

# System Configuration

## User management



## Administration manual

### for system providers

8/8/2022

### Product line Neo, version 7.x

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

EVOIP<sup>neo</sup>

EVOLUTION<sup>neo</sup> / XXL / eco

INSPIRATION<sup>neo</sup>

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

Copyright © 2022 ASC Technologies AG. All rights reserved.

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



## Contents

<b>1</b>	<b>General information.....</b>	<b>6</b>
<b>2</b>	<b>Introduction.....</b>	<b>7</b>
<b>3</b>	<b>LDAP.....</b>	<b>10</b>
3.1	Install certificate .....	10
3.2	Troubleshooting .....	11
<b>4</b>	<b>Tenants module .....</b>	<b>12</b>
4.1	Main view .....	12
4.1.1	Toolbar.....	12
4.2	Detail view .....	13
4.2.1	Detail view for the tenant account of the system provider .....	13
4.2.2	Detail view for normal tenants .....	14
4.2.3	Detail view for resellers.....	16
4.2.4	Tab Details.....	16
4.2.4.1	Add time zone .....	18
4.2.4.2	Group field System Availability .....	19
4.2.4.3	Group field Address .....	21
4.2.4.4	Group field Contact Person .....	21
4.2.5	Tab Extensions .....	22
4.2.5.1	Add extensions .....	22
4.2.5.2	Remove extensions .....	24
4.2.6	Tab PBX Agent IDs.....	25
4.2.6.1	Add PBX Agent ID .....	26
4.2.6.2	Remove PBX Agent ID .....	27
4.2.7	Tab Chat IDs.....	28
4.2.7.1	Add chat ID .....	29
4.2.7.2	Remove chat ID .....	30
4.2.8	Tab Passwords .....	31
4.2.8.1	Edit entry.....	36
4.2.9	Tab General Settings.....	36
4.2.9.1	Group field Inactivity .....	37
4.2.9.2	Group field SMTP Account .....	37
4.2.9.3	Group field SNMP Agent .....	39
4.2.9.4	Group field Login Settings .....	41
4.2.9.5	Group field Miscellaneous Settings .....	54
4.2.9.6	Group field Terms of Use.....	55
4.2.10	Tab LDAP Connection Data .....	55
4.2.10.1	Edit LDAP connection data.....	56
4.2.11	Tab Web Service .....	56
4.2.11.1	Configure web service for the system provider.....	57
4.2.11.2	Configure Web Service for the tenant.....	59

4.2.11.3	Path of the WSDL file .....	62
4.2.11.4	Configure Web Service for the reseller .....	62
4.2.12	Tab PBX .....	64
4.2.12.1	Assign PBX .....	65
4.2.12.2	Remove PBX assignment .....	65
4.2.13	Tab Tenant Features .....	66
4.3	Create new tenants manually .....	67
4.4	Edit tenants manually .....	69
4.5	Delete tenant .....	70
<b>5</b>	<b>Employees module .....</b>	<b>71</b>
5.1	Main view .....	71
5.1.1	Toolbar .....	72
5.1.1.1	Show summary .....	73
5.1.1.2	Show locked employees .....	73
5.1.1.3	Make employee visible or not visible .....	74
5.1.1.4	Search .....	74
5.2	Detail view .....	75
5.2.1	Tab Details .....	75
5.2.1.1	Group field Employee Information .....	76
5.2.1.2	Group field Address .....	79
5.2.1.3	Group field Privacy and Terms .....	79
5.2.2	Tab Account .....	80
5.2.2.1	Authentication via LDAP .....	81
5.2.2.2	Assign combination user .....	81
5.2.2.3	Delete combination user assignment .....	82
5.2.2.4	Two-factor authentication .....	82
5.2.3	Tab Settings .....	83
5.2.3.1	Group field Permissions .....	83
5.2.3.2	Group field Logging Settings .....	84
5.2.4	Tab Roles .....	85
5.2.4.1	Assign roles .....	85
5.2.4.2	Delete role assignment .....	86
5.2.5	Tab Individual Function Rights .....	86
5.3	Create new employee .....	88
5.4	Edit employee .....	88
5.5	Delete employee .....	89
<b>6</b>	<b>Roles module .....</b>	<b>90</b>
6.1	Main view .....	90
6.1.1	Toolbar .....	90
6.2	Detail view .....	91
6.2.1	Tab Details .....	92
6.2.2	Tab Employees .....	92

6.2.2.1	Assign users .....	92
6.2.2.2	Delete user assignment .....	93
6.2.3	Tab Function Rights.....	93
6.3	Create new role .....	95
6.4	Duplicate role.....	95
6.5	Edit role.....	96
6.6	Delete role .....	96
<b>7</b>	<b>Predefined function packages.....</b>	<b>98</b>
7.1	Create superuser .....	98
7.2	Create superadmin .....	98
	<b>List of figures .....</b>	<b>100</b>
	<b>List of tables.....</b>	<b>104</b>
	<b>Glossary .....</b>	<b>105</b>

## 1 General information

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

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

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

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

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

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

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

## 2 Introduction

The Neo system has been designed as a potential multi-tenant system. This means several different tenants can be administered within one system. These tenants are created and administered by the system provider 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:	<i>system-admin</i>
Neo version < 6.3	
Default password:	1
	If the default password 1 has never been changed before a software update to a Neo version $\geq 6.3$ , 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 $\geq 6.3$ , the changed password remains.
Neo version $\geq 6.3$	
Default password:	<i>A\$c123</i>

Tab. 1: Login data - system provider

Login data for the administrator of the 1st tenant:

User name:	<i>1st-tenant-admin</i>
Neo version < 6.3	
Default password:	1
	If the default password 1 has never been changed before a software update to a Neo version $\geq 6.3$ , 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 $\geq 6.3$ , the changed password remains.
Neo version $\geq 6.3$	
Default password:	<i>A\$c123</i>

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. 71.](#)

- 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. 90.](#)



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



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



If you change users' function rights or their assigned roles while they are logged in, this change only comes into effect after the users have logged off and in again.

Users are not notified when their function rights or roles have been changed.





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

The product line Neo supports 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. 55.
- Always activate **LDAP** authentication.  
See chapter "Group field Login Settings", p. 41.
- Activate **LDAP** authentication for individual users.  
See chapter "Authentication via LDAP", p. 81.



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



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




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

### 3.1

#### Install certificate

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

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

## 3.2

## Troubleshooting

**LDAP SSL connection does not work**

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

## 4 Tenants module

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

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

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

### 4.1 Main view

In the main view, all saved tenants are displayed.

+ × Tenants General ▾					
Name ▴	Customer ID ⇅	Type	Country ⇅	Creation Date ⇅	Updated ⇅
▼ System		System provider		02/28/2011 3:20:52 PM	11/06/2018 11:56:38 AM
1st-tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM
2nd-Tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM
3rd-Tenant		Tenant		01/01/2012 1:00:00 PM	11/06/2018 12:39:52 PM

Fig. 1: Tenants module - main view



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

#### 4.1.1 Toolbar

The toolbar offers the following functions.

+ × Tenants General ▾
-----------------------

Fig. 2: Tenants module - toolbar

	<i>Add</i>	Creates a new tenant or reseller (see <a href="#">chapter "Create new tenants manually", p. 67</a> ).
	<i>Delete</i>	Deletes the selected tenant (see <a href="#">chapter "Delete tenant", p. 70</a> ).
<i>Tenants</i>		This menu is currently not available
<i>General</i>	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.

