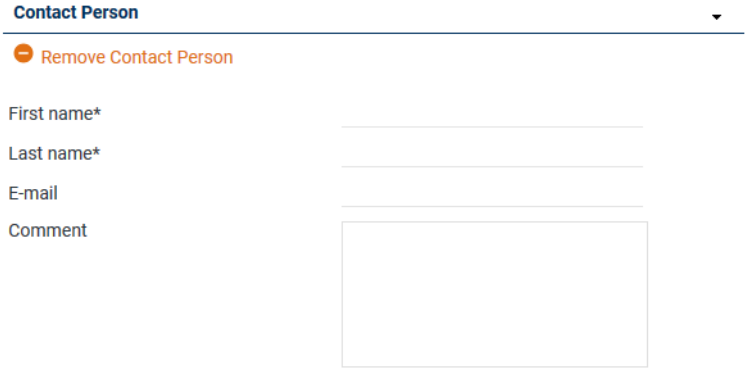

Fig. 16: Add contact person

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.

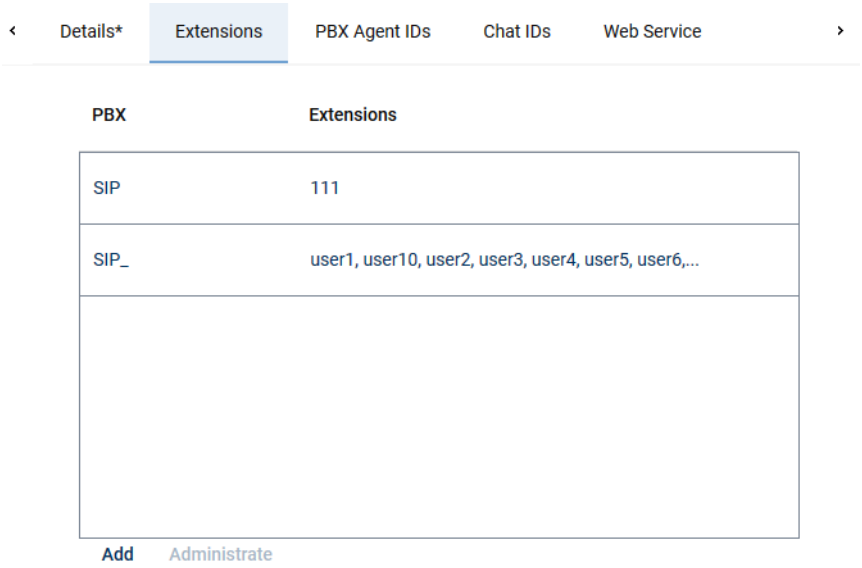

Fig. 17: Tenants module - tab Extensions

- 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:

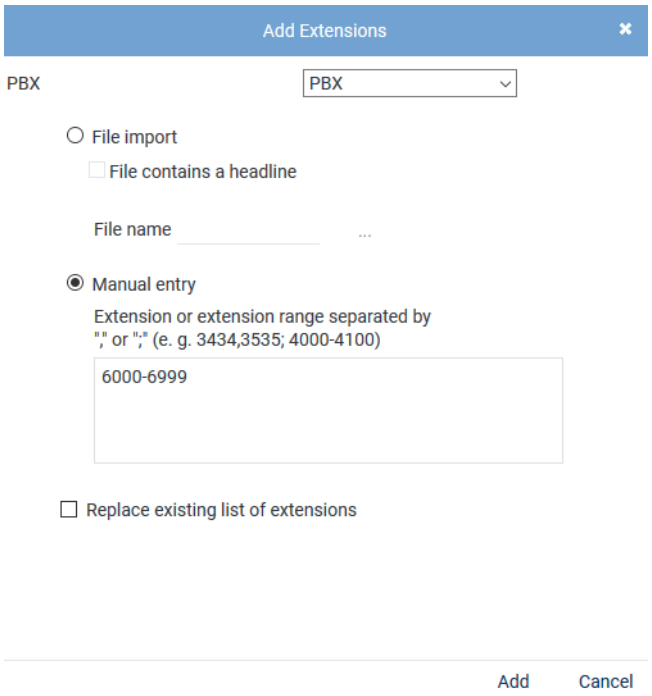

Fig. 18: Assign extensions to tenants

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

File import	Select the option to import extensions from an existing file and add them to the table of extensions. The following file formats are supported: • *ZIP* • *TXT* • *CSV* **NOTICE! The maximum number of extensions in a file has been limited to 2000 for performance reasons. If more extensions are required, you can import several files.**
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. The file must not contain more than one column. If commas or other column separators are detected in the file, the file is considered invalid and an error message is displayed.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective file in the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter extensions or extension ranges manually.

	To import number ranges, you must enter the same number of digits for the beginning and the end of the range, e. g. 1-9, 10-99, 01-20, 001-200, 4000-5000. If the end of the range asks for several digits, you have to add zeros for the beginning of the range, e. g. 01-10, 010-100. Enter country codes as number ranges as follows: +4984496800-+4984496810 **NOTICE! The number of digits must be equal. Add zeros in front of digits to level up possible incongruences.** **NOTICE! Wildcards cannot be used!**
Replace existing list of extensions	Activate the check box to replace the list of extensions. ☑ = Function has been activated; the entry replaces the extensions of the selected PBX. ☐ = Function has not been activated; the configured extensions of all PBXs are kept and the new extensions are added to the selected PBX.

5. Click on the button *Add*.
   ⇨ The extensions are added in the table of extensions.
6. If errors have been detect, 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.

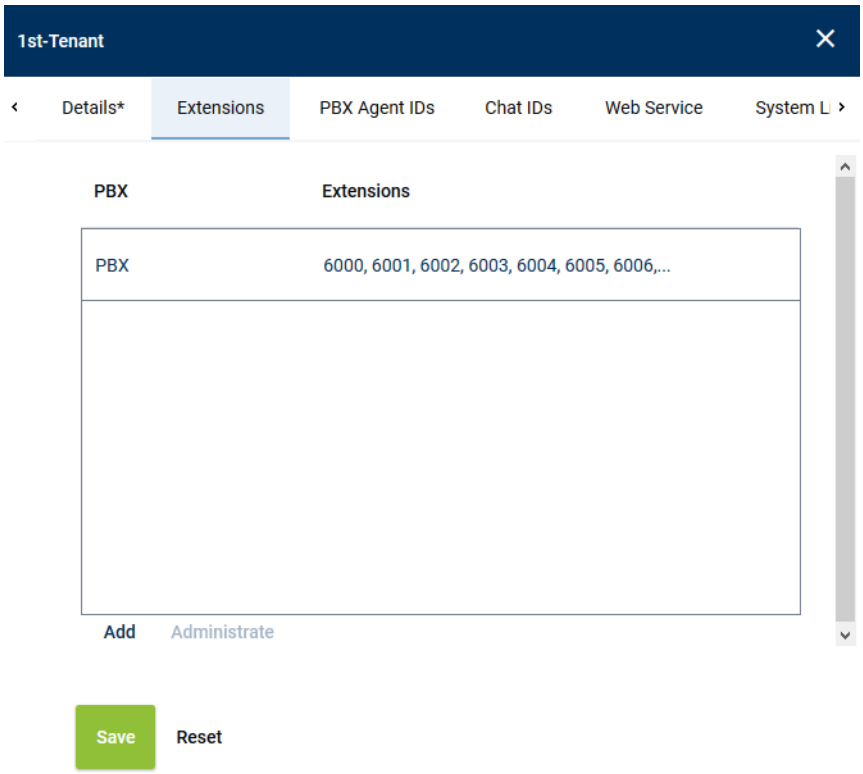

Fig. 19: Remove extensions

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. 20: 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.

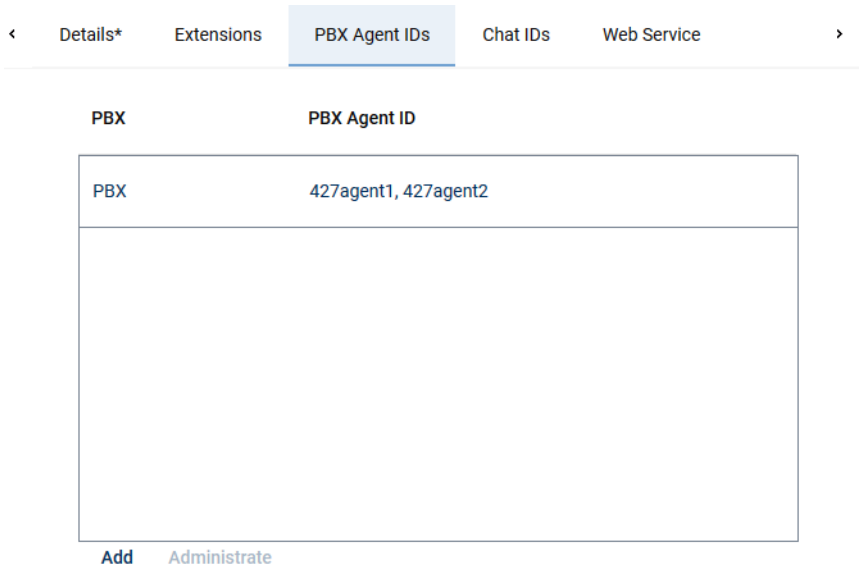

Fig. 21: Tenants module - tab PBX Agent ID

- 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:

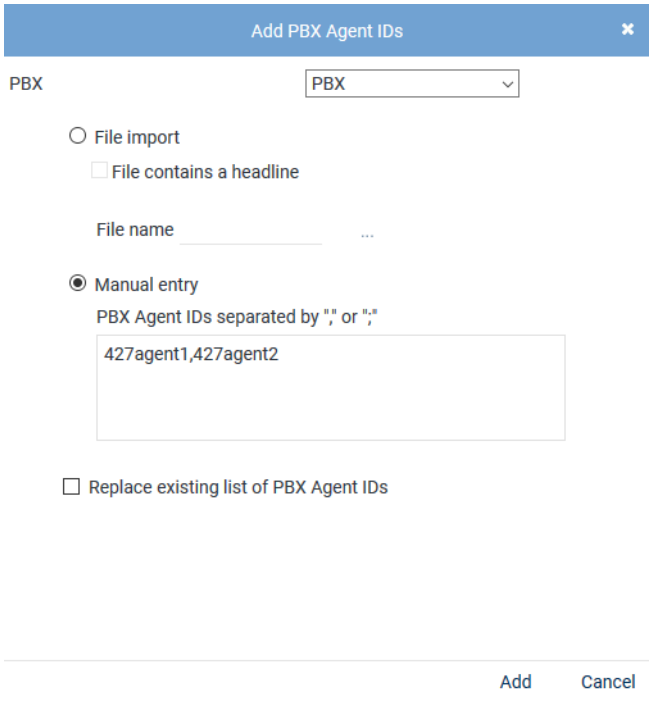

Fig. 22: Assign PBX Agent IDs to tenants

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

File import	Select the option to import PBX Agent IDs from an existing CSV file and add them to the table of PBX Agent IDs.
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. 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. 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.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter PBX Agent IDs manually. You can separate the individual PBX Agent IDs by the delimiters indicated in the screenshot. **NOTICE! Wildcards cannot be used!**
Replace existing list of PBX Agent IDs	Activate the check box to replace the list of PBX Agent IDs. ☑ = Function has been activated; the entry replaces the PBX Agent IDs of the selected PBX. ☐ = 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.

5. Click on the button *Add*.
   ⇨ The PBX Agent IDs are added to the table of PBX Agent IDs.
6. If errors have been detect, 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.

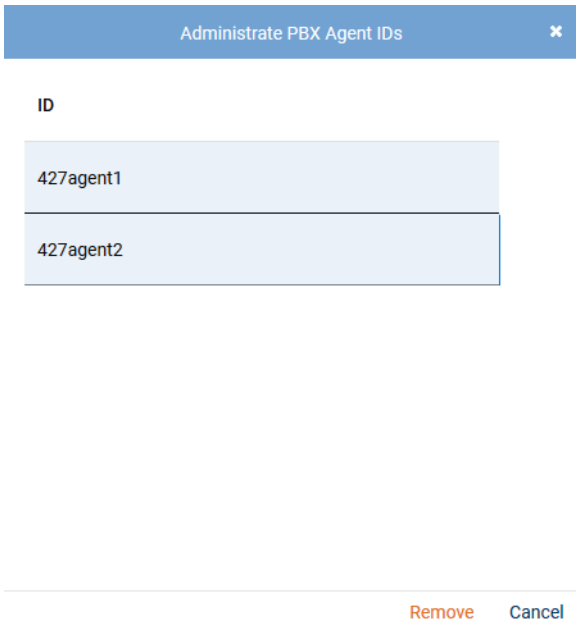

Fig. 23: Select PBX Agent IDs

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.

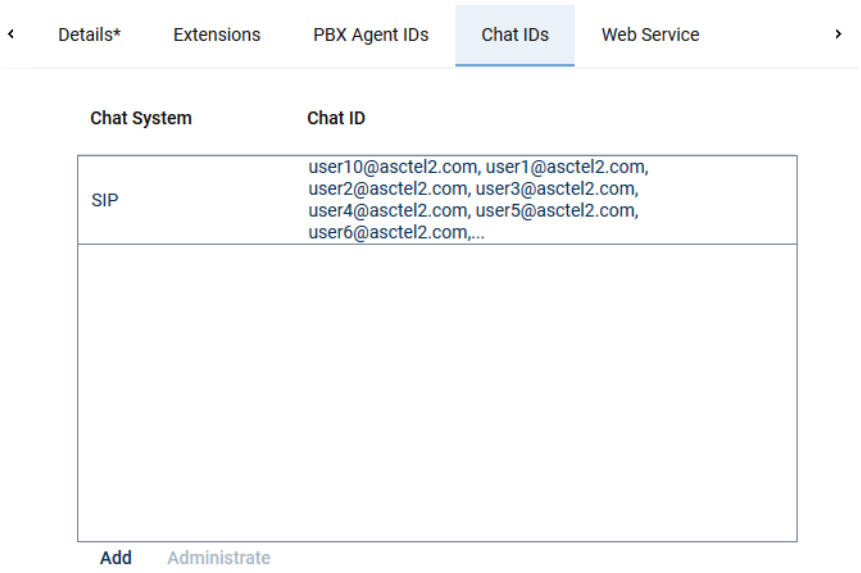

Fig. 24: Tenants module - tab Chat IDs

- 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:

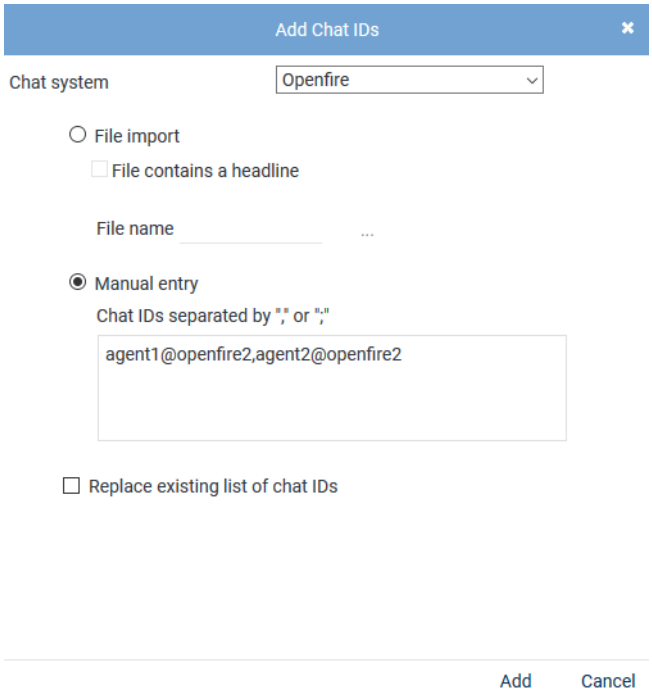

Fig. 25: Assign chat IDs to tenants

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

File import	Select this option to import the chat IDs from an existing CSV file and add them to the table of chat IDs.
	File contains a headline Activate this option so that this structed is recognized correctly when importing the file. 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. 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.
	File name To import the file, proceed as follows: • Click on the button ··· behind the field *File name*. • Click on the button *Choose File*. • Select the respective ZIP file via the Explorer and click on the button *Open*. • Click on the button *Upload File*.
Manual entry	Select this option to enter chat IDs manually. 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. **NOTICE! Wildcards cannot be used!**
Replace existing list of chat IDs	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. ☑ = Function has been activated; the entry replaces the chat IDs of the selected chat system. ☐ = Function has not been activated; the configured chat IDs are kept and the new chat IDs are added to the selected chat system.

5. Click on the button *Add*.
   ⇨ The chat IDs are added to the table of chat IDs.
6. If errors have been detect, 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.