*Module Help*

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



For detailed 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

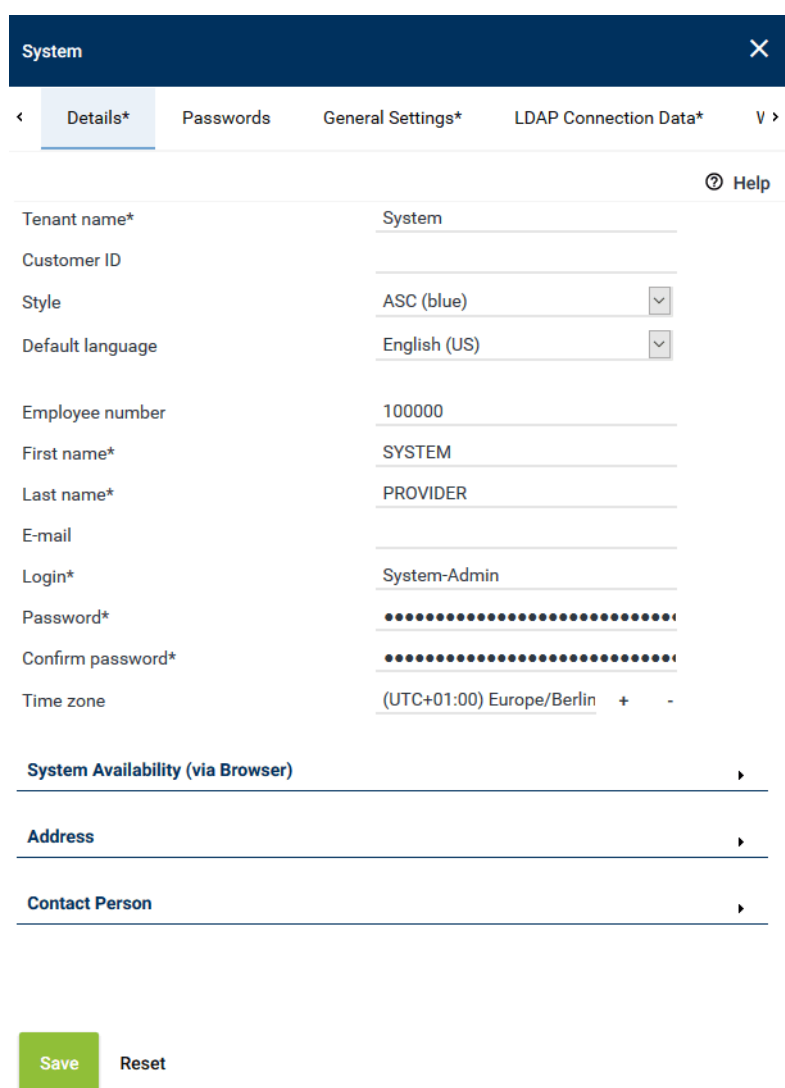


Fig. 3: Tenants module - detail view for the tenant "System"

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.

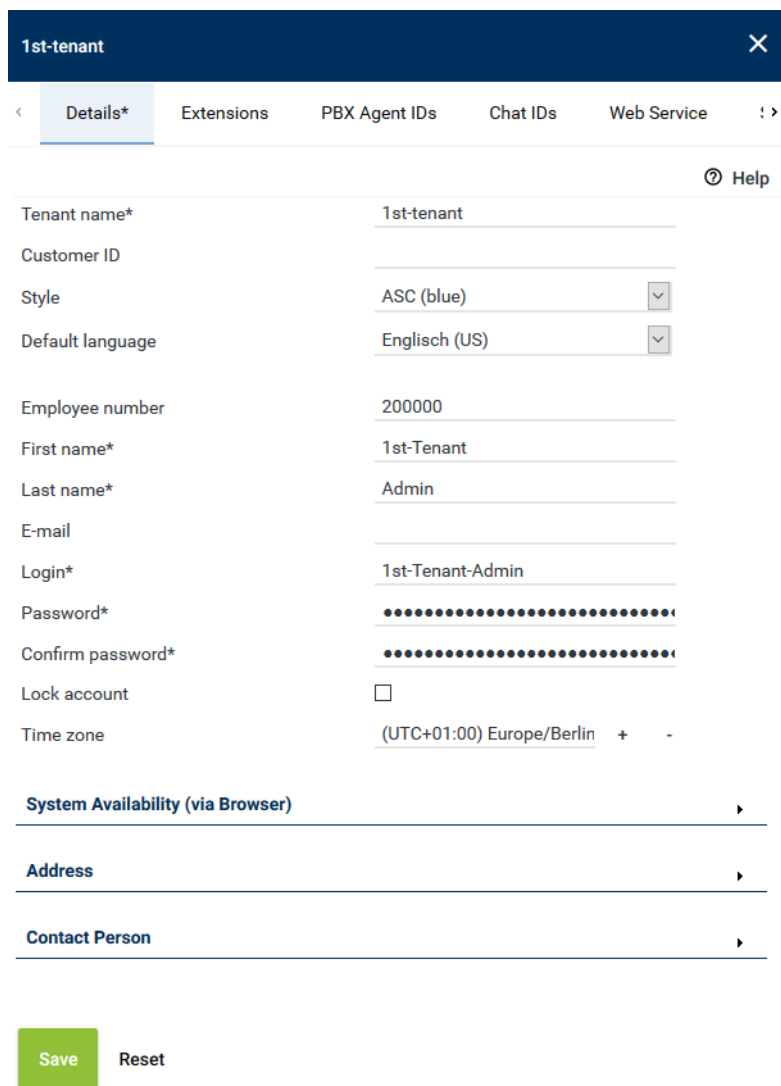
See [chapter "Tab LDAP Connection Data", p. 55](#).

- *Web Service*

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

See [chapter "Tab Web Service", p. 56](#).

#### 4.2.2 Detail view for normal tenants



The screenshot shows the '1st-tenant' detail view in the Tenants module. The interface has a dark blue header with the tenant name and a close button. Below the header is a tabbed interface with 'Details\*' selected. The 'Details\*' tab contains a form with the following fields:

- Tenant name\*: 1st-tenant
- Customer ID: (empty)
- Style: ASC (blue) (dropdown)
- Default language: Englisch (US) (dropdown)
- Employee number: 200000
- First name\*: 1st-Tenant
- Last name\*: Admin
- E-mail: (empty)
- Login\*: 1st-Tenant-Admin
- Password\*: (masked with dots)
- Confirm password\*: (masked with dots)
- Lock account: ☐
- Time zone: (UTC+01:00) Europe/Berlin (dropdown)

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

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.

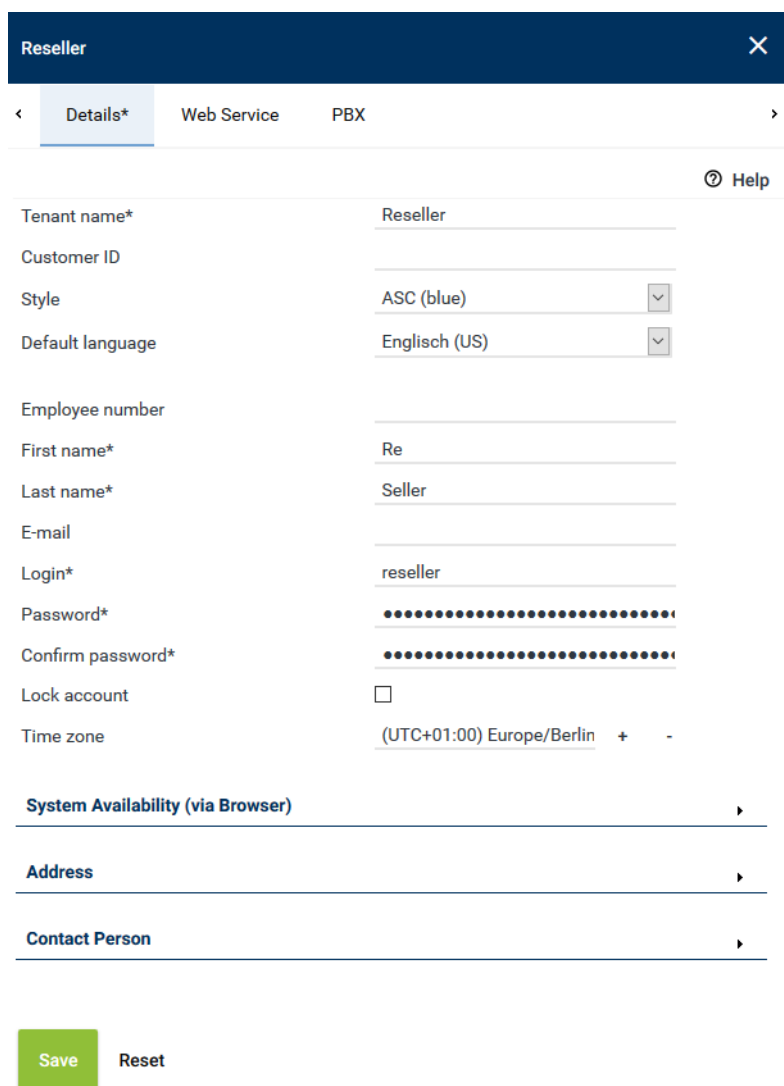
See [chapter "Tab Web Service"](#), p. 56.

- *Tenant Features*

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

See [chapter "Tab Tenant Features"](#), p. 66.

### 4.2.3 Detail view for resellers



**Reseller** [X]

< **Details\*** Web Service PBX >

[?] Help

Tenant name\* Reseller

Customer ID

Style ASC (blue) [v]

Default language Englisch (US) [v]

Employee number

First name\* Re

Last name\* Seller

E-mail

Login\* reseller

Password\* .....

Confirm password\* .....

Lock account ☐

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

**System Availability (via Browser)** [v]

**Address** [v]

**Contact Person** [v]

**Save** **Reset**

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. 56.](#)
- **PBX**  
Here, you can activate and administrate **PBX** filters which have been assigned to the selected reseller.  
See [chapter "Tab PBX", p. 64.](#)

### 4.2.4 Tab Details

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

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



1st-tenant

<

Details\*

Extensions

PBX Agent IDs

Chat IDs

Web Service

>

Help

Tenant name\*

1st-tenant

Customer ID

Style

ASC (blue)

Default language

Englisch (US)

Employee number

200000

First name\*

1st-Tenant

Last name\*

Admin

E-mail

Login\*

1st-Tenant-Admin

Password\*

Confirm password\*

Lock account

☐

Time zone

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

System Availability (via Browser)

Address

Contact Person



Save

Reset

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

- Enter the following information in the general section:
  - General information about the tenant profile
  - Personal data of the administrator of the tenant
  - Login data for the administrator of the tenant

<i>Tenant name</i>	Name which is displayed for the tenant in the system.
<i>Customer ID</i>	Enter the customer ID. <b>NOTICE!</b> The assignment of customer IDs is subject to the hierarchy in the system: The customer ID that a system provider assigns to a reseller or to a tenant cannot be changed or deleted by this reseller or tenant.
<i>Style</i>	Layout in which the tenant sees the user interface of the system. Select one of the available layouts from the drop-down list.
<i>Default language</i>	Language in which the user interface of the system is displayed for the tenant. Select the language from the drop-down list.
<i>Employee number</i>	Employee number of the administrator of the tenant.
<i>First name</i>	First name of the administrator of the tenant.
<i>Last name</i>	Last name of the administrator of the tenant.


<i>E-mail</i>	E-mail address of the administrator of the tenant.
<i>Login</i>	User name of the administrator of the tenant.
<i>Password</i>	Password which is required for the administrator of the tenant to log in to the system.
<i>Confirm password</i>	Repetition of the password for the administrator.
<i>Lock account</i>	<p>This option allows locking the tenant's account. The tenant can then no longer log in to Neo.</p> <p><b>NOTICE!</b></p> <p>This option locks the account of exclusively this tenant. The lock does not extend to the users of the tenants. This means that the users of the tenant can continue to log in to Neo.</p>
<i>Time zone</i>	<p>Shows the time zone in which the conversations are supposed to be displayed in the replay applications. This time zone is defined as a pre-setting for all other, newly created employees. If required, you can edit the time zone for each employee separately. The configuration in the Employees module has a higher priority.</p> <p>To select the time zone, click on the button . See <a href="#">chapter "Add time zone", p. 18</a>.</p> <p>To delete the selection, click on the button .</p>

The information in the following group fields is optional:




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



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

#### 4.2.4.1 Add time zone

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


 

Fig. 7: Add time zone

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

Example:

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

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

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

3. Select a time zone from the list.

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

Fig. 9: Add time zone

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

#### 4.2.4.2 Group field System Availability

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

System Availability (via Browser)

+ System Availability (via Browser)

Fig. 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*.

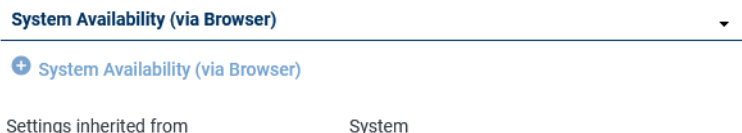



Fig. 11: System Availability (via Browser)

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.

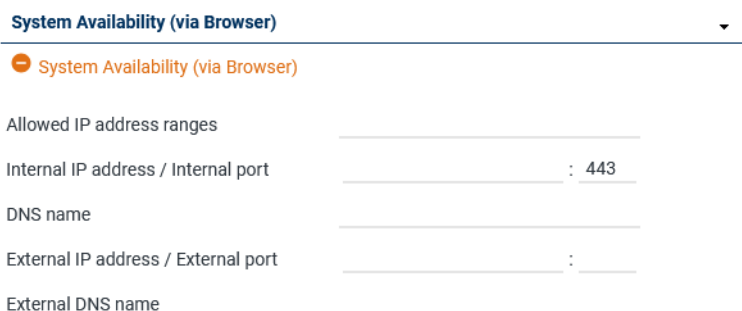


Fig. 12: Configure system availability


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



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



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


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.

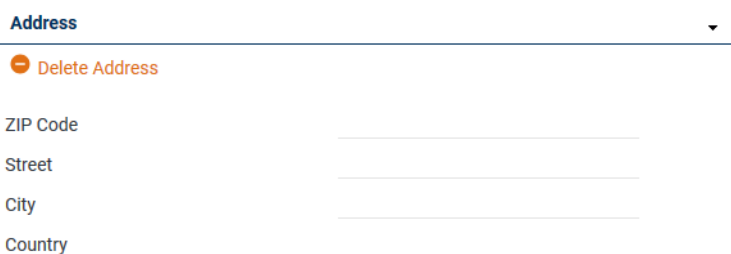



Fig. 14: Add address


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.

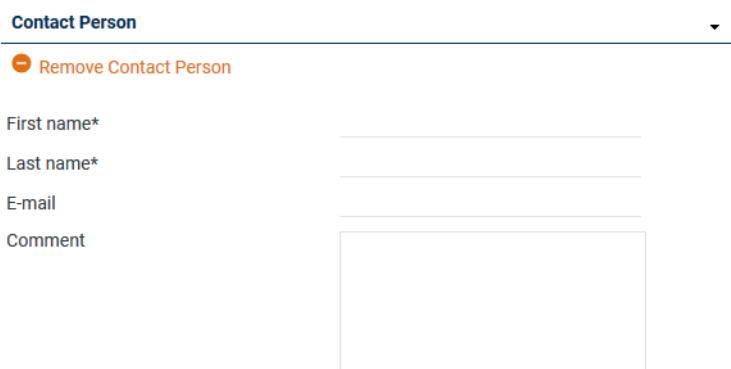


Fig. 16: Add contact person



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

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

#### 4.2.5 Tab Extensions

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



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

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



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

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

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

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

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

Add Extensions
✕

PBX

PBX

☐ File import

☐ File contains a headline

File name  ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 18: Assign extensions to tenants

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

<i>File import</i>	<p>Select the option to import extensions from an existing file and add them to the table of extensions.</p> <p>The following file formats are supported:</p> <ul style="list-style-type: none"> <li>ZIP</li> <li>TXT</li> <li>CSV</li> </ul> <p><b>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.</b></p>
	<p><i>File contains a headline</i></p> <p>Activate this option so that this structured is recognized correctly when importing the file.</p> <p>The 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.</p>
	<p><i>File name</i></p> <p>To import the file, proceed as follows:</p> <ul style="list-style-type: none"> <li>Click on the button <span style="background-color: #f1f3f4; padding: 0 5px;">...</span> behind the field <i>File name</i>.</li> <li>Click on the button <i>Choose File</i>.</li> <li>Select the respective file in the Explorer and click on the button <i>Open</i>.</li> <li>Click on the button <span style="background-color: #4285f4; color: white; padding: 0 5px;">↗</span> <i>Upload File</i>.</li> </ul>
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