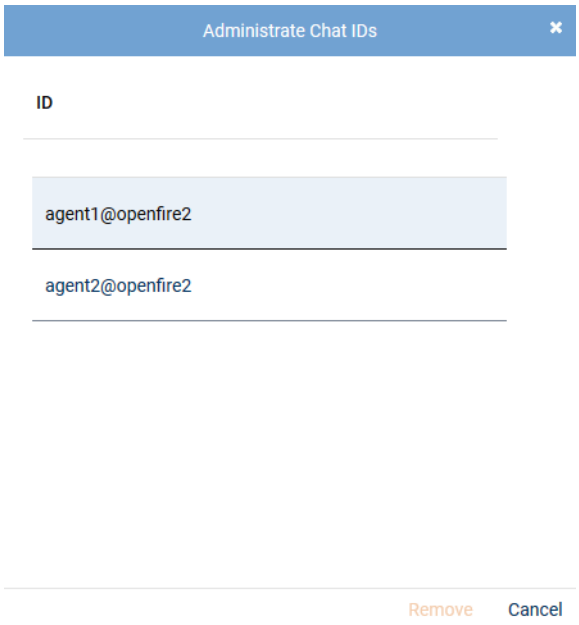

Fig. 26: Select chat IDs

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.

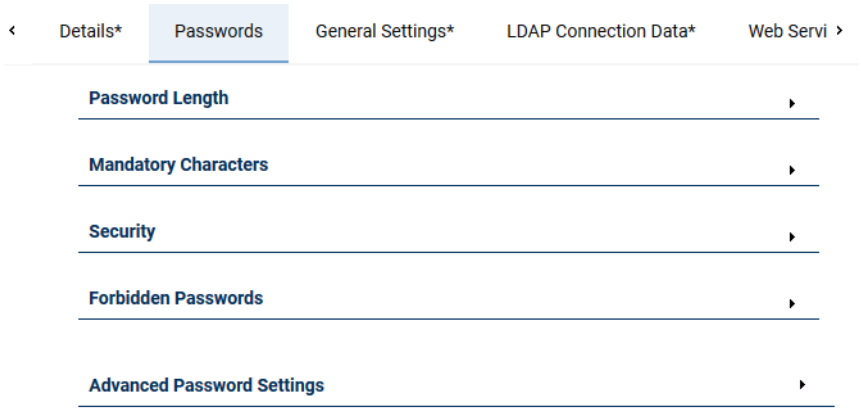

Fig. 27: Tenants module - tab Passwords

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

Exceptions:

- *Validity*

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

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

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

- Authentication via LDAP

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

Parameters containing the value *0* or no value at all are ignored.

Defining password rules is optional.

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

Group field Password Length

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

Fig. 28: Define password length

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

Group field Mandatory Signs

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

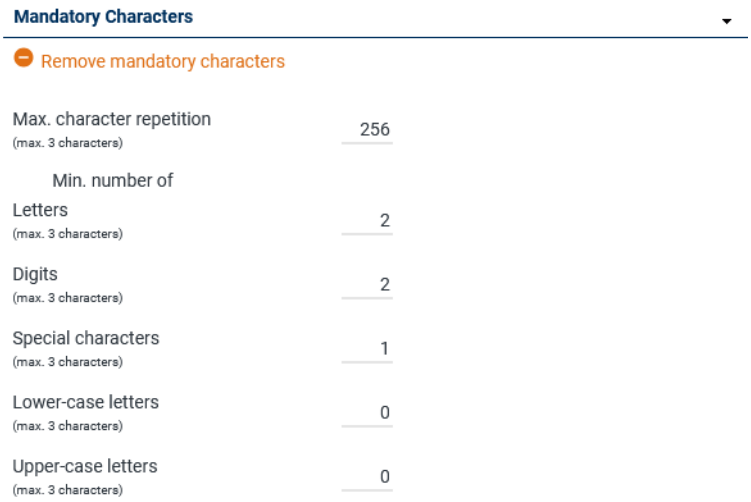

Fig. 29: Define mandatory characters

Max. character repetition	Enter how often a character may be repeated directly one after another. Examples: Max. character repetition: Valid: Invalid *0*: *abc*: *aabc* *1*: *aabcabc*: *aaabcabc* *2*: *aaabc*: *aaaabcabc*
Min. number of letters	Enter how many letters a password must contain at least.
Min. number of digits	Enter how many digits a password must contain at least.
Min. number of special characters	Enter how many special characters a password must contain at least. Valid special characters: Full stop: . Comma: , Semicolon: ; Colon: : Question mark: ? Exclamation mark: ! Quotation marks: "" Apostrophe: ' Hyphen: - Dash: / Brackets: () [] {} Hashtag: # Dollar sign: $ Percent sign: % Ampersand: & Asterisk: * Plus sign: + Inequality sign (greater-than, less-than sign): <>

	Equals sign	=
	At sign	@
	Caret	^
	Underscore	_
	Grave accent	`
	Pipe (vertical bar)	|
	Tilde	~
	All other punctuation characters are interpreted as letters.	
Min. number of lower-case letters	Enter how many lower-case letters a password must contain at least.	
Min. number of upper-case letters	Enter how many upper-case letters a password must contain at least.	

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

Group field Security

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

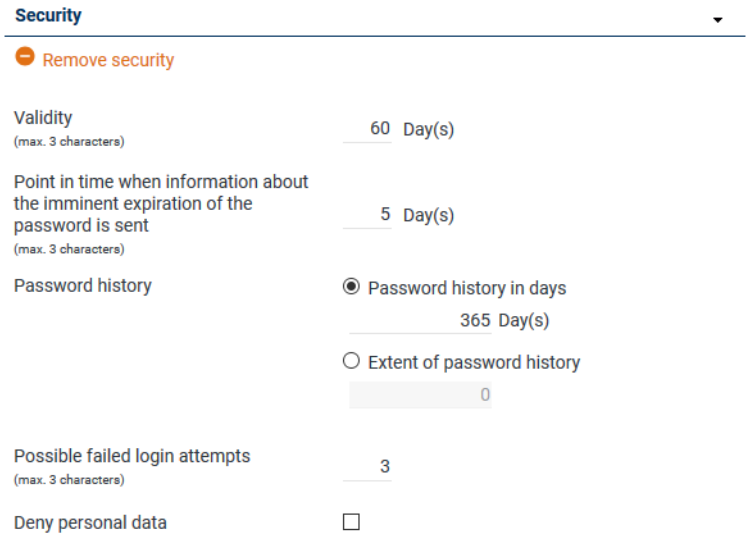

Fig. 30: Configure password security

Validity	Enter for how long a password is supposed to remain valid. *Validity = 0*: Passwords never expire
Point in time when information about the imminent expiration of the password is sent	Enter how many days before the expiration of the password users are to be reminded that they will have to change their password soon. *Point in time ... = 0*: User does not receive any information **NOTICE!** The value for the point in time to send information must be smaller than the value for the validity of the password.

Password history	Enter for how long the password history is supposed to be saved. Select one of the following options: • *Password history in days* For this option, enter for how long the passwords are supposed to be saved in the password history. • *Extent of password history* For this option, enter the number of passwords which are supposed to be saved in the password history. In both cases, the password history is never deleted entirely. If the entered value is reached, only the oldest entries are deleted.
Possible failed login attempts	Enter how often the user may enter an incorrect password before the account is locked. **NOTICE!** A locked account can be released again by any user with access to the Employees module and to the data of the locked user.
Deny personal data	Define whether users are allowed to use private data from their profiles for the password (e. g. name, user name, date of birth). ☑ = Personal data is not allowed. ☐ = Personal data is allowed.

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

Group field Forbidden Passwords

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

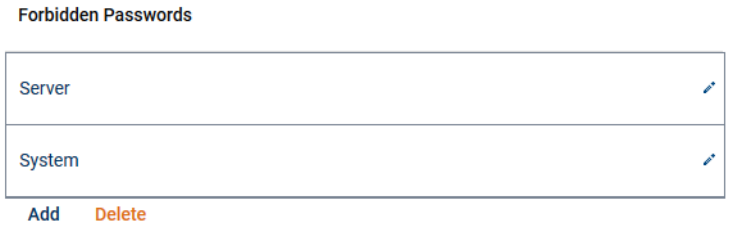

Fig. 31: Define forbidden passwords

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.

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

Use blacklist for passwords	☑ = Monitoring has been activated. ☐ = Monitoring has been deactivated. The entries in the list are ignored.

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

Group field Advanced Password Settings

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

Fig. 32: 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

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

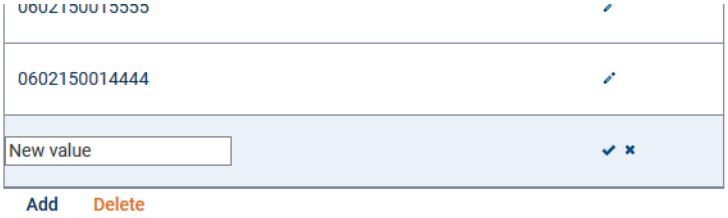

Fig. 33: Edit entry in the list

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

4.2.9 Tab General Settings

Here, you can change several general settings.

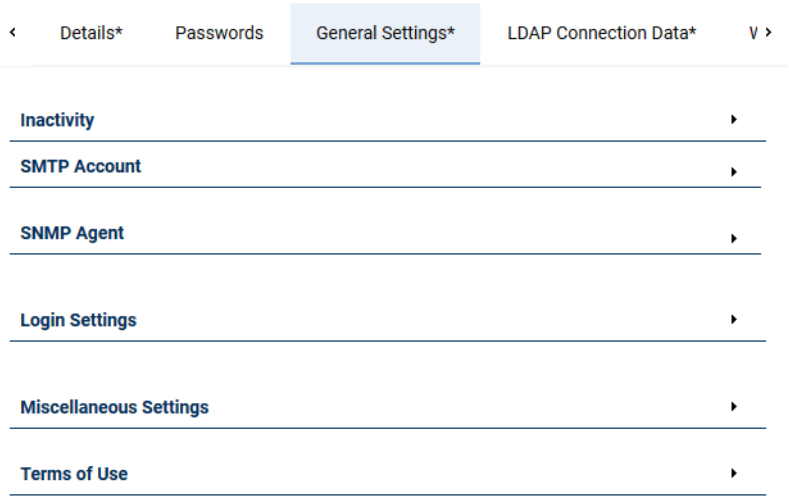

Fig. 34: Tenants module - tab General Settings

4.2.9.1 Group field Inactivity

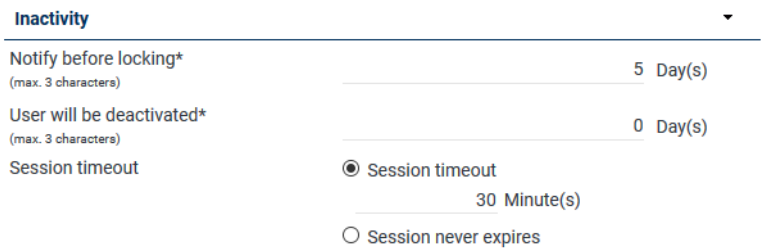

Fig. 35: Configure user activity

Notify before locking	Select how many days before the locking of the account the user is supposed to be notified that the account will be locked due to inactivity. The account is locked if the user has been inactive for the number of days entered in the field *User will be deactivated*. *Notify before locking = 0*: User is not notified. The notification is sent to the e-mail address of the user.
User will be deactivated	Select after how many days of inactivity the account of the user is locked. *User will be deactivated = 0*: User is not deactivated.
Session timeout	Select after how many minutes of inactivity the session of the user is supposed to be ended automatically by timeout. Select one of the following options: • *Session timeout* This option activates the session timeout. Enter a value between *5* and *1440*. • *Session never expires* This option deactivates the session timeout and enables endless sessions. **NOTICE!** Before activating this option, consider the following: If the user does not close the application by using the logoff function as recommended (menu item *(Logged in As) > Logoff*) but closes the browser directly, then the started session will never be finished. Each endless session consumes storage space. This may result in the necessity to reboot the server. Upon rebooting the server, all sessions are ended.

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

4.2.9.2 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*.

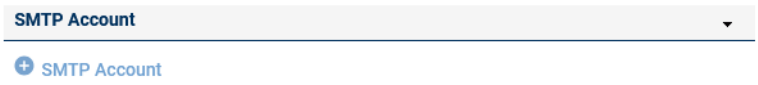

Fig. 36: SMTP account

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

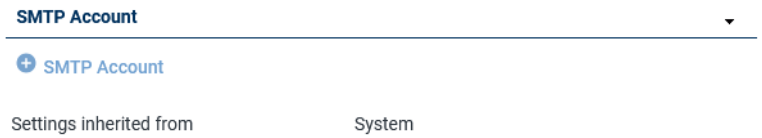

Fig. 37: SMTP account

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

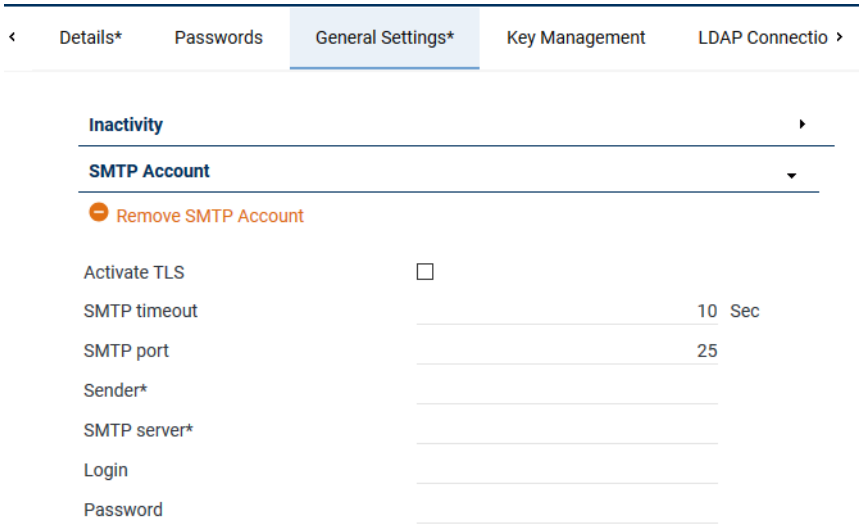

Fig. 38: Add SMTP account

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

6. Complete the following fields:

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

SMTP server	Enter the IP address or the name of the SMTP server on which the account has been created.
Login	Enter the login name for the authentication on the SMTP server.
Password	Enter the password for the authentication on the SMTP server.

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

4.2.9.3 Group field SNMP Agent

To enable the recording system to handle SNMPget requests of external monitoring programs, you must configure an SNMP agent here.

The recording system uses a native SNMP service for SNMPget requests. The SNMP service of the operating system is **not** used.

Deactivate the SNMP service of the operating system if you do not require it for any other applications.

Use a different network port for the “*neo*” SNMP agent than the default SNMP port of the operating system.

By means of SNMPget, the system status can be polled. 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 *DESCRIPTION* of the SMNP 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 *System Monitoring*.

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

1. To set up the function, open the group field *SNMP Agent*.
2. 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.

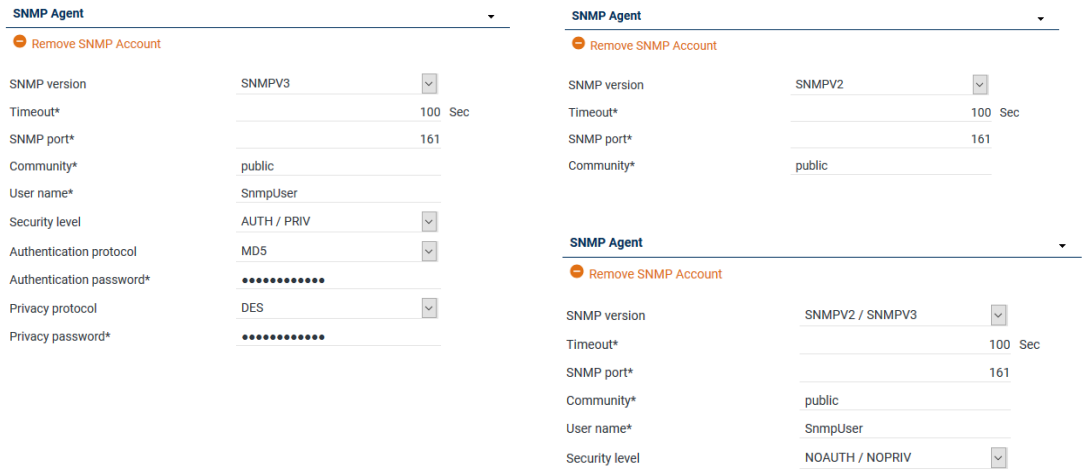

Fig. 39: Group field SNMP Agent (examples)

3. Complete all required fields:

SNMP version	From the drop-down list, select the SNMP version you would like to use. The following versions are available: • *SNMPV2* • *SNMPV2 / SNMPV3* • *SNMPV3*
Timeout	Enter after how many seconds a timeout notification is supposed to be sent if no connection to the SNMP server could be established.
SNMP port	Enter the port via the SNMP request are supposed to come in. Default value: *161* **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.
User name	(Only for SNMP versions *SNMPV2/SNMPV3* and *SNMPV3*.) Define the user name which has to be used for SNMP requests.
Security level	(Only for SNMP versions *SNMPV2/SNMPV3* and *SNMPV3*.) From the drop-down list, select the security level you would like to use. The following security levels are available: • *NOAUTH / NOPRIV* The external SNMP program does not have to authenticate. The SNMP answer is transferred without encryption. • *AUTH / NOPRIV* Select this option if you want the external SNMP program to authenticate while the SNMP answer is transferred without encryption. In this case, select a protocol type in the field *Authentication protocol* and enter a corresponding password in the field *Authentication password*. • *AUTH / PRIV* Select this option if you want the external SNMP program to authenticate and the SNMP answer to be transferred with encryption. In this case, select a protocol type in the field *Authentication protocol* and enter a corresponding password in the field *Authentication password*.