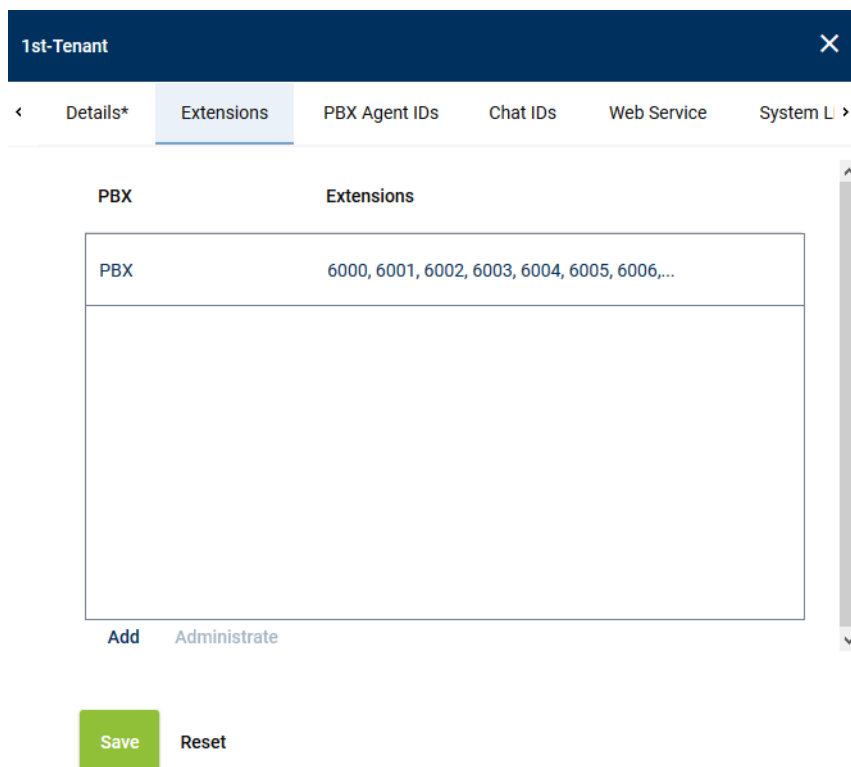
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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 detected, the window *Result* appears.  
Click on the button *Display Error Report* to open the window *Error Report*.  
To close the window *Error Report*, click on the button *Close*.  
To close the window *Result*, click on the button *Close*.
7. The configured extensions now appear in the detail view.
8. Click on the button *Save* in the detail view to save the entries.

#### 4.2.5.2 Remove extensions

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



The screenshot shows a web interface for managing a tenant's extensions. At the top, there's a header '1st-Tenant' with a close button. Below it is a navigation bar with tabs: 'Details\*', 'Extensions' (selected), 'PBX Agent IDs', 'Chat IDs', 'Web Service', and 'System L'. The main content area has a table with two columns: 'PBX' and 'Extensions'. The 'PBX' column has a single entry with a link 'PBX'. The 'Extensions' column has a single entry with the text '6000, 6001, 6002, 6003, 6004, 6005, 6006,...'. Below the table, there are two buttons: 'Add' and 'Administrate'. At the bottom of the interface, there are two buttons: 'Save' and 'Reset'.

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.



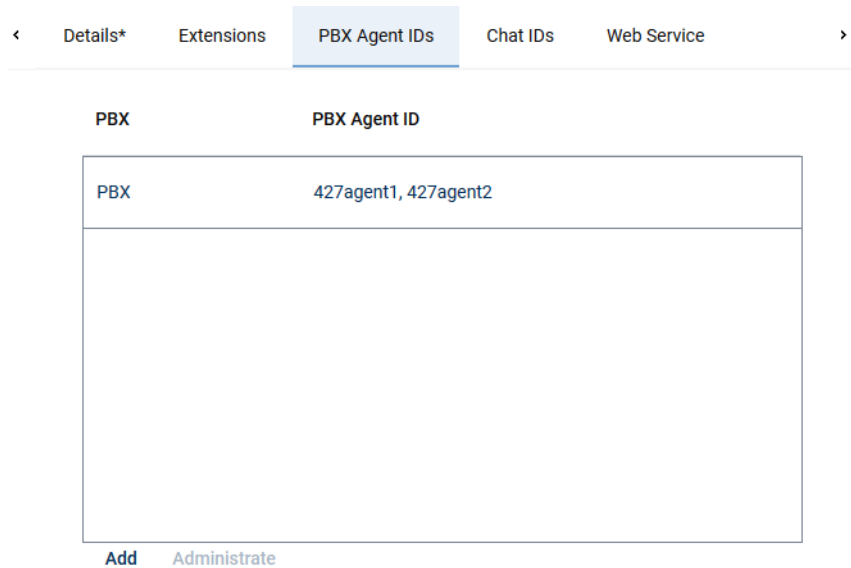
In 1-tenant systems, the PBX Agent IDs are automatically assigned to the tenant who has been created by the system (1st tenant). PBX Agent IDs are assigned to the user in the Employees module.

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.



PBX	PBX Agent ID
PBX	427agent1, 427agent2

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

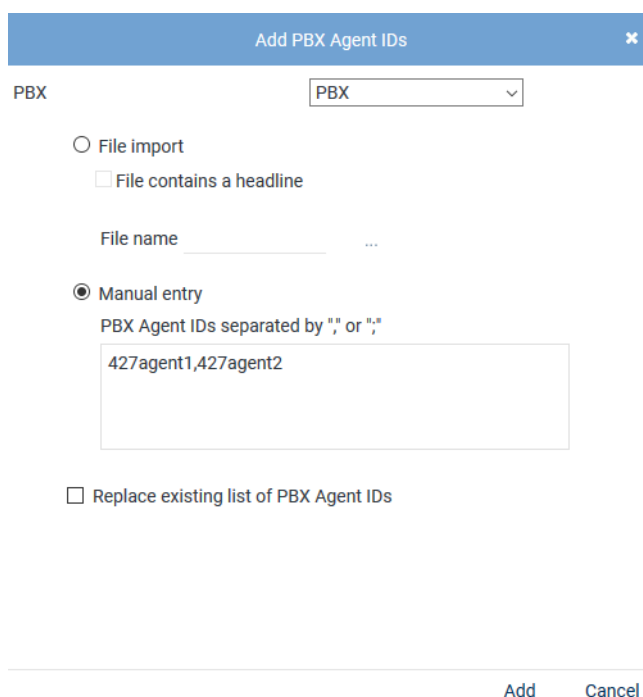
Fig. 21: Tenants module - tab PBX Agent ID

- 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:



Add PBX Agent IDs

PBX
PBX

☐ File import
☐ File contains a headline

File name

☒ Manual entry

PBX Agent IDs separated by ";" or ","



427agent1,427agent2

☐ Replace existing list of PBX Agent IDs

Add Cancel

Fig. 22: Assign PBX Agent IDs to tenants

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

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

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

#### 4.2.6.2 Remove PBX Agent ID

- In the list, select the **PBX** for which you would like to remove the assigned PBX Agent IDs.
- Click the button *Administrate*.
- 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.

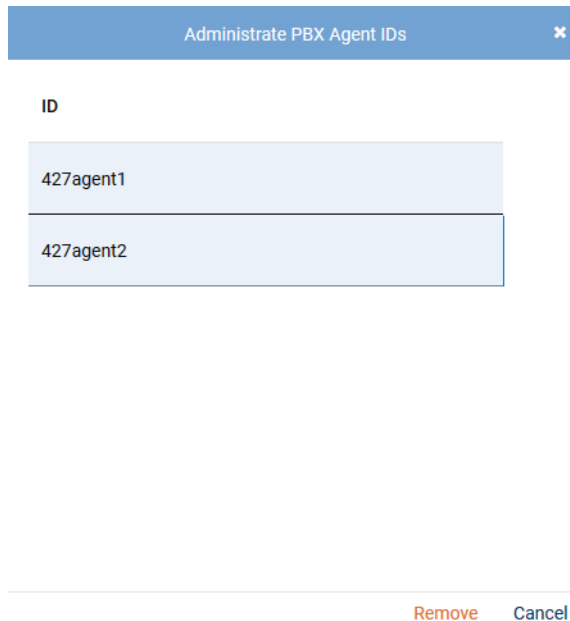


Fig. 23: Select PBX Agent IDs

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.

[Details\\*](#)
[Extensions](#)
[PBX Agent IDs](#)
[Chat IDs](#)
[Web Service](#)

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

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

Fig. 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:

Add Chat IDs

Chat system Openfire

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



☒ Manual entry  
 Chat IDs separated by ";" or "

☐ Replace existing list of chat IDs

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

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.

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

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

#### 4.2.7.2 Remove chat ID

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

Administrate Chat IDs
✕

ID

---

agent1@openfire2

agent2@openfire2

---

Remove
Cancel

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.

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

Password Length
▸

Mandatory Characters
▸

Security
▸

Forbidden Passwords
▸

Advanced Password Settings
▸

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.




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

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  $\geq$  *minimum length*.
5. If you would like to remove the entries, click on the button  *Remove password length* in the title bar of the group field.

### Group field Mandatory Signs

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



## Mandatory Characters


 Remove mandatory characters

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


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

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

### Group field Security

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

**Security**


 Remove security

Validity  
(max. 3 characters)
 Day(s)

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

Password history
 

☒ Password history in days  
 Day(s)

☐ Extent of password history


Possible failed login attempts  
(max. 3 characters)

Deny personal data
 ☐


Fig. 30: Configure password security

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



<i>Password history</i>	<p>Enter for how long the password history is supposed to be saved. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Password history in days</i> For this option, enter for how long the passwords are supposed to be saved in the password history.</li> <li>• <i>Extent of password history</i> For this option, enter the number of passwords which are supposed to be saved in the password history.</li> </ul> <p>In both cases, the password history is never deleted entirely. If the entered value is reached, only the oldest entries are deleted.</p>
<i>Possible failed login attempts</i>	<p>Enter how often the user may enter an incorrect password before the account is locked.</p> <p><b>NOTICE!</b> A locked account can be released again by any user with access to the Employees module and to the data of the locked user.</p>
<i>Deny personal data</i>	<p>Define whether users are allowed to use private data from their profiles for the password (e. g. name, user name, date of birth).</p> <p><input checked="" type="checkbox"/> = Personal data is not allowed. <input type="checkbox"/> = Personal data is allowed.</p>

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.

#### Forbidden Passwords

Server	
System	







 

Fig. 31: Define forbidden passwords

	Adds a new entry to the list.
	Deletes the selected entry from the list.
	Opens the selected entry for editing, see <a href="#">chapter "Edit entry", p. 36</a> .

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

<i>Use blacklist for passwords</i>	<input checked="" type="checkbox"/> = Monitoring has been activated. <input type="checkbox"/> = 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.

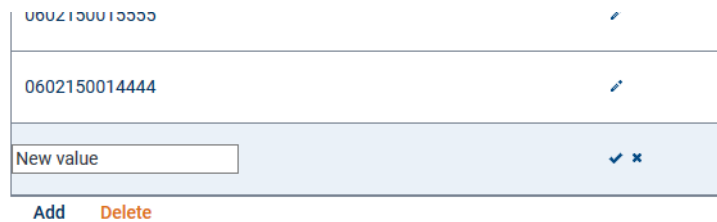




Fig. 33: Edit entry in the list

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.

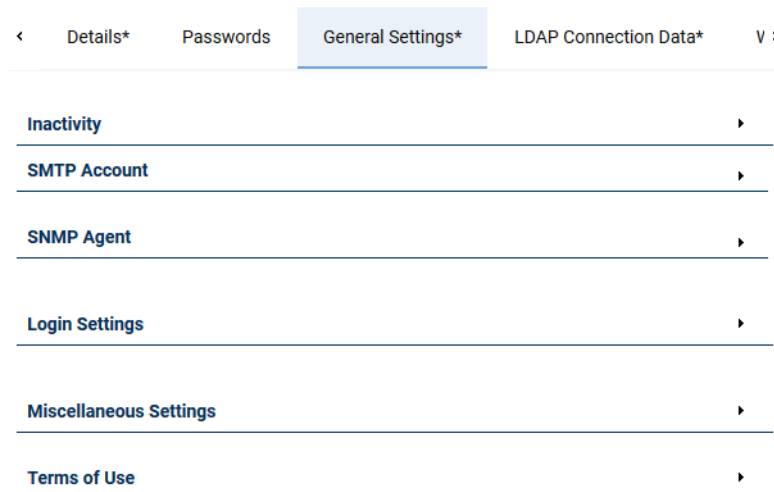
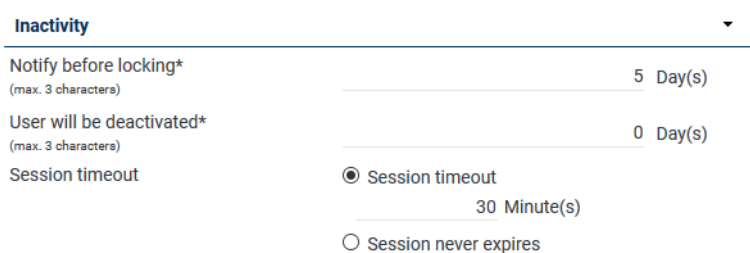


Fig. 34: Tenants module - tab General Settings

## 4.2.9.1 Group field Inactivity



**Inactivity**

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


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

Session timeout

☒ Session timeout 30 Minute(s)

☐ Session never expires

Fig. 35: Configure user activity

<i>Notify before locking</i>	<p>Select how many days before the locking of the account the user is supposed to be notified that the account will be locked due to inactivity. The account is locked if the user has been inactive for the number of days entered in the field <i>User will be deactivated</i>.</p> <p><i>Notify before locking</i> = 0: User is not notified.</p> <p>The notification is sent to the e-mail address of the user.</p>
<i>User will be deactivated</i>	<p>Select after how many days of inactivity the account of the user is locked.</p> <p><i>User will be deactivated</i> = 0: User is not deactivated.</p>
<i>Session timeout</i>	<p>Select after how many minutes of inactivity the session of the user is supposed to be ended automatically by timeout. Select one of the following options:</p> <ul style="list-style-type: none"> <li><i>Session timeout</i> This option activates the session timeout. Enter a value between 5 and 1440.</li> <li><i>Session never expires</i> This option deactivates the session timeout and enables endless sessions.</li> </ul> <p><b>NOTICE!</b> 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) &gt; Logoff) but closes the browser directly, then the started session will never be finished. Each endless session consumes storage space. This may result in the necessity to reboot the server. Upon rebooting the server, all sessions are ended.</p>



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

## 4.2.9.2 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.

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



**SMTP Account**

+ 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.*

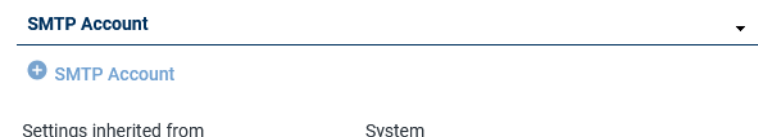


Fig. 37: SMTP account

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**.

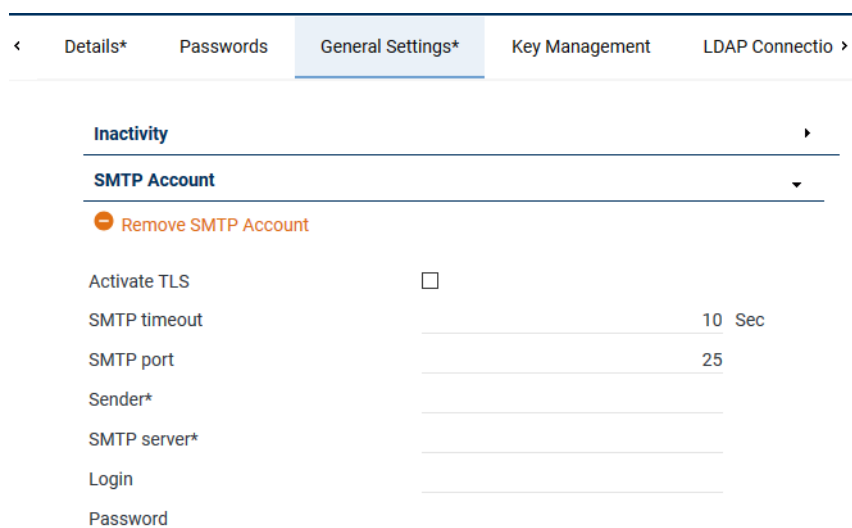


Fig. 38: Add SMTP account




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:

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

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

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

#### 4.2.9.3 Group field SNMP Agent

To 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.

Use a different network port for the Neo **SNMP** agent than the default **SNMP** port of the operating system or deactivate the **SNMP** service of the operating system if you do not need it for other applications.