	In this case, additionally select a protocol type in the field *Privacy protocol* and enter a corresponding password in the field *Privacy password*.
Authentication protocol	(Only for security levels *AUTH / NOPRIV* and *AUTH / PRIV*.) Select the protocol that you would like to use for the authentication of the external SNMP program. The following protocol types are available: • *MD5* • *SHA*
Authentication password	(Only for security levels *AUTH / NOPRIV* and *AUTH / PRIV*.) Enter a password for the authentication here. Length of the password: 8 to 15 characters
Privacy protocol	(Only for security level *AUTH / PRIV*.) Select the protocol that you would like to use for the encryption of the SNMP answer. The following protocol types are available: • *DES* • *AES-128*
Privacy password	(Only for security level *AUTH / PRIV*.) Enter a password for the encryption of the SNMP answer here. Length of the password: 8 to 15 characters

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

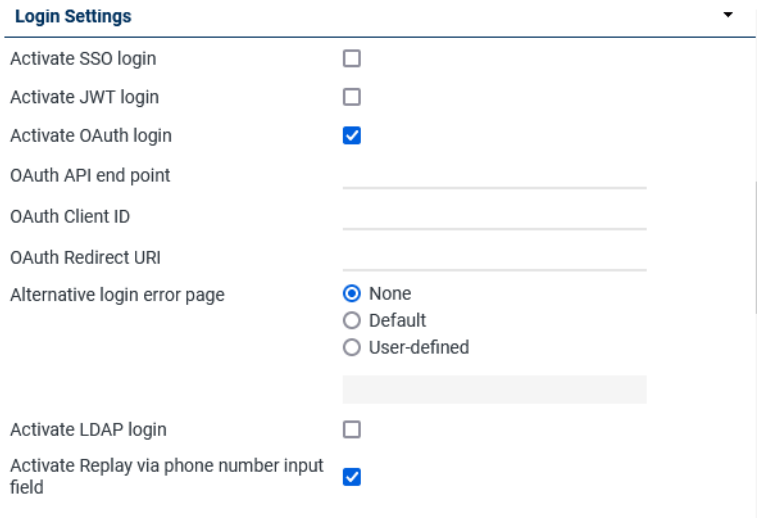

Fig. 40: Configure login settings

Activate SSO login	Here, you can activate or deactivate SSO login for the users of the recording system. Activate or deactivate the login via Single Sign On (SSO). ☑ = SSO login has been activated. ☐ = SSO login has not been activated. Upon activating the function here, all users of all tenants can use SSO. The individual tenants do not have to make any further configurations. **The only other condition** for using SSO: • 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. **NOTICE!** If you activate SSO login as well as LDAP login, the LDAP data is 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 an 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 user 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*.
Activate OAuth login	Here, you can activate or deactivate the authentication by means of OAuth login for the users of the recording system. Activate or deactivate the authentication by means of OAuth. ☑ = activated ☐ = not activated
OAuth API endpoint	Here, you can enter the OAuth API endpoint (e. g. https://authentication.example.org.token).
OAuth Client ID	Here, you can enter an OAuth Client ID (e. g. ef0129223a2e3bf76e7c3d8422b15b).
OAuth Redirect URI	Here, you can enter the OAuth Redirect URI.
Alternative login error page	Here, you can activate that an alternative login page is displayed in case of an invalid login. Activate that an alternative login page in case of an invalid login is displayed.

	• *None* This option does not activate an login error page. In case of a login error, an error message is displayed in the login screen. Upon closing the error message, users can try to log in once again. • *Default* This option activates that a default alternative page in case of an invalid login is displayed. In case of a login error, a new page is displayed. This page explains that the login has failed and asks the user to contact the administrator. • *User-defined* This option activates that a user-defined alternative page in case an invalid login is displayed. Enter a corresponding web address in the entry field (e. g. www.example-login-error.de). In case of a login error, users are forwarded to the entered web address.
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 is ignored if users log in with their Windows accounts. **NOTICE!** LDAP login cannot be activated before you have configured at least one LDAP connection, see chapter "Tab LDAP Connection Data", p. 44.
Activate Replay via telephone number input field	Activate or deactivate the entry field to enter the replay via phone number when logging in to POWER*play* Web. ☑ = Field to enter replay via phone number is displayed on the login screen of POWER*play* Web. ☐ = Field to enter replay via phone number is not displayed on the login screen of POWER*play* Web.

4.2.9.5 Group field Miscellaneous Settings

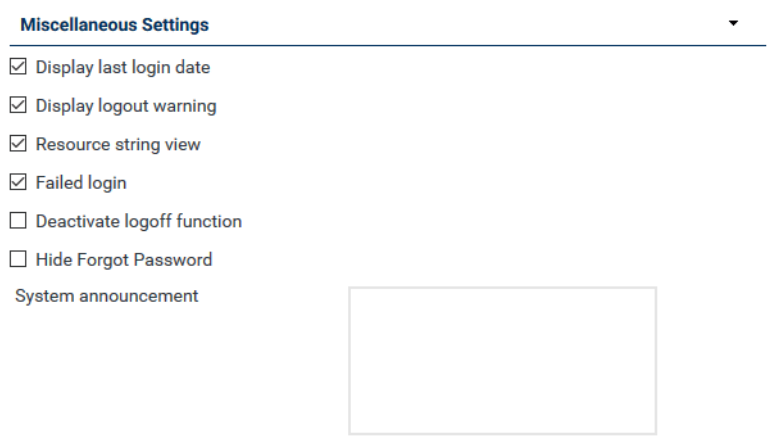

Fig. 41: Configure miscellaneous settings

Display last login date	Select whether you would like to have the date of the last login displayed in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Display logout warning	Select whether you would like to issue a logout warning in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Resource string view	Select whether you would like to display the button to activate the resource string view in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Failed login	Select whether you would like to display the information about a failed login in all applications. ☑ = Displaying information has been activated. ☐ = Displaying information has not been activated.
Deactivate logoff function	Select whether you would like to display the logoff function (menu item *(Logged in as) > Logoff*). ☑ = Logoff function is not displayed. ☐ = Logoff function is displayed.
Hide Forgot Password	Select whether you would like to display the function *Forgot Password?* in the login windows. ☑ = Function *Forgot Password?* is not displayed. ☐ = Function *Forgot Password?* 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 *neo* application.

4.2.9.6 Group field Terms of Use

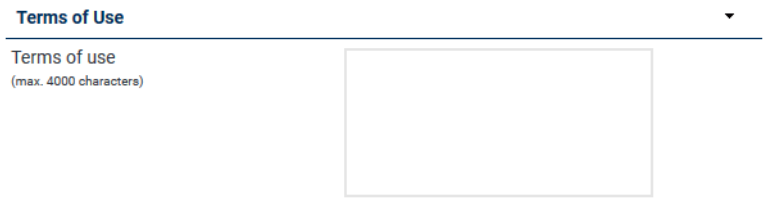

Fig. 42: Configure terms of use

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

4.2.10 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. 41).

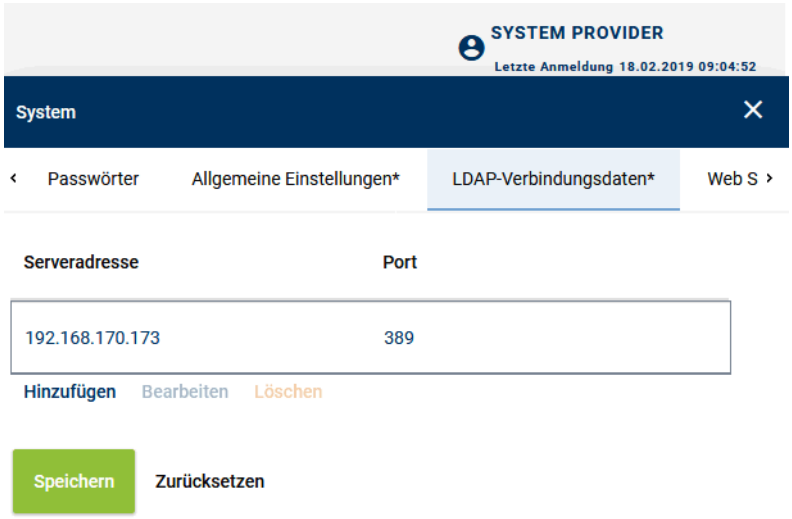

Fig. 43: Tenants module - tab LDAP Authentication

Add	Opens a window in which you can add a new LDAP connection (see chapter "Edit LDAP connection data", p. 45).
Edit	Opens the selected entry for editing (see chapter "Edit LDAP connection data", p. 45).
Delete	Deletes the selected entry from the list.

4.2.10.1 Edit LDAP connection data

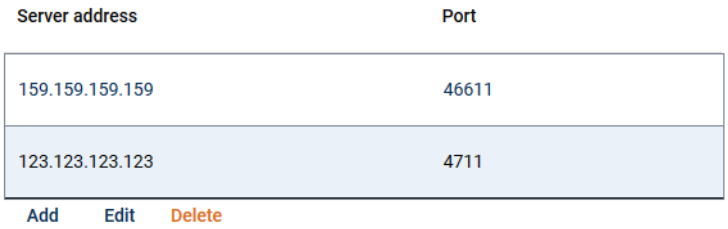

Fig. 44: LDAP Connection Data

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

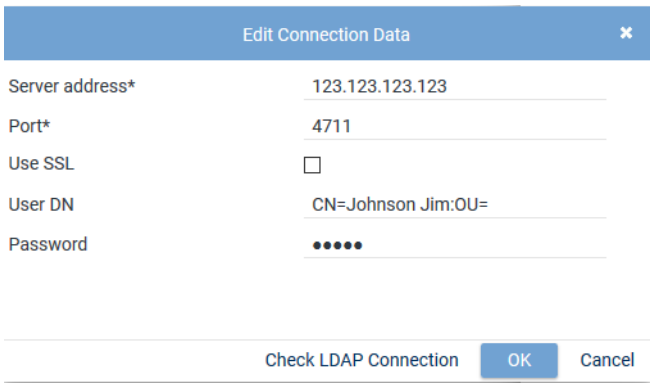

Fig. 45: Edit LDAP connection data (example)

Server address	IP address of the LDAP server.
Port	Port on the LDAP server which is used to establish a connection.

	By default, the following port is used: 389 = LDAP connection, unencrypted 636 = LDAP connection, encrypted
Use SSL	Activate or deactivate the usage of the SSL protocol. ☑ = SSL is used. ☐ = SSL is not used. **NOTICE!** SSL can only be used if the LDAP server supports SSL.
User DN	Distinguished name (DN) of the user required for the authentication to the LDAP server.
Password	Password required for the authentication to the LDAP server.

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

4.2.11 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*.

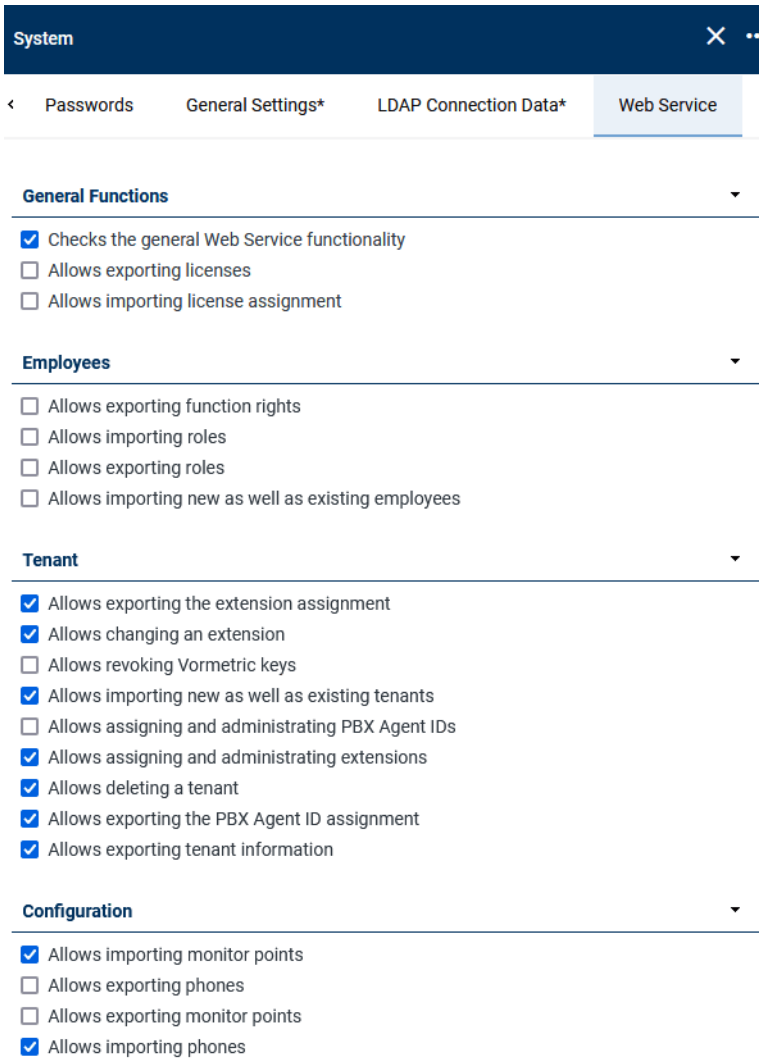

Fig. 46: Web service functionalities for the system provider

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 general function.

Checks the general web service functionality	Activate the check box, if you would like to allow checking the general web service functionality.
Allows exporting licenses	Activate the check box if you would like to allow exporting licenses.
Allows importing license assignment	Activate the check box if you would like to allow importing the license assignment.

Group field Employees

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

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

Allows exporting roles	Activate the check box if you would like to allow the tenant to export roles via the Web Service.
Allows importing new as well as existing employees	Activate the check box if you would like to allow the tenant to import new and already existing employees via the Web Service.

Group field Tenant

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

Allows exporting the extension assignment	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
Allows changing an extension	Activate the check box if you would like to allow the tenant to change an extension via the Web Service.
Allows revoking Vormetric keys	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
Allows importing new as well as existing tenants	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.
Allows assigning and administrating PBX Agent IDs	Activate the check box if you would like to allow the tenant to assign and administrate Agent PBX IDs via the Web Service.
Allows assigning and administrating extensions	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
Allows deleting a tenant	Activate the check box if you would like to allow the tenant to delete a tenant via the Web Service.
Allows exporting the PBX Agent ID assignment	Activate the check box if you would like to allow the tenant to export the PBX Agent ID assignment via the Web Service.
Allows exporting tenant information	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.

Group field Configuration

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

Allows importing monitor points	Activate the check box if you would like to allow the tenant to import monitor points via the Web Service.
Allows importing phones	Activate the check box if you would like to allow the tenant to import phones via the Web Service.
Allows exporting phones	Activate the check box if you would like to allow the tenant to export phones via the Web Service.
Allows exporting monitor points	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 functions 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 that you would like to enter the settings for.
2. Select the tab *Web Service*.

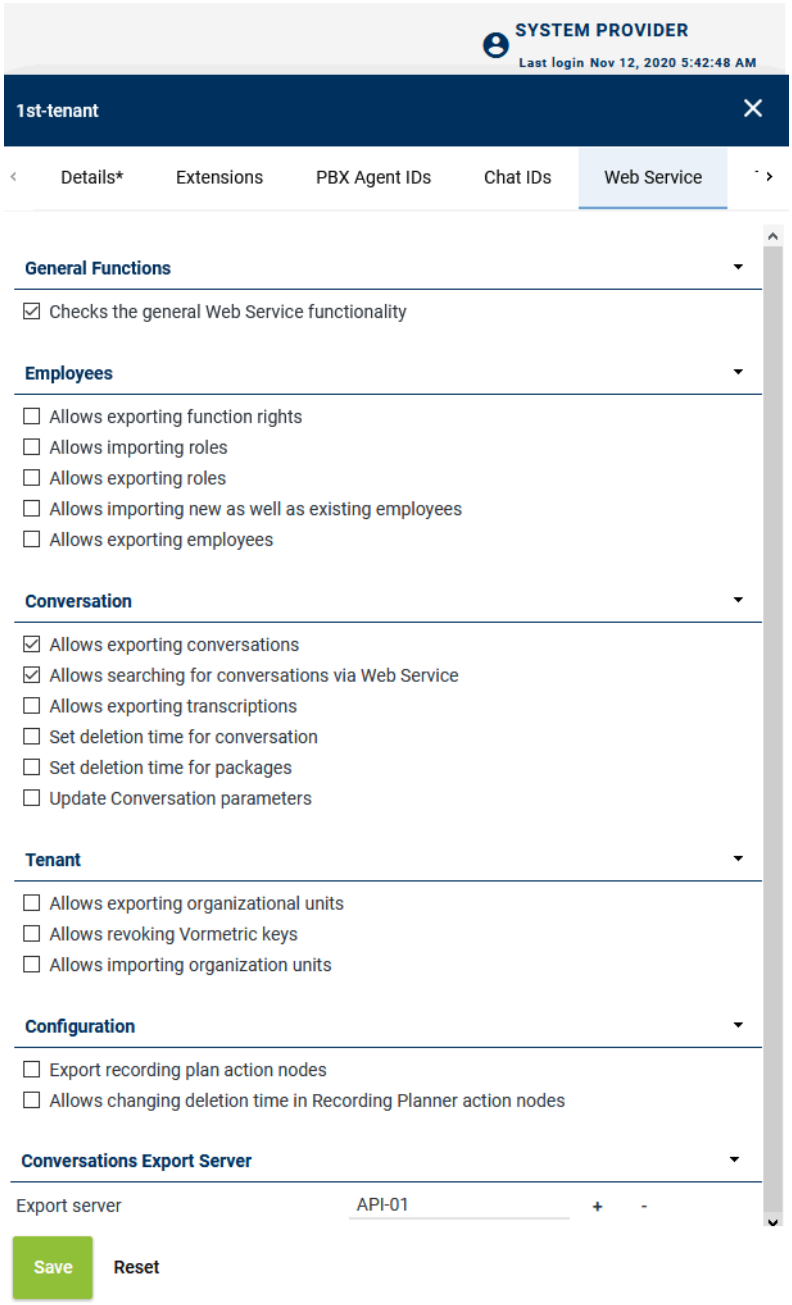

Fig. 47: Web Service functions for the tenant

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 general function.

Checks the general web service functionality	Activate the check box, if you would like to allow checking the general web service functionality.
Allows exporting licenses	Activate the check box if you would like to allow exporting licenses.
Allows importing license assignment	Activate the check box if you would like to allow importing the license assignment.

Group field Employees

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

Allows exporting function rights	Activate the check box if you would like to allow the tenant to export function rights via the Web Service.
Allows importing new as well as existing employees	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.
Allows importing roles	Activate the check box if you would like to allow the tenant to import roles via the Web Service.
Allows exporting roles	Activate the check box if you would like to allow the tenant to export roles via the Web Service.
Allows exporting employees	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.

Allows exporting conversations	Activate the check box if you would like to allow the tenant to export conversations via the Web Service. **NOTICE!** If you activate this function, you must enter an export server in the group field *Conversations Export Server*
Allows searching for conversations via Web Service	Activate the check box if you would like to allow the tenant to search conversations via the Web Service.
Allows exporting transcriptions	Activate the check box if you would like to allow the tenant to export transcriptions via the Web Service.
Set deletion time for conversations	Activate the check box if you would like to allow the tenant to set a deletion time for conversations via the Web Service.
Set deletion time for packages	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.

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

Group field Configuration

Allows importing audio analysis configurations	Shows whether importing audio analysis configurations is possible.
Allows importing Recording Planner action nodes	Shows whether importing Recording Planner action nodes is possible.
Allows exporting audio analysis configurations	Shows whether exporting audio analysis configurations is possible.

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

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.

Export server	Click on the button + next to the field *Export server*.

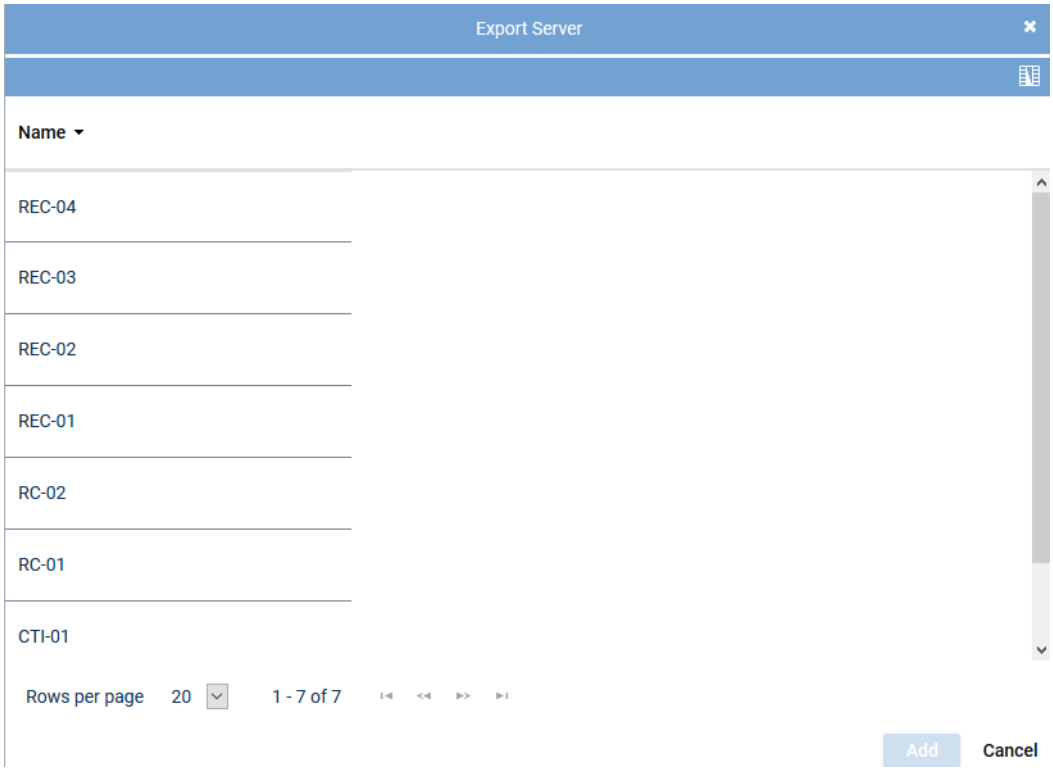

Fig. 48: Select export server

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. 49: Assign server

2. Select the appropriate server from the list.

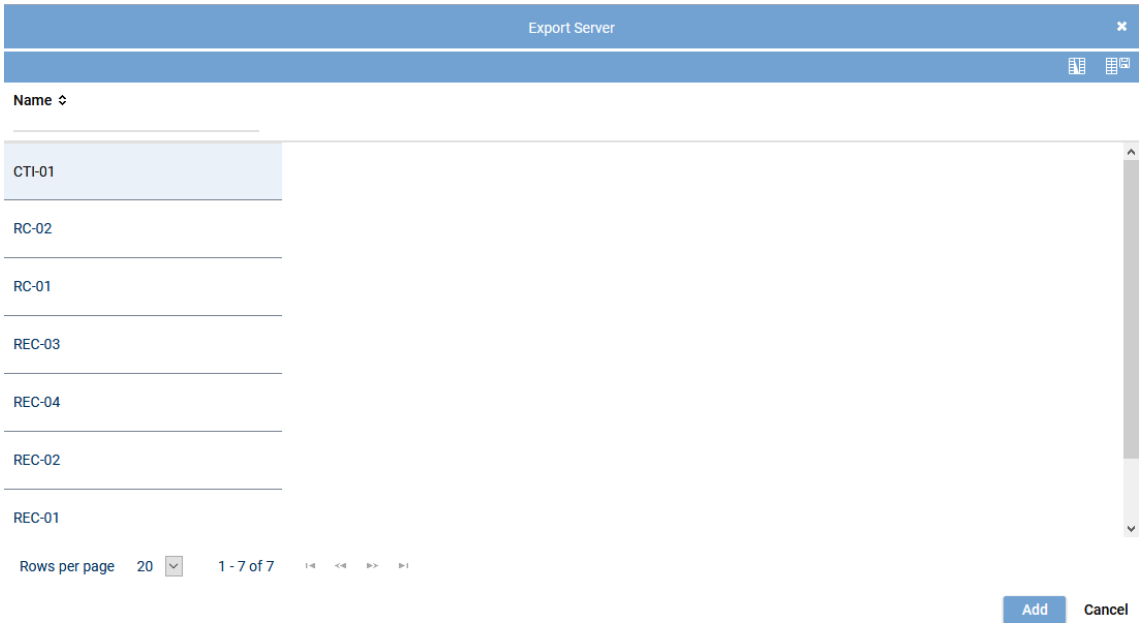

Fig. 50: Select server (example)

3. 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.

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

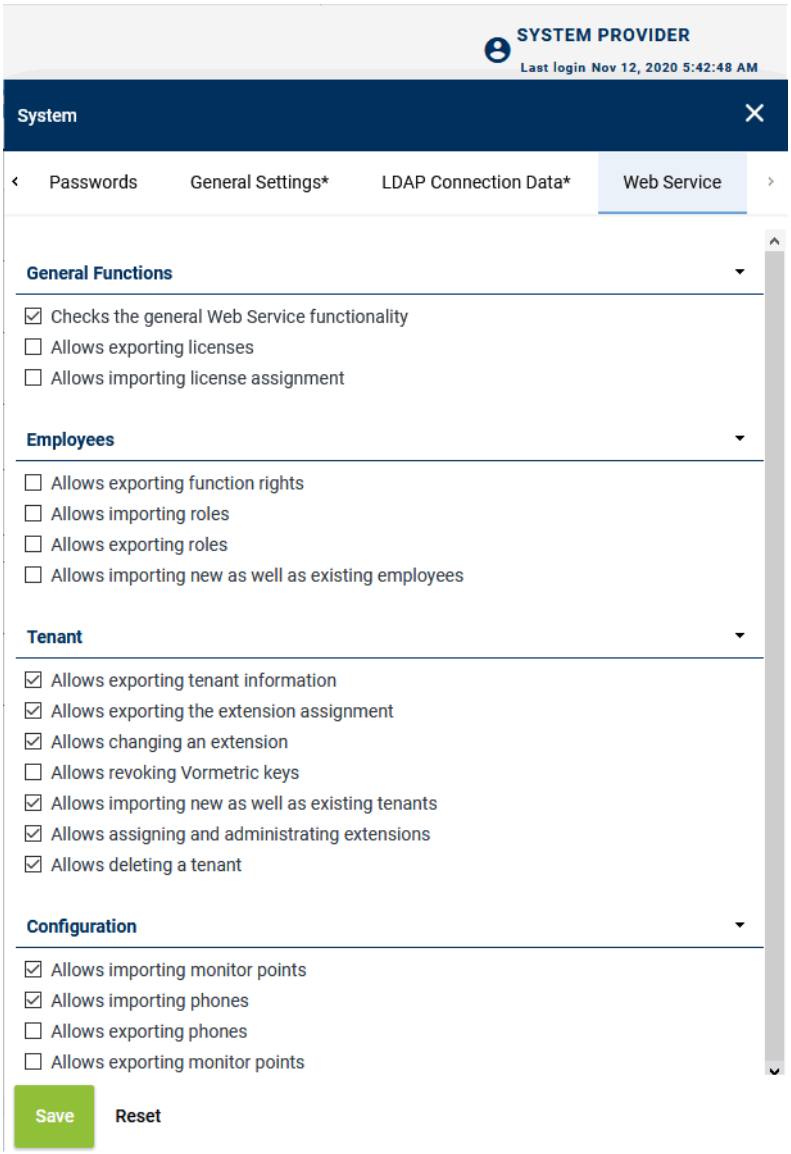

Fig. 51: Web service functionalities for the reseller

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 general function.

Checks the general web service functionality	Activate the check box, if you would like to allow checking the general web service functionality.
Allows exporting licenses	Activate the check box if you would like to allow exporting licenses.
Allows importing license assignment	Activate the check box if you would like to allow importing the license assignment.

Group field Employees

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

Allows exporting function rights	Activate the check box if you would like to allow the tenant to export function rights via the Web Service.

Allows importing roles	Activate the check box if you would like to allow the tenant to import roles via the Web Service.
Allows exporting roles	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.

Allows exporting tenant information	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.
Allows exporting the extension assignment	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
Allows assigning and administrating extensions	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
Allows deleting a tenant	Activate the check box if you would like to be able to delete the tenant via the Web Service.
Allows changing an extension	Activate the check box if you would like to be able to change the extension via the Web Service.
Allows revoking Vormetric keys	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
Allows importing new as well as existing tenants	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.

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

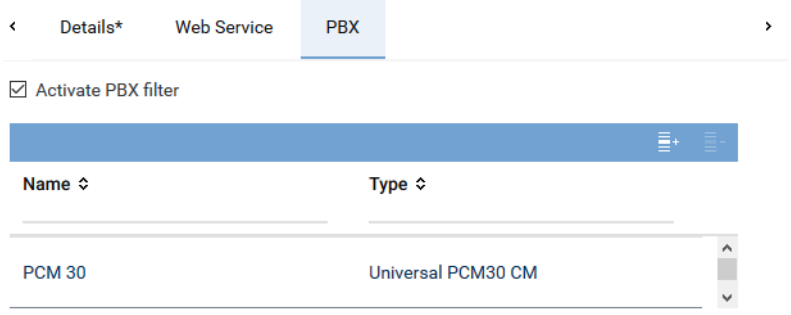

Fig. 52: Tenants module - tab PBX

Activate PBX filter	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. 55.
- To remove the assignment of a PBX to a reseller, proceed as described in chapter "Remove PBX assignment", p. 55.

4.2.12.1 Assign PBX

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

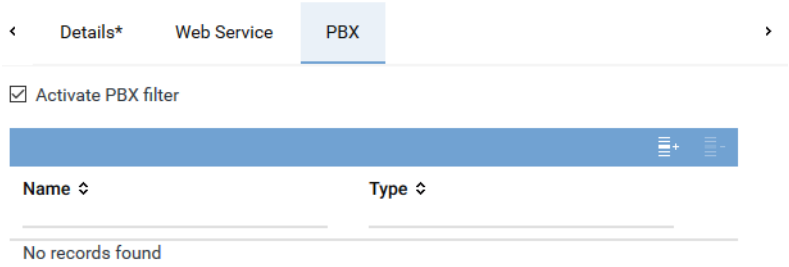

Fig. 53: Assign PBX

2. 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.

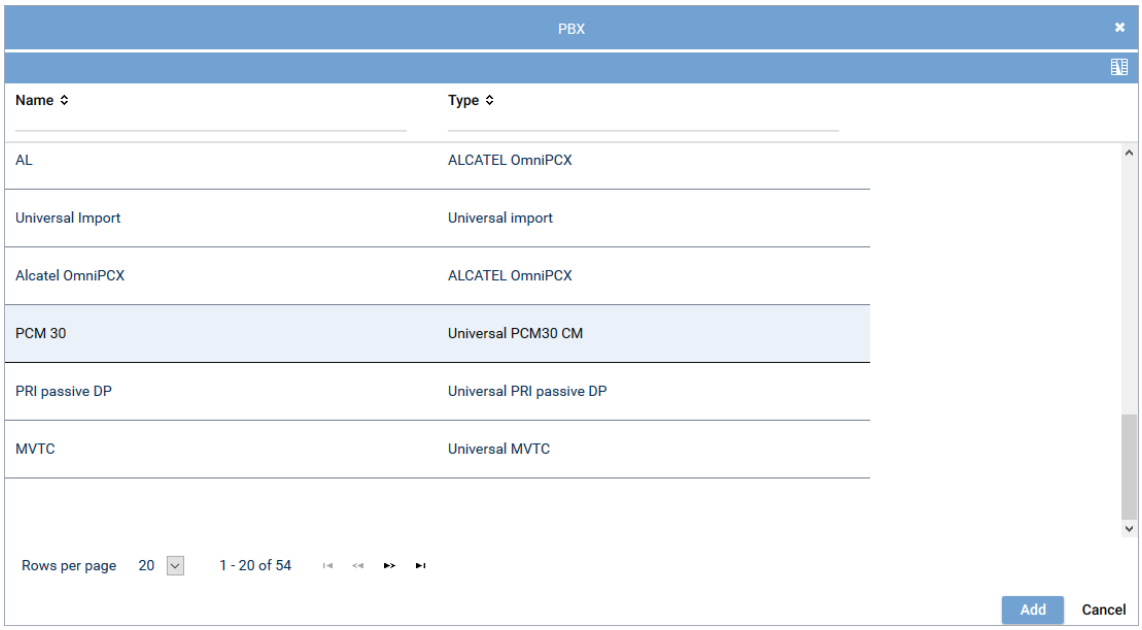

Fig. 54: Add PBX

3. 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

1. 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.