By means of SNMPget, the system status can be polled. Possible results from a system status request are:

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

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

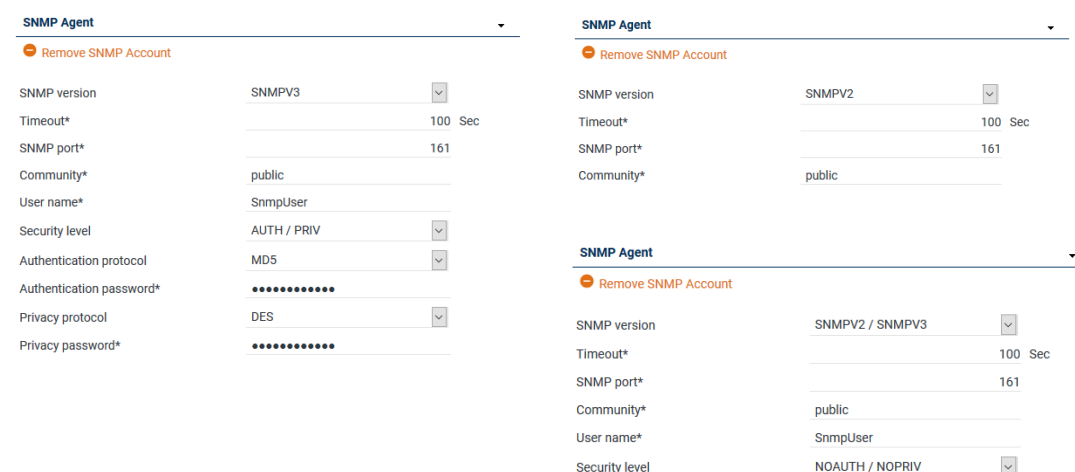
- C:\Program Files (x86)\ASC\ASC Product Suite\data\mib\ASC-SNMP-MIB-NEO.txt*

#### Set up SNMP agent

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



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



The figure displays two examples of the 'SNMP Agent' configuration form. Both forms include a title bar with a 'Remove SNMP Account' button. The left form is for 'SNMPV3' and includes fields for 'SNMP version' (SNMPV3), 'Timeout\*' (100 Sec), 'SNMP port\*' (161), 'Community\*' (public), 'User name\*' (SnmpUser), 'Security level' (AUTH / PRIV), 'Authentication protocol' (MD5), 'Authentication password\*' (masked), 'Privacy protocol' (DES), and 'Privacy password\*' (masked). The right form is for 'SNMPV2' and includes fields for 'SNMP version' (SNMPV2), 'Timeout\*' (100 Sec), 'SNMP port\*' (161), 'Community\*' (public), 'User name\*' (SnmpUser), and 'Security level' (NOAUTH / NOPRIV).

Fig. 39: Group field SNMP Agent (examples)

## 3. Complete all required fields:

<i>SNMP version</i>	<p>From the drop-down list, select the <b>SNMP</b> version you would like to use.</p> <p>The following versions are available:</p> <ul style="list-style-type: none"> <li>• <i>SNMPV2</i></li> <li>• <i>SNMPV2 / SNMPV3</i></li> <li>• <i>SNMPV3</i></li> </ul>
<i>Timeout</i>	Enter after how many seconds a timeout notification is supposed to be sent if no connection to the <b>SNMP</b> server could be established.
<i>SNMP port</i>	<p>Enter the port via the <b>SNMP</b> request are supposed to come in. Default value: <i>161</i></p> <p><b>NOTICE!</b> If the <b>SNMP</b> service of the operating system is used as well, you <b>cannot</b> use the default port. In this case, enter a different port, e. g. <i>1161</i>.</p> <p><b>NOTICE!</b> For more information about the installation of the <b>SNMP</b> service refer to the respective installation manual <i>Configuration Microsoft Windows Server</i>.</p>
<i>User name</i>	<p>(Only for <b>SNMP</b> versions <i>SNMPV2/SNMPV3</i> and <i>SNMPV3</i>.)</p> <p>Define the user name which has to be used for <b>SNMP</b> requests.</p>
<i>Security level</i>	<p>(Only for <b>SNMP</b> versions <i>SNMPV2/SNMPV3</i> and <i>SNMPV3</i>.)</p> <p>From the drop-down list, select the security level you would like to use.</p> <p>The following security levels are available:</p> <ul style="list-style-type: none"> <li>• <i>NOAUTH / NOPRIV</i> <p>The external <b>SNMP</b> program does not have to authenticate.</p> <p>The <b>SNMP</b> answer is transferred without encryption.</p> </li> <li>• <i>AUTH / NOPRIV</i> <p>Select this option if you want the external <b>SNMP</b> program to authenticate while the <b>SNMP</b> answer is transferred without encryption.</p> <p>In this case, select a protocol type in the field <i>Authentication protocol</i> and enter a corresponding password in the field <i>Authentication password</i>.</p> </li> <li>• <i>AUTH / PRIV</i> <p>Select this option if you want the external <b>SNMP</b> program to authenticate and the <b>SNMP</b> answer to be transferred with encryption.</p> <p>In this case, select a protocol type in the field <i>Authentication protocol</i> and enter a corresponding password in the field <i>Authentication password</i>.</p> <p>In this case, additionally select a protocol type in the field <i>Privacy protocol</i> and enter a corresponding password in the field <i>Privacy password</i>.</p> </li> </ul>
<i>Authentication protocol</i>	<p>(Only for security levels <i>AUTH / NOPRIV</i> and <i>AUTH / PRIV</i>.)</p> <p>Select the protocol that you would like to use for the authentication of the external <b>SNMP</b> program.</p> <p>The following protocol types are available:</p> <ul style="list-style-type: none"> <li>• <i>MD5</i></li> <li>• <i>SHA</i></li> </ul>
<i>Authentication password</i>	<p>(Only for security levels <i>AUTH / NOPRIV</i> and <i>AUTH / PRIV</i>.)</p> <p>Enter a password for the authentication here.</p> <p>Length of the password: 8 to 15 characters</p>




**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 **SNMP** account, click on the button  *Remove SNMP Account* in the title bar of the group field.

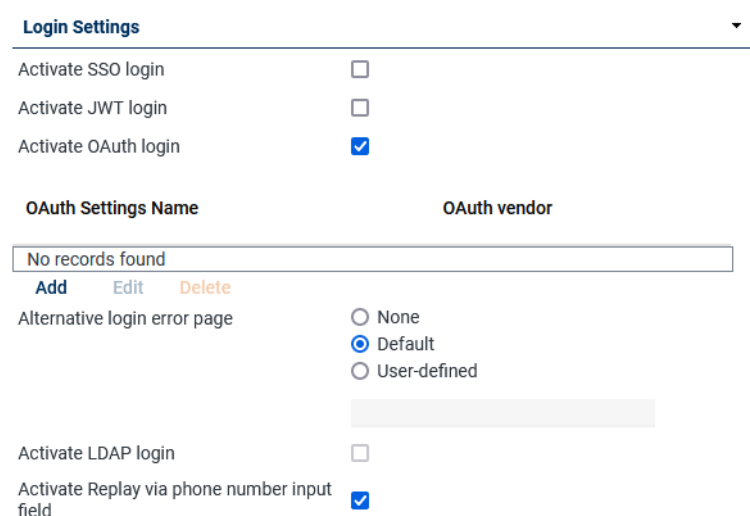


Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.



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

#### 4.2.9.4 Group field Login Settings



**Login Settings**

Activate SSO login ☐

Activate JWT login ☐

Activate OAuth login ☒

OAuth Settings Name	OAuth vendor
No records found	

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

Alternative login error page ☐ None ☒ Default ☐ User-defined

Activate LDAP login ☐

Activate Replay via phone number input field ☒

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.

	<p>Format: <i>Domain\Windows_login_name</i></p> <p><b>NOTICE!</b> The login password in the recording system does <b>not</b> have to be the same as the password of the Windows account.</p> <p><b>NOTICE!</b> If you activate <a href="#">SSO</a> login as well as <a href="#">LDAP</a> login, the LDAP data is ignored if users log in with their Windows accounts.</p> <p><b>Restrictions</b> when using <a href="#">SSO</a>:</p> <ul style="list-style-type: none"> <li>• Combination login not possible</li> <li>• 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.</li> </ul>
Activate JWT login	<p>Here, you can activate or deactivate the authentication by means of <a href="#">JSON</a> Web Token login for the users of the recording system.</p> <p>Activate or deactivate the authentication by means of JWT login.</p> <p><input checked="" type="checkbox"/> = activated  <input type="checkbox"/> = not activated</p> <p>JWT login is a special login procedure; the application receives an external <a href="#">JSON</a> Web Token with certain identification attributes that it is asked to authenticate.</p> <p>If the information in the token is valid, the user is logged in to the system without having to enter another password.</p> <p>If the information in the token is invalid, the user is denied access.</p> <p><b>NOTICE!</b> To be able to check the validity of external tokens, a valid certificate of the external system must be imported in Neo.</p>
Activate OAuth login	<p>Here, you can activate or deactivate the authentication by means of OAuth2 login for the users of the recording system.</p> <p>Activate or deactivate the authentication by means of OAuth2.</p> <p><input checked="" type="checkbox"/> = activated  <input type="checkbox"/> = not activated</p>
OAuth Settings Name/ OAuth provider	<p>Click on the button <i>Add</i> to configure the OAuth provider, see <a href="#">chapter "Edit OAuth provider settings", p. 43</a>.</p> <p>To edit an existing OAuth provider, click on the button <i>Edit</i>.</p> <p>To delete an existing OAuth provider, click on the button <i>Delete</i>.</p>
Alternative login error page	<p>Here, you can activate that an alternative login error page is displayed in case of an invalid login.</p> <p>Activate that an alternative login error page is displayed.</p> <ul style="list-style-type: none"> <li>• <i>None</i>  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.</li> <li>• <i>Default</i>  This option activates the default login error page.  In case of a login error, a new page is displayed. This page explains that the login has failed and asks users to contact the administrator.</li> </ul> <p><b>CAUTION!</b> This option is only useful for JWT login or Mitel OAuth. If this option is selected, no login page appears! Login will then only be possible via JWT or Mitel OAuth.</p>