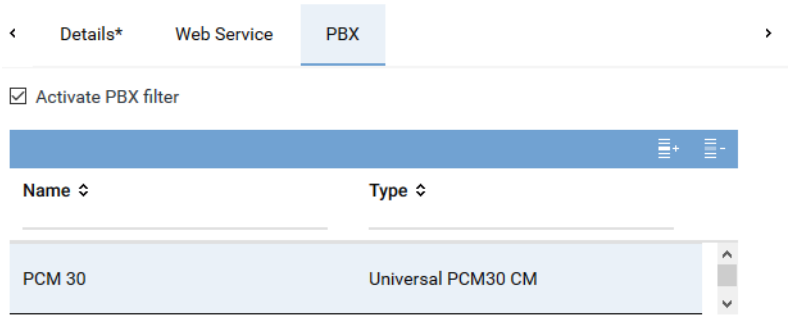

Fig. 55: Remove PBX assignment

2. Click on the icon *(Remove)*.

4.2.13 Tab Tenant Features

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.

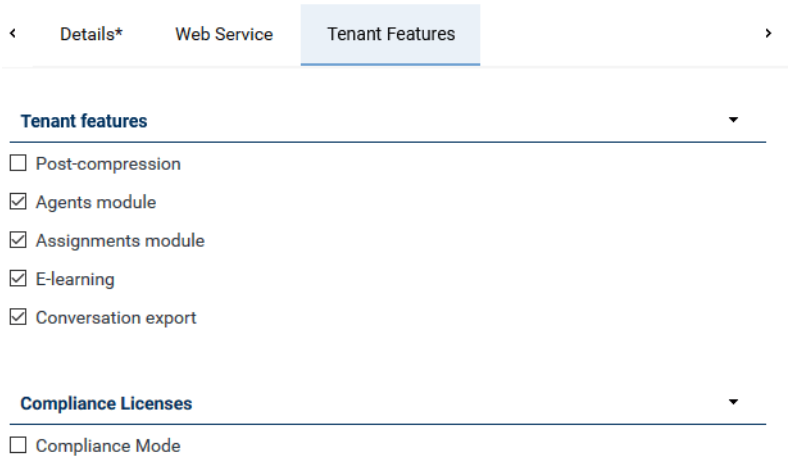

Fig. 56: Tab Tenant Features

Group field Tenant Features

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 a 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 *System Configuration - Configuration drives*. Post-compression applies for all drives for which post-compression has been activated.
Agents module	Select whether the Agents module is supposed to be activated. ☑ = Agents module has been activated. ☐ = Agents module has not been activated.
Assignments module	Select whether the Assignments module is supposed to be activated. ☑ = Assignments module has been activated. ☐ = Assignments module has not been activated.
E-learning	Select whether the E-Learning module is supposed to be activated. ☑ = E-Learning module has been activated. ☐ = E-Learning module has not been activated.
Conversation export	Select whether the export of conversations is supposed to be activated. ☑ = Export of conversations has been activated. ☐ = 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.

Compliance mode	Select whether the compliance mode for INSPIRATION*neo* is supposed to be activated. ☑ = Compliance mode has been activated. ☐ = 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.

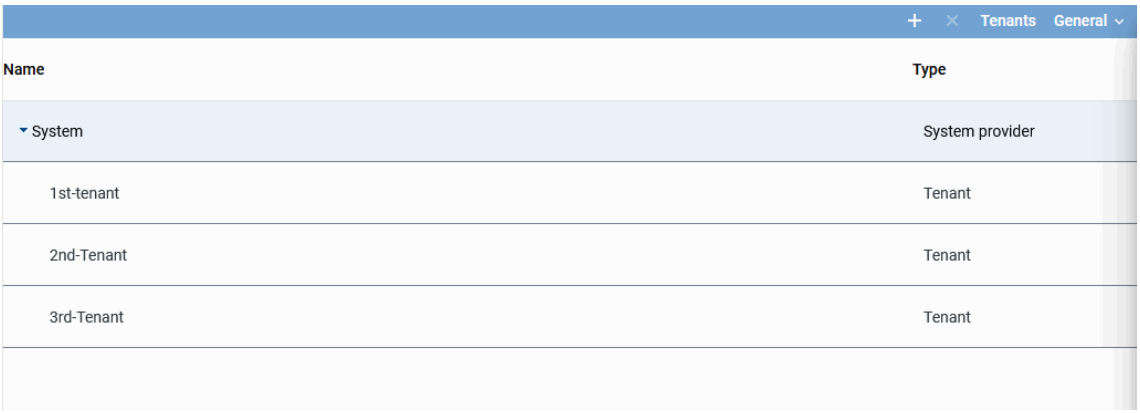

Fig. 57: Tenants module - main view (example)

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

Create Tenant	A new tenant is created.
Create Reseller	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*.

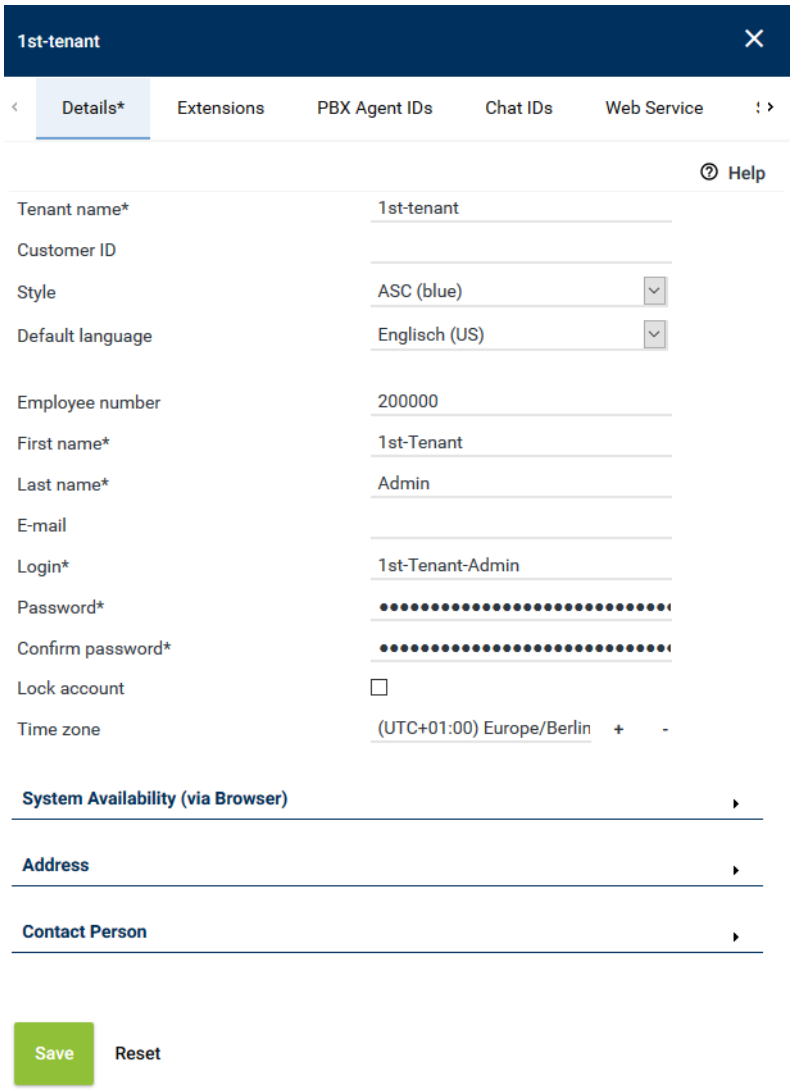

Fig. 58: Save tenant

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*.

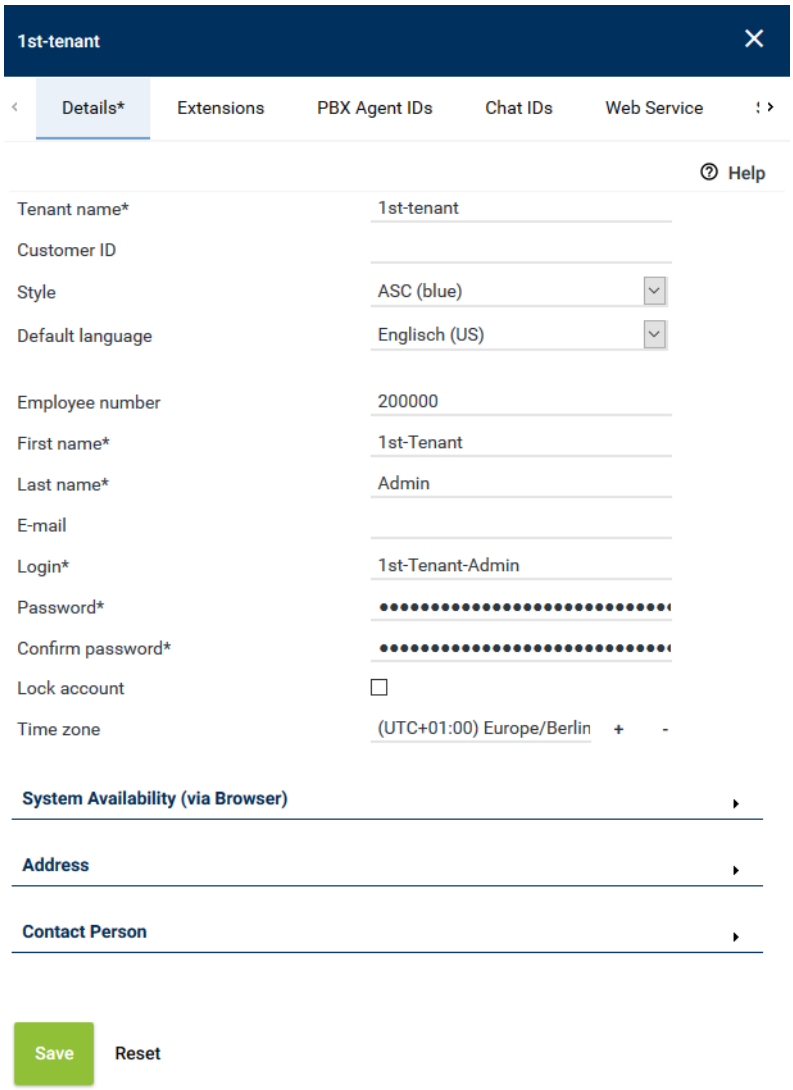

Fig. 59: Save changes

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.

4.6 Activate OAuth login for system

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

1. In the navigation bar, open the Tenants module and select the user *System* in the main view.
   ⇨ The detail view opens.
2. In the tab *General Settings*, open the group field *Login Settings*.

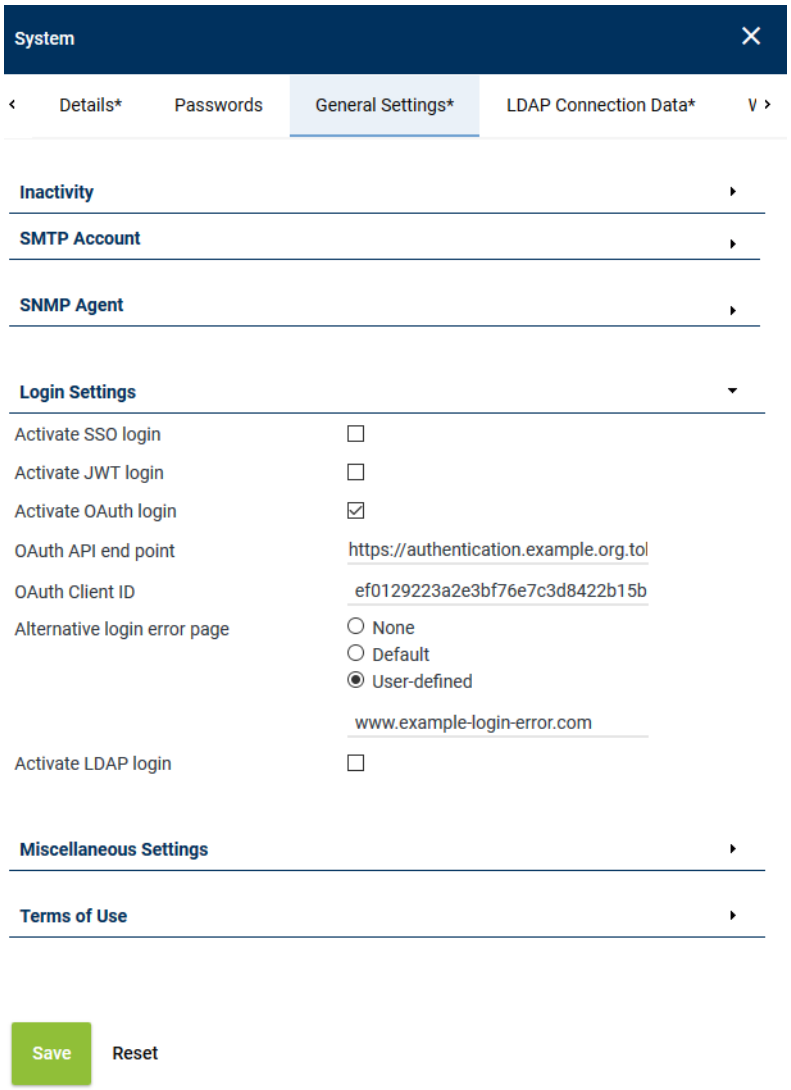

Fig. 60: Activate OAuth login - example

3. Activate the check box *Activate OAuth login* and enter your individual OAuth settings.
4. Click on the button *Save* to save the entries.
   Click on the button *Cancel* to discard the entries.

Once the entries have been saved, employees with OAuth login can be configured.

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

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.

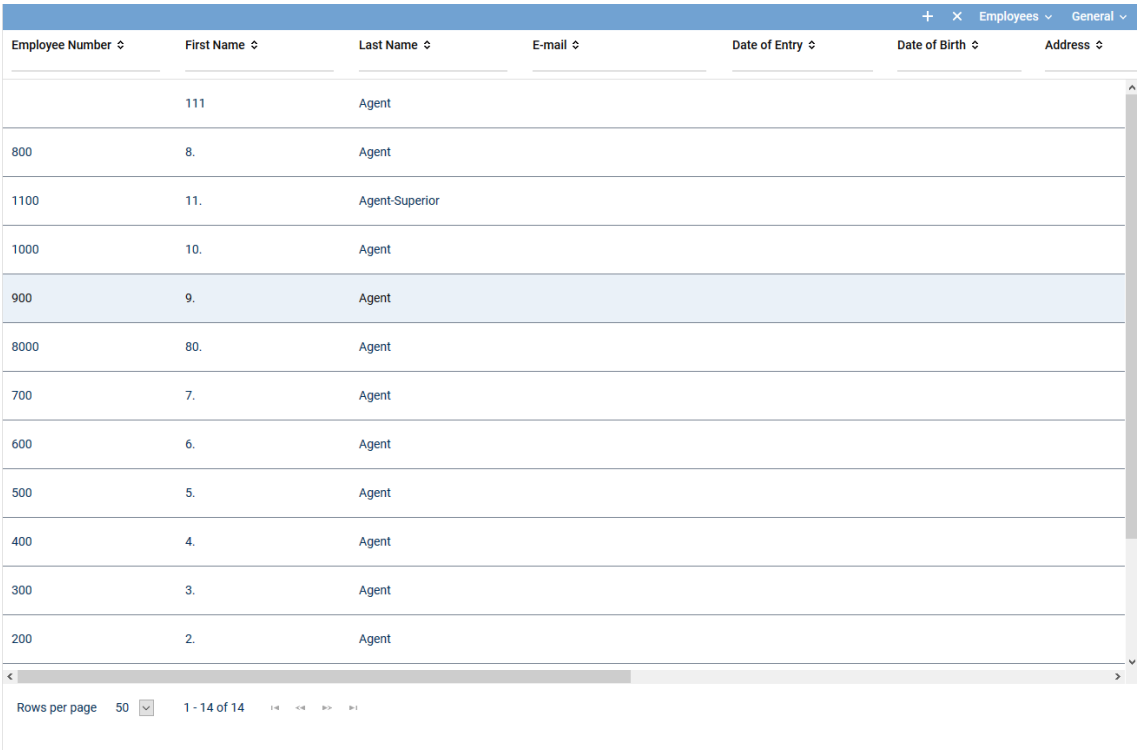

Fig. 61: Employees module - main view

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

Employee Number	ID of the employee.

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

5.1.1 Toolbar

The toolbar offers the following functions.

Fig. 62: Employees module - toolbar

	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 65. The icon *(Search)* is displayed whenever the search has been adjusted by means of a filter.
	Reset search	Resets all manually entered search criteria. The search is started without manual filter settings.
	Create	Creates a new employee (see chapter "Create new employee", p. 78).
	Delete	Deletes the selected employee (see chapter "Delete employee", p. 79).
Employees	*Summary*	Lists all function rights of the selected employee (see chapter "Show summary", p. 64).
	Show Locked Employees/Show All Employees	Lists only the locked employees in the main view (see chapter "Show locked employees", p. 64).
	Make Employee Visible or Not Visible	Function which makes the selected employee visible or not visible for others (see chapter "Make employee visible or not visible", p. 65).
	Export User Data	Exports the user data of the employee of the current tenant in XML format.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • Displayed information

	• Order of the displayed columns • Number of rows per page
General Help	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.
Module Help	By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.

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

5.1.1.1 Show summary

This function allows displaying the function rights of the employee.

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

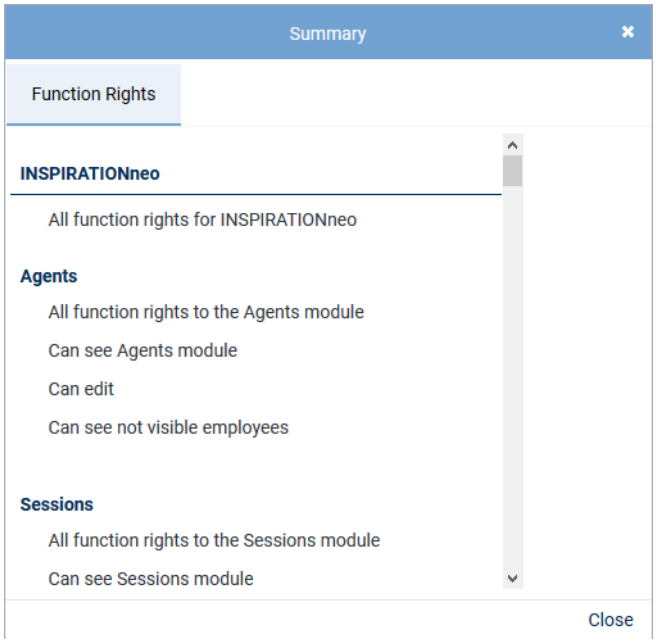

Fig. 63: Summary of the function rights

	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. 71.

5.1.1.3 Make employee visible or not visible

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

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

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

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

5.1.1.4 Search

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

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

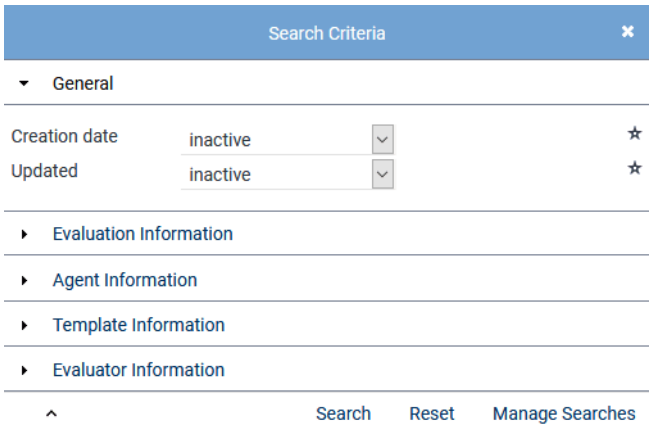

Fig. 64: Window Search Criteria (example)

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

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

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

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

5.2 Detail view

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

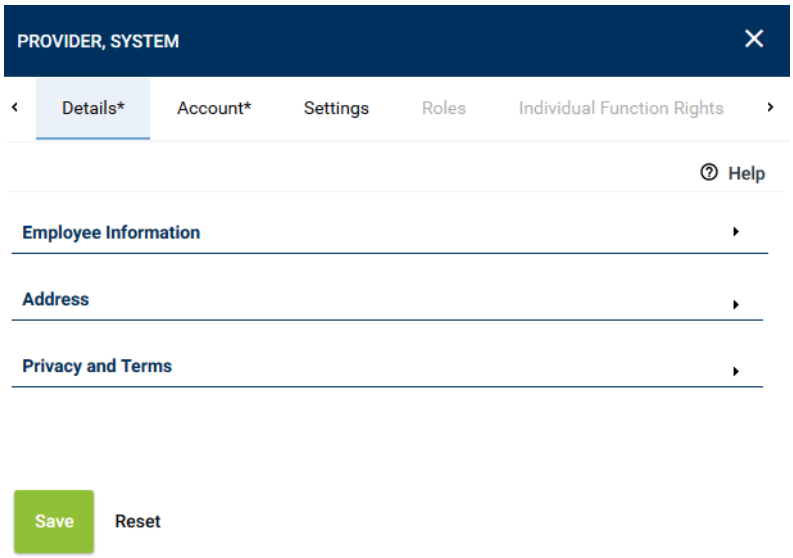

Fig. 65: Employees module - detail view

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. 66.
- *Account*

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

  See chapter "Tab Account", p. 71.
- *Settings*

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

  See chapter "Tab Settings", p. 73.
- *Roles*

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

  See chapter "Tab Roles", p. 75.
- *Individual Function Rights*

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

  See chapter "Tab Individual Function Rights", p. 77.

5.2.1 Tab Details

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

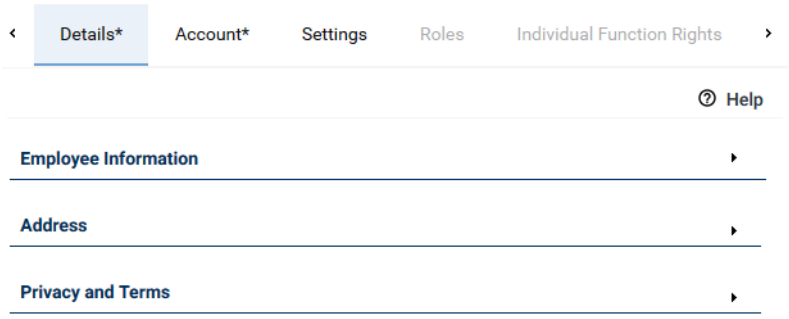

Fig. 66: Employees module - tab Details

Entering an address is optional.

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

5.2.1.1 Group field Employee Information

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

Fig. 67: Edit employee information

	Placeholder for the employee's photo. See chapter "Upload or delete image", p. 69.
Employee number	ID of the employee.
First name	First name of the employee.
Last name	Last name of the employee.
Date of birth	Date of birth of the employee. You can enter the date directly via the keyboard or via the icon.
E-mail	E-mail address of the employee.
Date of entry	Day on which the employee was hired. You can enter the date directly via the keyboard or via the icon.
Comment	Comment on the employee information.

Address for replay via phone	Enter the address of the phone which is supposed to replay the calls. Depending on which agent logs in on this phone, the audio data that the participant is allowed to replay is provided. You can use the following additional data as address: • Extension if it has been configured in the PBX for replay via phone. • Complete phone number, e. g. *06021 5001 1015* if the PBX is connected to the public telephone network. • IP address if it has been configured. • MAC address if it has been configured. • SIP address, e. g. *Extension@IP-Address*.
Import key	Key to unambiguously identify an employee imported from an external source. When importing the employee information for the first time, the import key is entered here automatically. Upon each new import, this import key is checked to determine whether the employee has already been imported before. In addition, the import key is used when transferring (export/import) recordings from a *neo* system to another *neo* system to map the recordings to the agents. If the employee does not have an automatically created import key, you can enter an import key manually for this mapping. **NOTICE!** If you change an import key manually, the employee will not be recognized as an already imported employee upon the next import of employee data. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordigs.
Extended import key	Extended key to unambiguously identify employees imported from an external source. The extended import key is used whenever the standard import key is not sufficient for an unambiguous identification. An example where the extended import key is used is during the import of calls from the application Recording Insights. Here, the import key alone is not sufficient as the users come from different LDAP systems and several attributes are compiled in an extended import key for unambiguous identification. When the employee's data is imported for the first time, the import key is entered here automatically. With every new import, this import key is checked to determine whether the employee has already been imported. In addition, the import key is used during the export/import of recordings from one *neo* system to another *neo* system to map the recordings to the agents. If the employee does not have an automatically generated import key, you can enter an import key manually for this purpose. **NOTICE!** If you change an import key manually, the employee will not be recognized as having been imported before already. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordings.
Time zone	Shows the time zone in which the conversations are supposed to be displayed in the replay applications. The settings which have been configured for the respective employee prevail over the default settings in the Tenants module

To select the time zone, click on the button + . See chapter "Add time zone", p. 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.

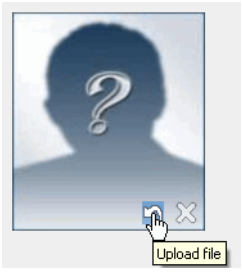

Fig. 68: Upload image

⇨ The window *Upload File* appears.

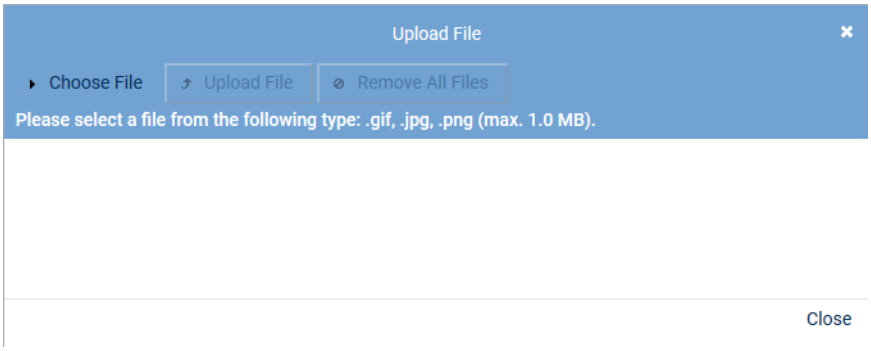

Fig. 69: Upload File

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.

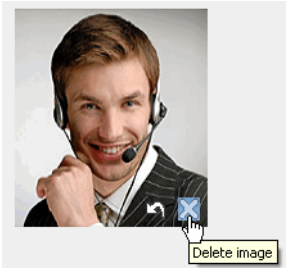

Fig. 70: Delete image (example)

⇨ The image is deleted from the detail view.

5.2.1.2 Group field Address

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

Fig. 71: Add address

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

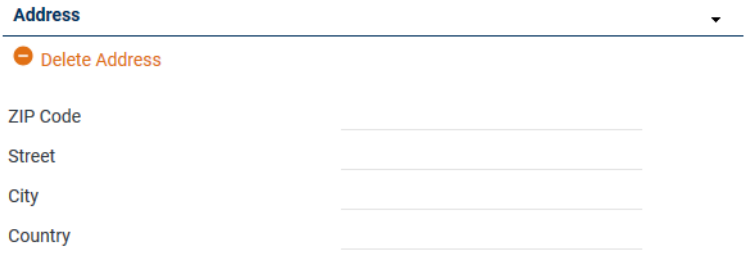

Fig. 72: Add address

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

5.2.1.3 Group field Privacy and Terms

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

Fig. 73: Add privacy statement and terms

2. In the title bar of the group field, click on the button *Add Link*.
3. Enter the respective links.

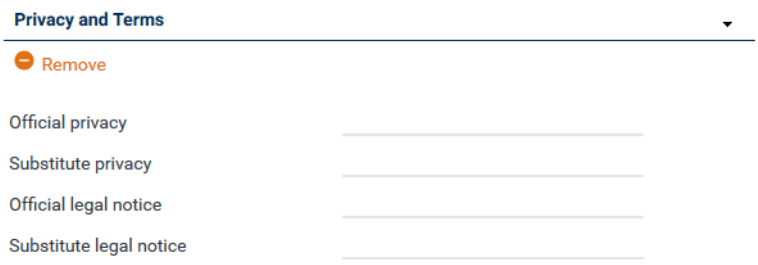

Fig. 74: Add privacy statement and terms

Official privacy	Enter the link to the official privacy statement.
Substitute privacy	Enter the link to the substitute privacy statement.
Official legal notice	Enter the link to the official legal notice.
Substitute legal notice	Enter the link to the substitute legal notice.

4. 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.

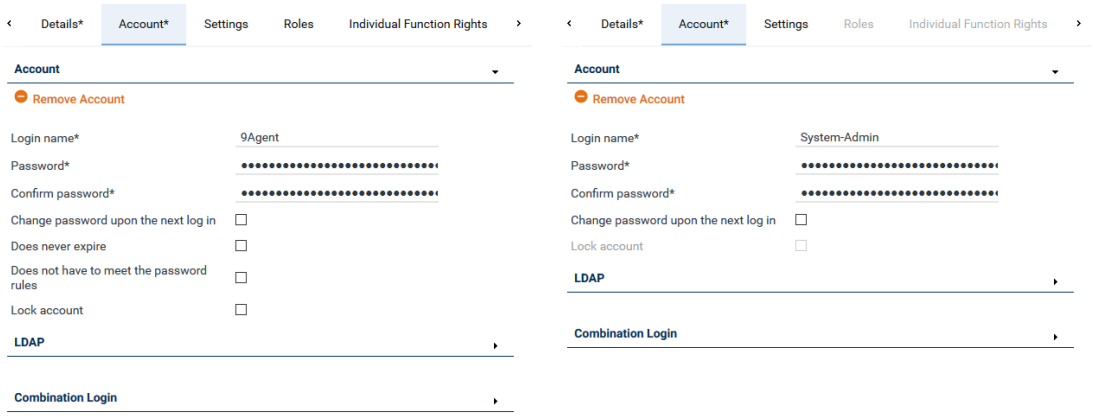

Fig. 75: Employees module - tab Account

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. 76: Add account

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

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

Does never expire	Activate this option if the password is never supposed to expire. **NOTICE!** This option is not available for superusers.
Does not have to meet the password rules	Activate this option if the password does not necessarily have to be consistent with the password rules. **NOTICE!** Password rules can be defined in the Tenants module in the tab *Passwords*. **NOTICE!** This option is not available for superusers.
Lock account	This option allows locking the employee's account. In the main view, you can filter for this criterion, see chapter "Show locked employees", p. 64. **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. 72.
6. To assign the employee a combination user, see chapter "Assign combination user", p. 72.

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*.

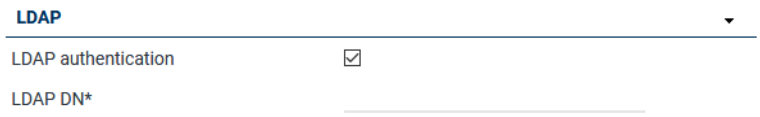

Fig. 77: Activate authentication via LDAP

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)*.