	<ul style="list-style-type: none"> <li>• <i>User-defined</i></li> </ul> <p>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. <a href="#">www.example-login-error.de</a>).</p> <p>In case of a login error, the entered web address is called up.</p> <p><b>CAUTION!</b> This option is only useful for JWT login or Mitel OAuth. If this option is selected, no login page appears! Login will then only be possible via JWT or Mitel OAuth.</p>
<i>Activate LDAP login</i>	<p>Here, you can activate or deactivate the authentication via <a href="#">LDAP</a> for the users of your environment.</p> <p>Activate or deactivate the authentication via <a href="#">LDAP</a>.</p> <p><input checked="" type="checkbox"/> = <a href="#">LDAP</a> login has been activated.  <input type="checkbox"/> = <a href="#">LDAP</a> login has not been activated.</p> <p><b>NOTICE!</b> If you activate <a href="#">SSO</a> login as well as <a href="#">LDAP</a> login, the LDAP data is ignored if users log in with their Windows accounts.</p> <p><b>NOTICE!</b> <a href="#">LDAP</a> login cannot be activated before you have configured at least one <a href="#">LDAP</a> connection, see <a href="#">chapter "Tab LDAP Connection Data", p. 55</a>.</p>
<i>Activate Replay via telephone number input field</i>	<p>Activate or deactivate the entry field to enter the replay via phone number when logging in to <a href="#">POWERplay</a> Web.</p> <p><input checked="" type="checkbox"/> = Field to enter replay via phone number is displayed on the login screen of <a href="#">POWERplay</a> Web.  <input type="checkbox"/> = Field to enter replay via phone number is not displayed on the login screen of <a href="#">POWERplay</a> Web.</p>

#### 4.2.9.4.1 Edit OAuth provider settings

Here, you can configure the settings for the OAuth provider to allow logging in to Neo via OAuth 2.0 protocol. Different providers such as Microsoft Azure, Google, Mitel or customer-specific providers can be selected.

Edit OAuth Vendor Settings
✕

**General**

---

OAuth Settings Name\*

OAuth vendor

CUSTOM ▼

OAuth Flow Type

OPENID ▼

**URLs**

---

Well-known OpenID Configuration URL

Authorize URL

Token URL

**Settings**

---

OAuth Client ID\*

OAuth Client Secret\*

Redirect URL\*

Request scope\*

User name field\*

"Login With" image

[Upload File](#)

Uploaded image

OK

Cancel

Fig. 41: Edit OAuth provider settings (example Custom)

<i>OAuth Settings Name</i>	Enter the name here under which you have published the application with your OAuth provider.
<i>OAuth provider</i>	Select the customer-specific OAuth provider.
<i>OAuth Flow Type</i>	The OAuth Flow Type has been preselected and cannot be changed.
<i>Well-known OpenID Configuration URL</i>	Enter the Well-known OpenID Configuration URL.
<i>Authorize URL</i>	Enter the Authorize URL.
<i>Token URL</i>	Enter the Token URL.
<i>OAuth Client ID</i>	Enter the OAuth Client ID (e. g. ef0129223a2e3bf76e7c3d8422b15b).
<i>OAuth Client Secret</i>	Enter the OAuth Client Secret.
<i>Redirect URL</i>	Enter the Neo <a href="#">URL</a> (e. g. https://serveraddress/).
<i>Request scope</i>	The request scope has been preselected and cannot be changed.
<i>User name field</i>	The user name field has been preselected and cannot be changed.

"Login with" image	Click on the button <i>Upload File</i> to add an image which is supposed to be displayed on the login screen of the application. <b>NOTICE!</b> The image must have the size of 100x100 pixels.
Uploaded image	Here, you see a preview of the image that will be displayed on the login screen, if you have uploaded an image.

1. Click on the button *OK* to save the entries.  
Click on the button *Cancel* to discard the entries.

### Edit OAuth vendor settings Azure

Edit OAuth Vendor Settings

General

OAuth Settings Name*	Test01
OAuth vendor	AZURE
OAuth Flow Type	OPENID

URLs

Well-known OpenID Configuration URL	https://login.microsoftonline.com/co
-------------------------------------	--------------------------------------

Settings

OAuth Client ID*	ef012922-3a2e-3bf7-6e7c-3d8422b1
Redirect URL*	https://test.asc-neo.cloud/

Please configure your application under the following link. Enter the client ID above. As redirect URL use the URL your users will use to access the ASC system. Use HTTPS. In your provider registration, add all the ASC applications that you will be using. e. g.: https://yourservername/SystemConfiguration/

https://portal.azure.com/#blade/Microsoft\_AAD\_RegisteredApps/ApplicationsListBlade

Request scope*	openid email profile
User name field*	email
Your Azure Tenant ID*	c07fe031-e64c-421c-bd4b-71ded27d
"Login With" image	Upload File
Uploaded image	

OK Cancel

Fig. 42: Edit OAuth provider settings (example Azure)

<i>OAuth Settings Name</i>	Enter the name here under which you have published the application in Azure.
<i>OAuth provider</i>	Select the OAuth provider, here: AZURE.
<i>OAuth Flow Type</i>	The OAuth Flow Type has been preselected and cannot be changed.
<i>OAuth Client ID</i>	Enter the OAuth Client ID from Azure (e. g. ef0129223a2e3bf76e7c3d8422b15b).
<i>Redirect URL</i>	Enter the Neo <a href="#">URL</a> (e. g. https://serveraddress/).

<i>Link to Azure portal</i>	Click on this link to create the application in Azure, see <a href="#">chapter "Create OAuth login settings for Azure"</a> , p. 46.
<i>Request scope</i>	The request scope has been preselected and cannot be changed.
<i>User name field</i>	The user name field has been preselected and cannot be changed.
<i>Your Azure Tenant ID</i>	Enter your Azure Tenant ID.
<i>"Login with" image</i>	Click on the button <i>Upload File</i> to add an image which is supposed to be displayed on the login screen of the application. <b>NOTICE!</b> The image must have the size of 100x100 pixels.
<i>Uploaded image</i>	Here, you see a preview of the image that will be displayed on the login screen, if you have uploaded an image.

- Click on the button *OK* to save the entries.  
Click on the button *Cancel* to discard the entries.



The user name of the employee logging in via Azure must be identical in the account settings (see Employees module [chapter "Tab Account"](#), p. 80) and in Azure.

### Create OAuth login settings for Azure

- In the window *Edit OAuth Provider Settings*, click on the link [https://portal.azure.com/#view/Microsoft\\_AAD\\_RegisteredApps/ApplicationsListBlade](https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade).
- Log in to Azure.

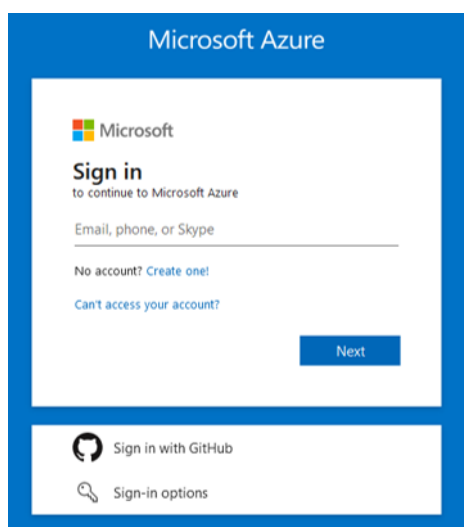


Fig. 43: Azure login

- Click on the button *+ New Registration*.