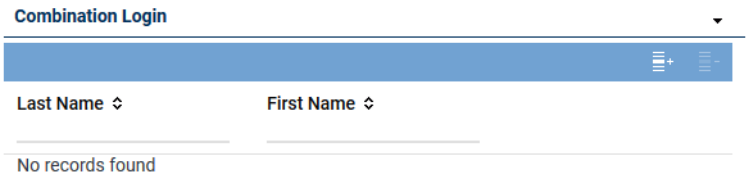

Fig. 78: Assign combination user

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

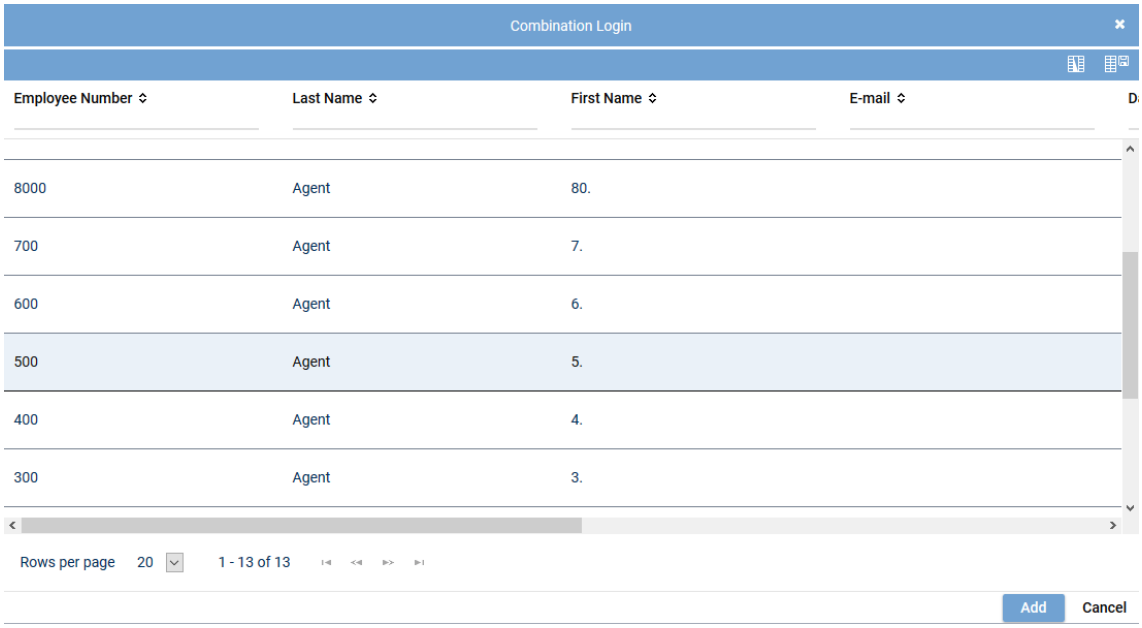

Fig. 79: Add combination user

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

5.2.2.3 Delete combination user assignment

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

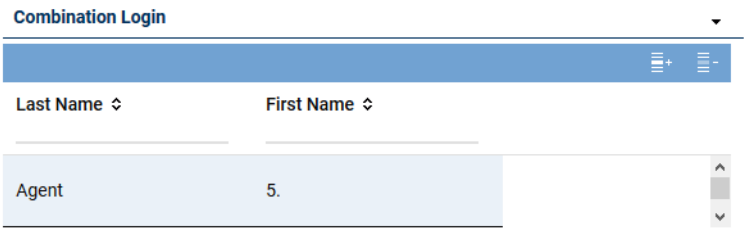

Fig. 80: Delete combination user assignment

5.2.3 Tab Settings

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

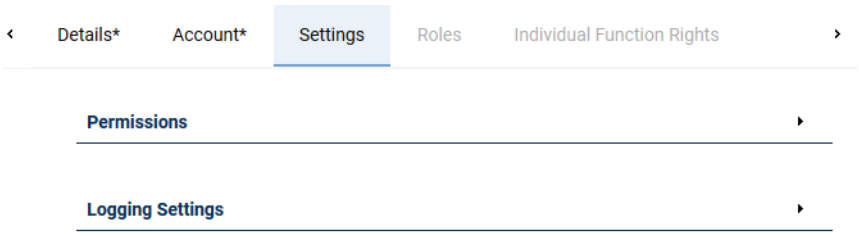

Fig. 81: Employees module - tab Settings

5.2.3.1 Group field Permissions

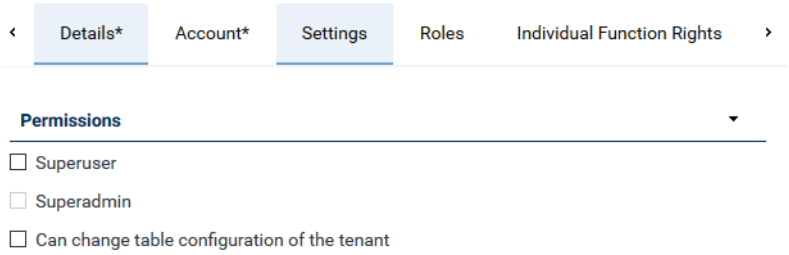

Fig. 82: Configure permissions

Superuser	This right assigns all function rights in the system to the user if their licenses are available. ☑ = Right has been activated. ☐ = Right has been deactivated.
Superadmin	This right assigns the user 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 in the following applications: • System Configuration • System Monitoring • Portal Information about the login for superadmins can be found in the respective user manuals *System Configuration - General information*, *System Monitoring*, and *Portal*. A superadmin does not have access to recordings. A superadmin cannot be assigned to an organization unit. ☑ = Right has been activated. ☐ = Right has been deactivated. **NOTICE!** Superadmin rights are only available in a Cloud environment and have to be activated when needed. The option *Superadmin* is only displayed if there is the respective license in the system. In a 1-tenant system, the option *Superadmin* is activated automatically. No extra license is required For the default superuser created by the system, the option *Superadmin* is not available.

Can change table configuration of the tenant	This right allows the user to change the default table configuration for the employees of the tenant. This applies to the main view of the respective modules as well as to dialog windows.

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

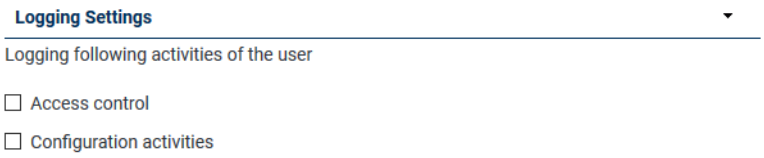

Fig. 83: Configure logging

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.

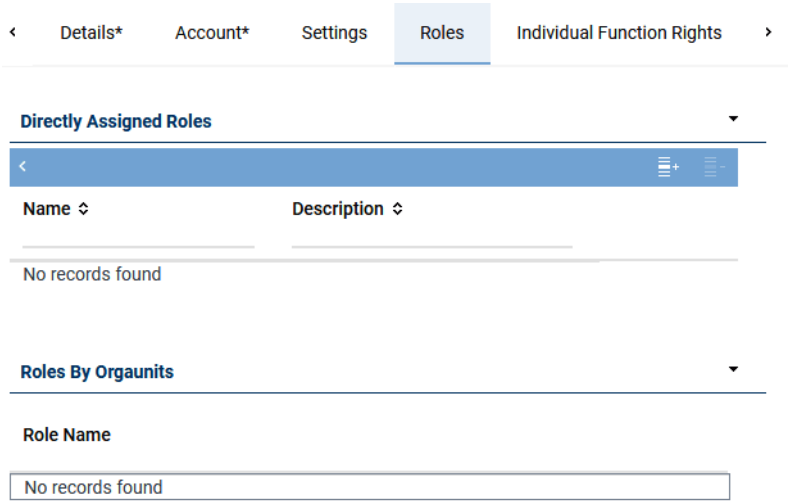

Fig. 84: Employees module - tab Roles

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)*.

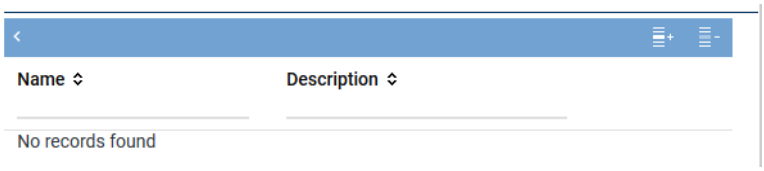

Fig. 85: Assign roles

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

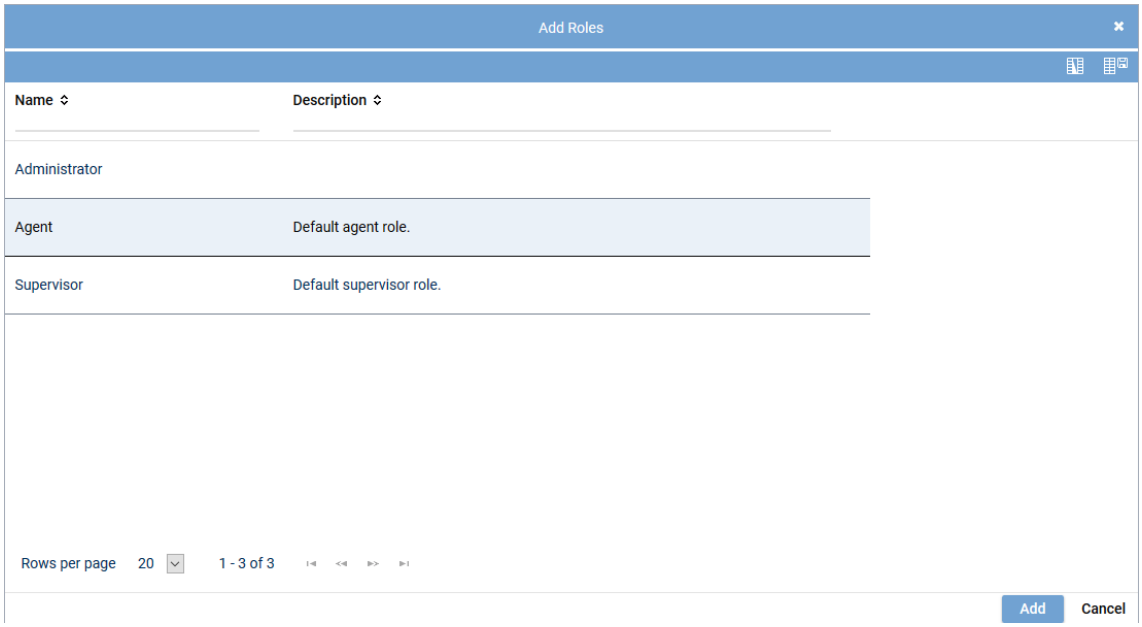

Fig. 86: Add role

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)*.

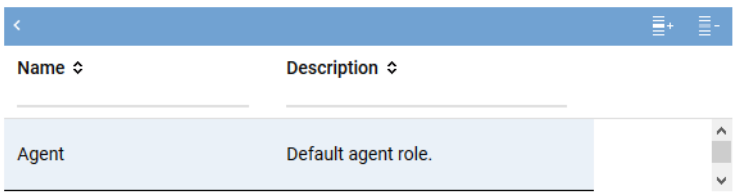

Fig. 87: Delete role assignment

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.

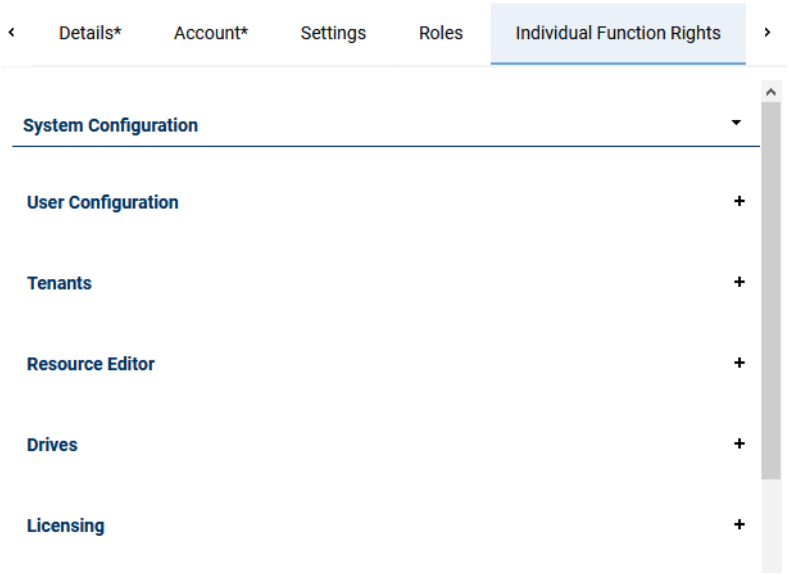

Fig. 88: Employees module - tab Individual Function Rights (example)

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.

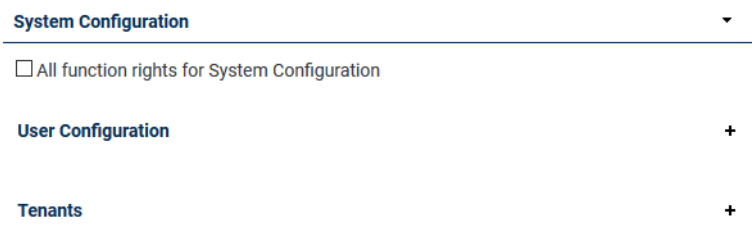

Fig. 89: Function rights - display sections (example)

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.

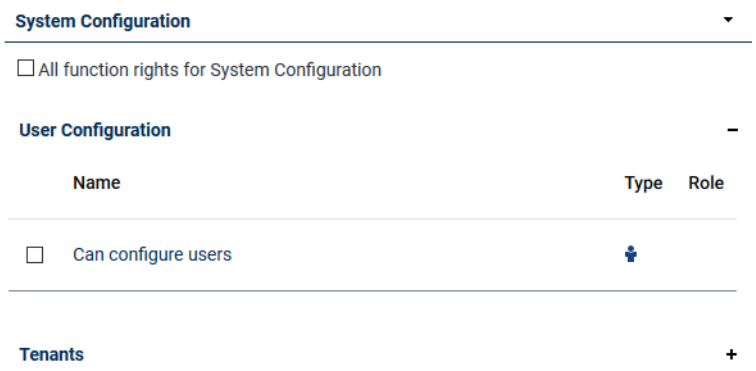

Fig. 90: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. ☑ = individual function right ☐ = no individual function right
Name	Description of the function right.
Type	Shows which license is required for this right. = agent license = supervisor license = basic license (without agent or supervisors rights)
Role	Shows whether the function right has been assigned to the user via a role (role right). no mark = no role right ✓ = role right **NOTICE!** In the window *Summary*, you can see via which role the function right has been assigned, see chapter "Show summary", p. 64.

Tab. 3: Function rights

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

5.3 Create new employee

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

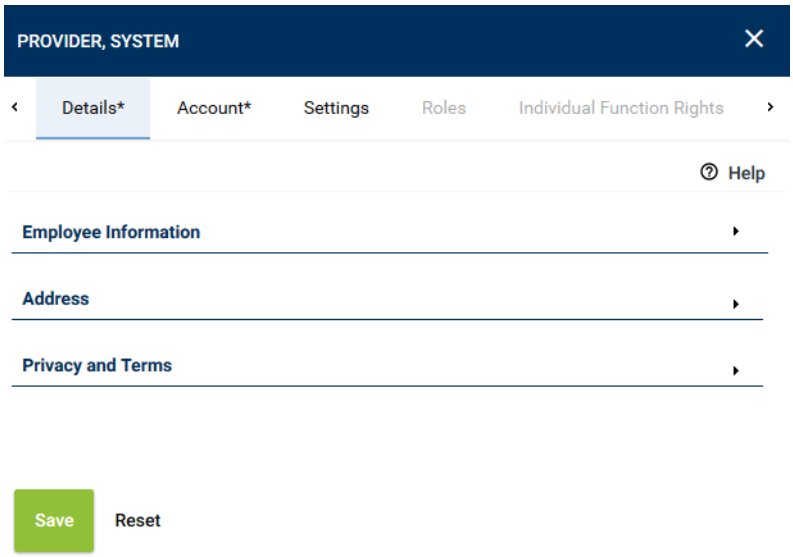

Fig. 91: Save employee

5.4 Edit employee

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

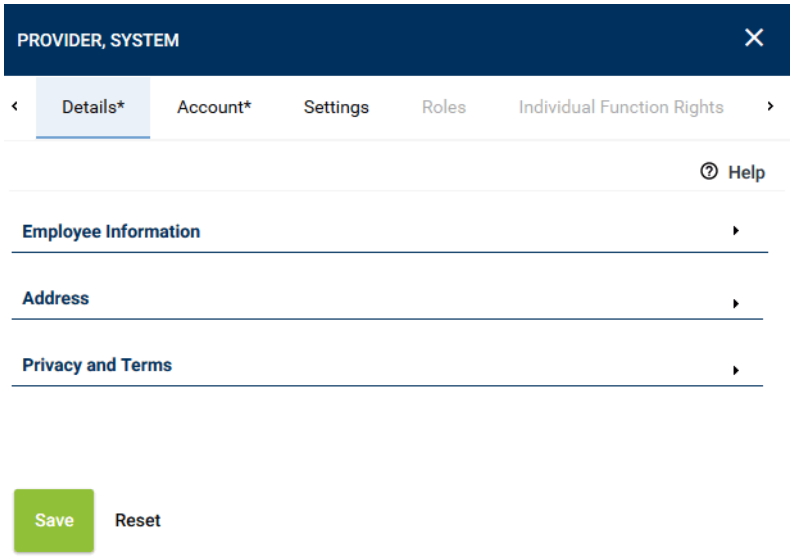

Fig. 92: Save changes

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.

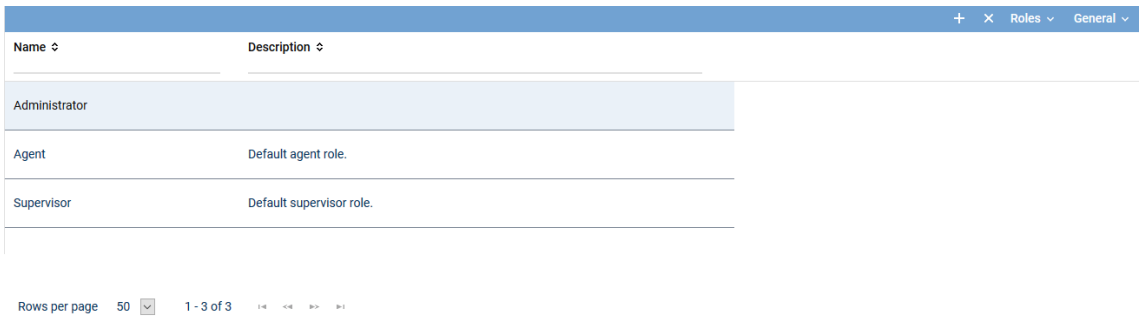

Fig. 93: Roles module - main view

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

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

6.1.1 Toolbar

The toolbar offers the following functions.

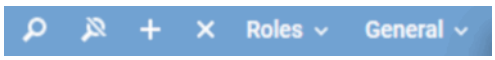

Fig. 94: Roles module - toolbar

	Search	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see chapter "Search", p. 65. The icon *(Search)* is displayed whenever the search has been adjusted by means of a filter.
	Reset Search	Resets all manually entered search criteria. The search is started without manual filter settings.
	Create	Creates a new role (see chapter "Create new role", p. 86).
	Delete	Deletes the selected role (see chapter "Delete role", p. 87).
Roles	*Duplicate with Employees*	Creates a copy of the selected role with the assigned employee, see chapter "Duplicate role", p. 86.
	Duplicate Without Employees	Creates a copy of the selected role without the assigned employee, see chapter "Duplicate role", p. 86.
General	*Print*	Prints the table of the main view.
	Adjust Table	Opens a window in which you can adjust the following settings for the main view: • Displayed information • Order of the displayed columns • Number of rows per page
	General Help	By clicking on the menu item *General Help*, a description of the application you are currently viewing is opened.
	Module Help	By clicking on the menu item *Module Help*, a description of the module you are currently viewing is opened.

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

6.2 Detail view

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

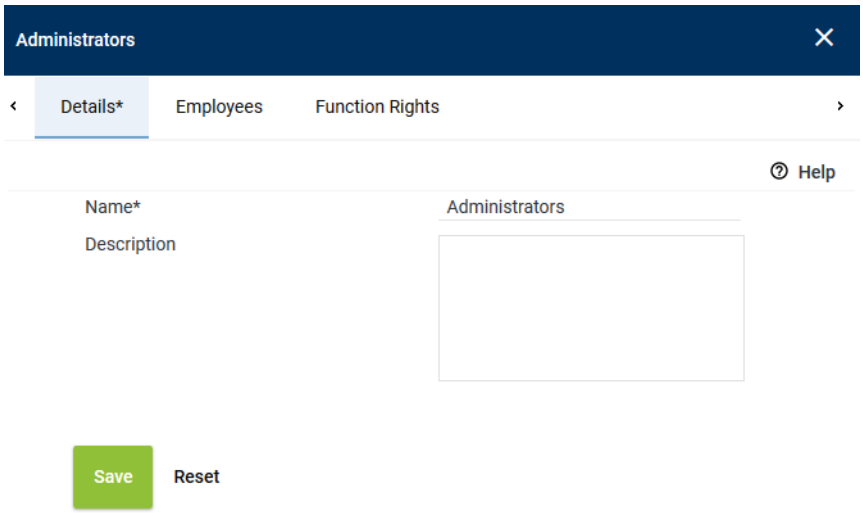

Fig. 95: Roles module - detail view

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. 83.

- *Employees*

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

  See chapter "Tab Employees", p. 83.

- *Function Rights*

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

  See chapter "Tab Function Rights", p. 84

6.2.1 Tab Details

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

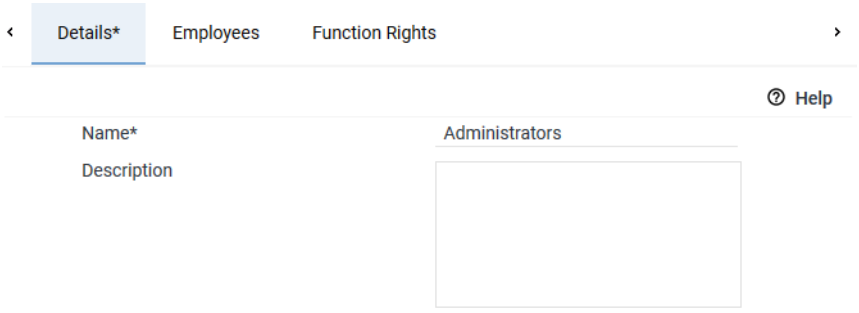

Fig. 96: Roles module - tab Details

Name	Name of the role.
Description	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.

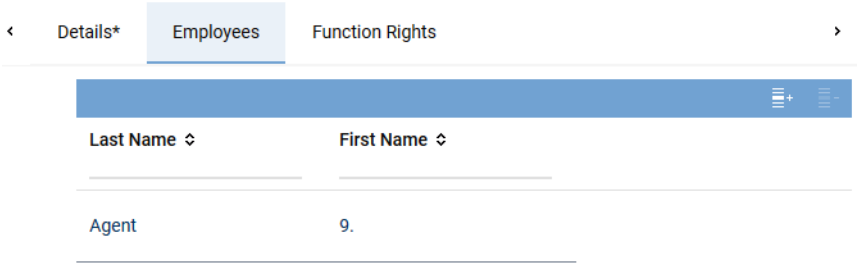

Fig. 97: Roles module - tab Employees

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)*.

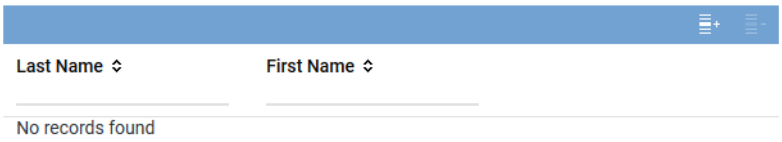

Fig. 98: Assign users

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

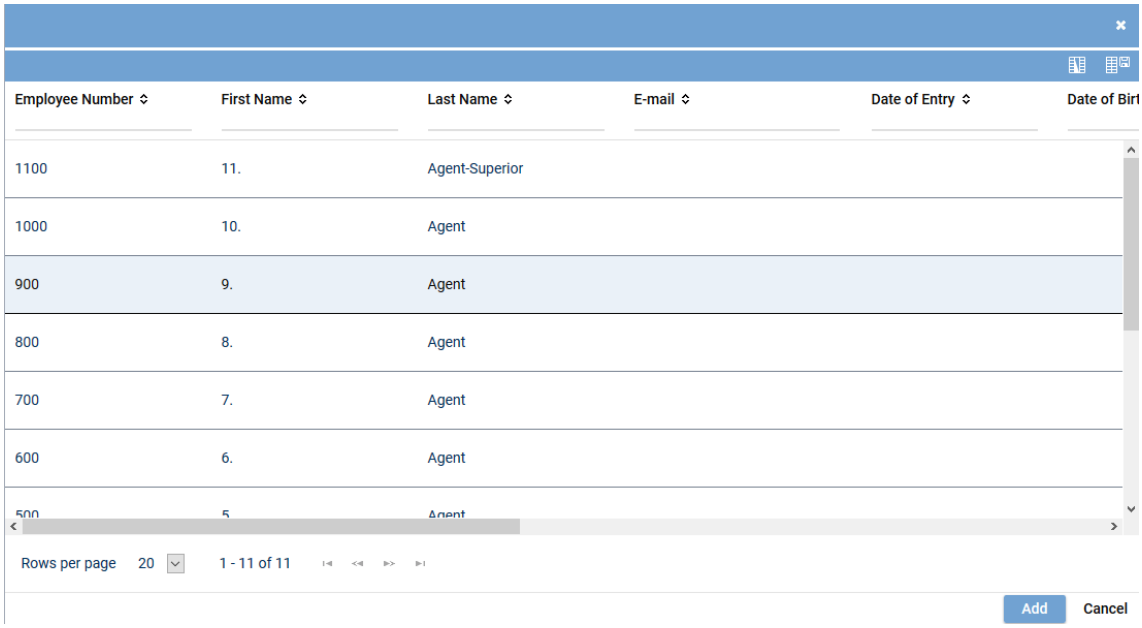

Fig. 99: Add user

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)*.

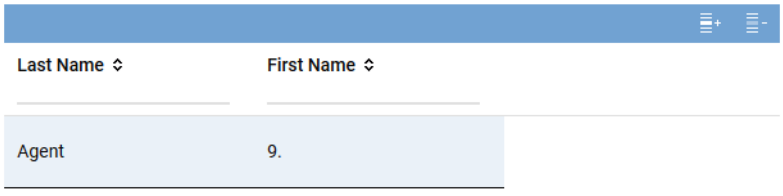

Fig. 100: Delete user assignment

6.2.3 Tab Function Rights

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

Fig. 101: Roles module - tab Function Rights (example)

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

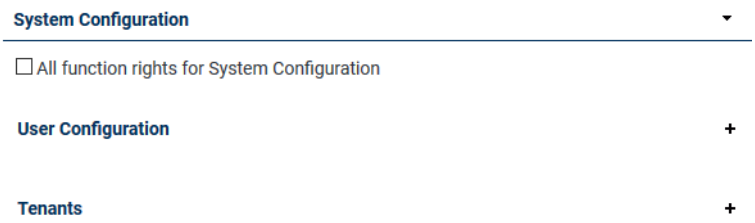

Fig. 102: Function rights - display sections (example)

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.

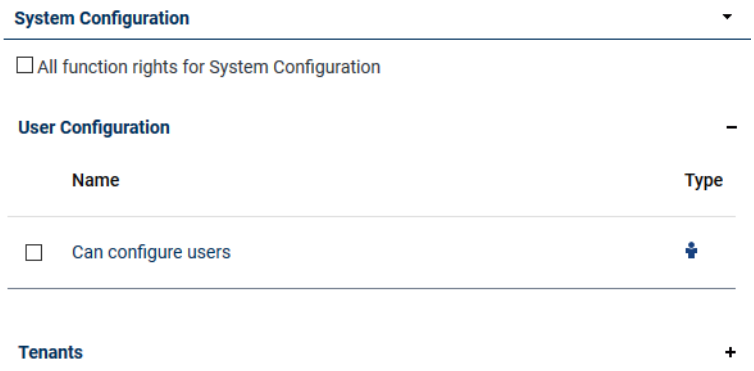

Fig. 103: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. ☑ = individual function right ☐ = no individual function right
Name	Description of the function right.
Type	Shows which license is required for this right.

= agent license

= supervisor license

= basic license (without agent or supervisors rights)

Tab. 4: Function rights

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

6.3 Create new role

1. Click on the icon + *(Create)* in the toolbar.
2. Adjust all settings in the tabs of the detail view as described in the respective chapters (see chapter "Detail view", p. 82).
   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*.

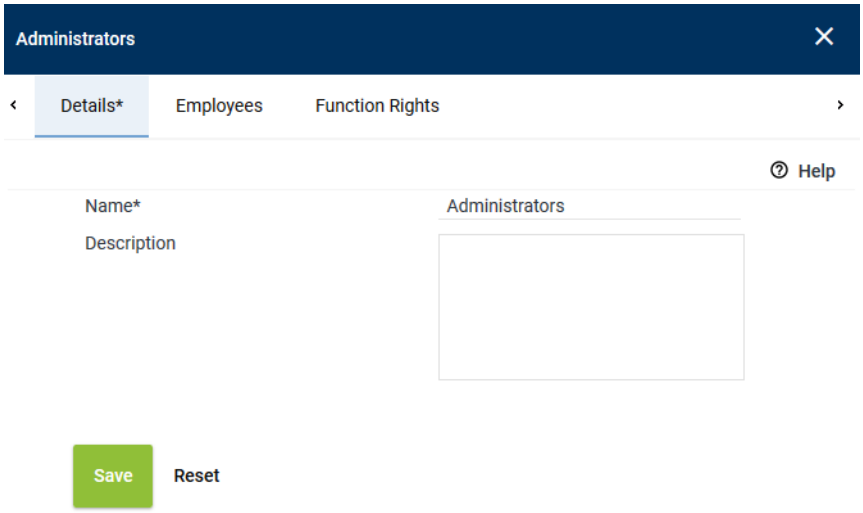

Fig. 104: Save role

6.4 Duplicate role

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

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

4. A copy of the role is created in the detail view.
5. Enter a new name for the copied role.

6. Adjust all settings in the tabs of the detail view as described in the respective chapters (see chapter "Detail view", p. 82).
   You can change tabs without buffering without risking the loss of your settings.
7. Once you have finished adjusting the settings, click on the button *Save* to save the settings.
   To discard the entries, click on the button *Reset*.

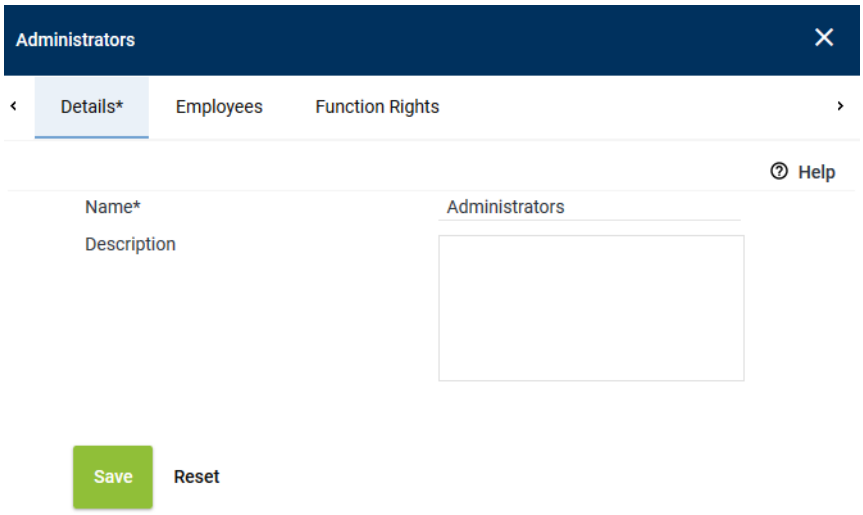

Fig. 105: Save role

6.5 Edit role

1. In the main view, select the role you would like to edit.
2. Make all necessary changes in the tabs of the detail view, see chapter "Detail view", p. 82.
   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*.

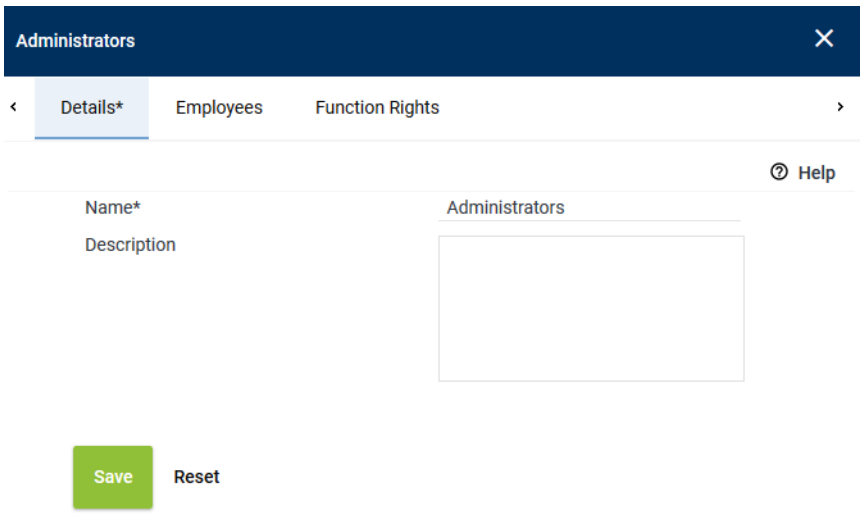

Fig. 106: Save changes

6.6 Delete role

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

The system does not issue a prompt if the role you are deleting has been assigned to a user.

By deleting this role the user loses all function rights he has been assigned via this role.

If this user is currently logged in to the system, the deletion of the role will come into effect after he has logged off from the system.

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*.

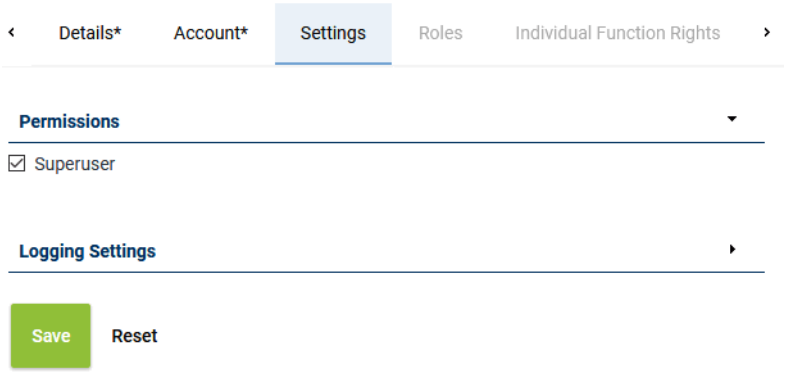

Fig. 107: Create superuser

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.

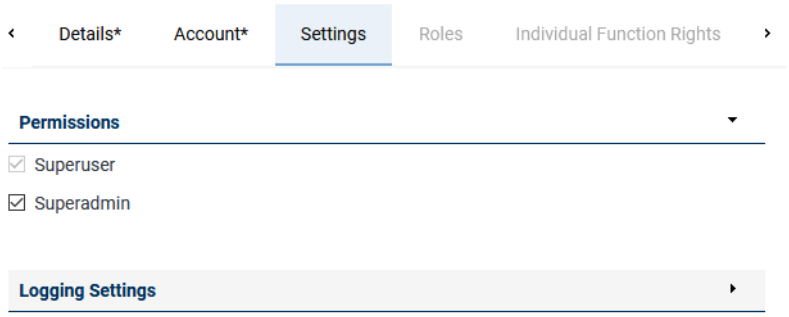

Fig. 108: Create superadmin

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

List of figures

List of figures

List of tables

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

URL

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

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.