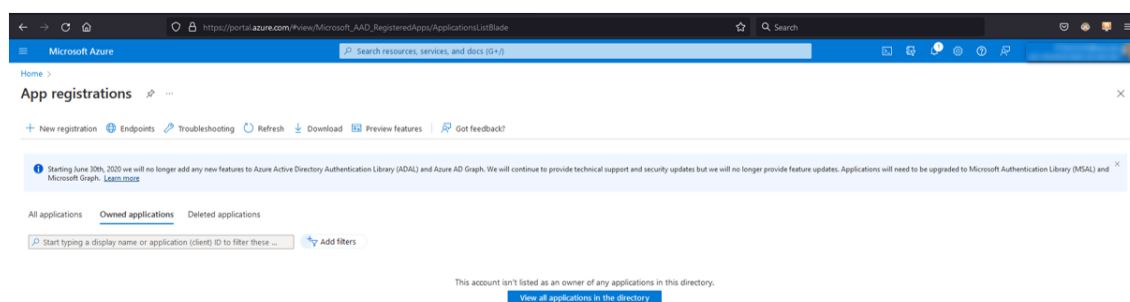


Fig. 44: New registration

- Enter a name in the entry field *Name*.

5. Under *Supported account types*, select an option who may use the app or access the API.
6. Under *Redirect URI (optional)*, select the platform and enter the Neo URL, e. g. `https://test.asc-neo.cloud/Portal/`.

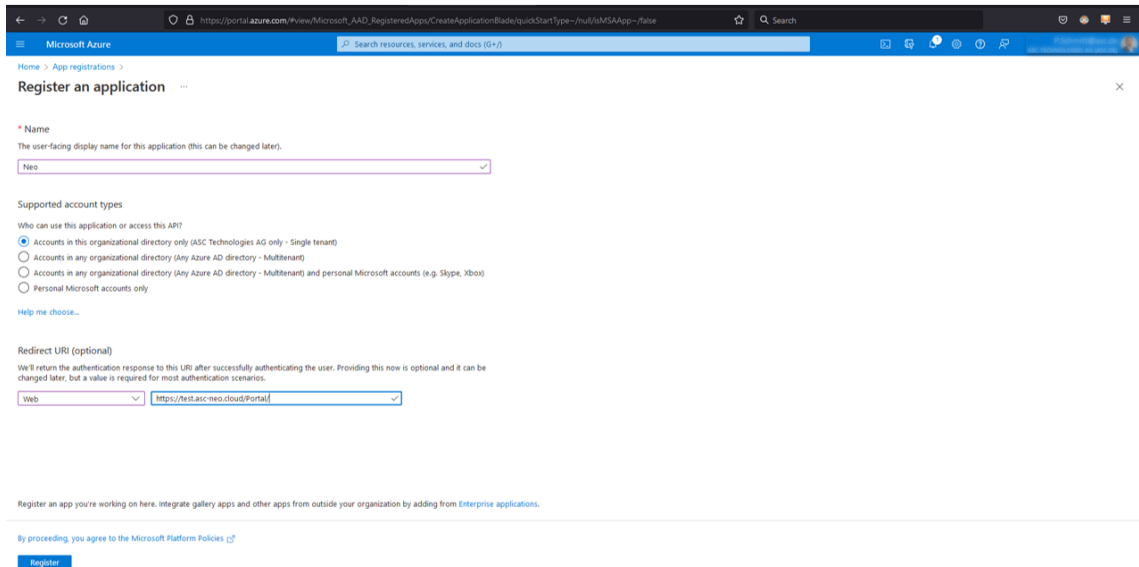


Fig. 45: Register application

7. Confirm your entries by clicking on the button *Register*.
8. Make a note of the *Application (client) ID* to enter it subsequently in the window *Edit OAuth Provider Settings* as OAuth Client ID.

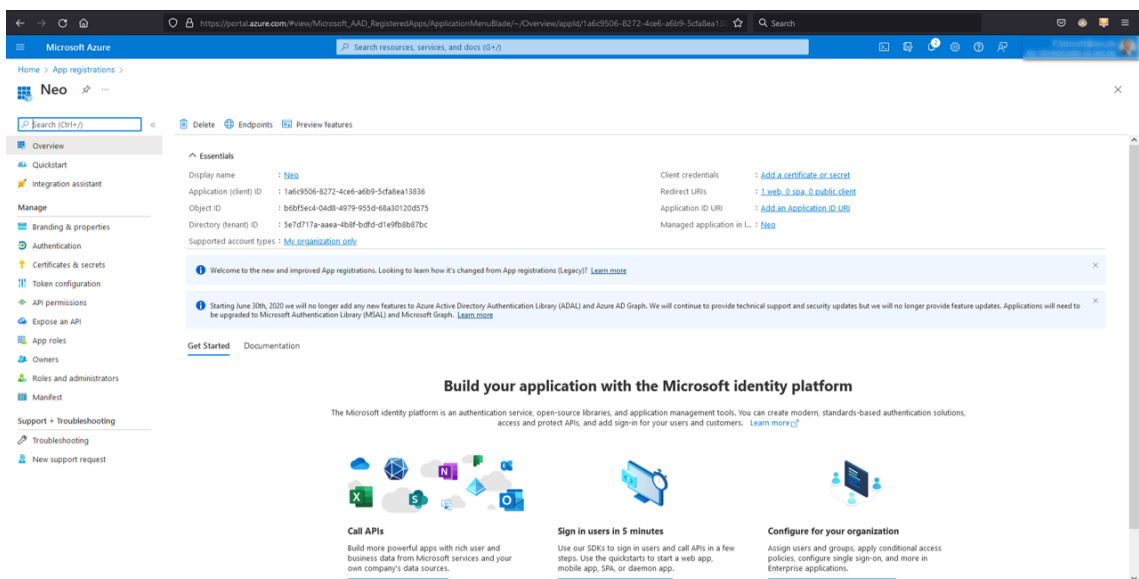


Fig. 46: Application (client) ID / OAuth Client ID

9. In the context menu, select the menu item *Authentication* and click on *Web > Redirect URIs*.
10. Enter the URIs of **all** web applications which are supposed to support the OAuth login.



The URI must finish in a "/".

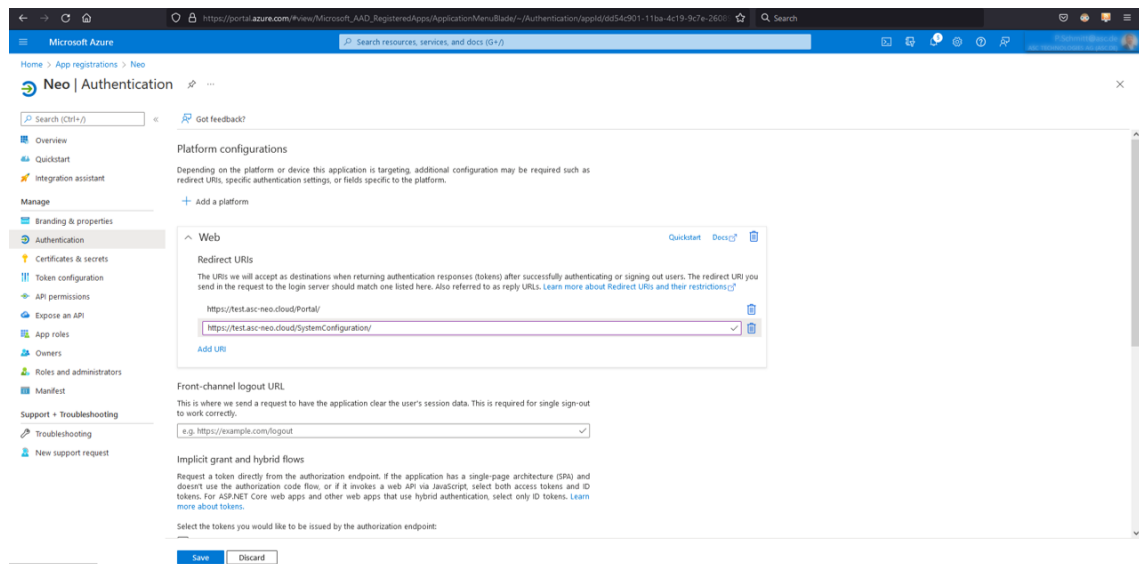


Fig. 47: Enter URI

11. Save your entries by clicking on the button **Save**.
12. Under *Implicit grant hybrid flows*, select which tokens are supposed to be issued by the authorization endpoint by activating the check box *ID tokens (used for implicit and hybrid flows)*.
13. Under *Supported account types*, select the option *Accounts in my organizational directory* to be able to turn the app into a multi-tenant app if required.

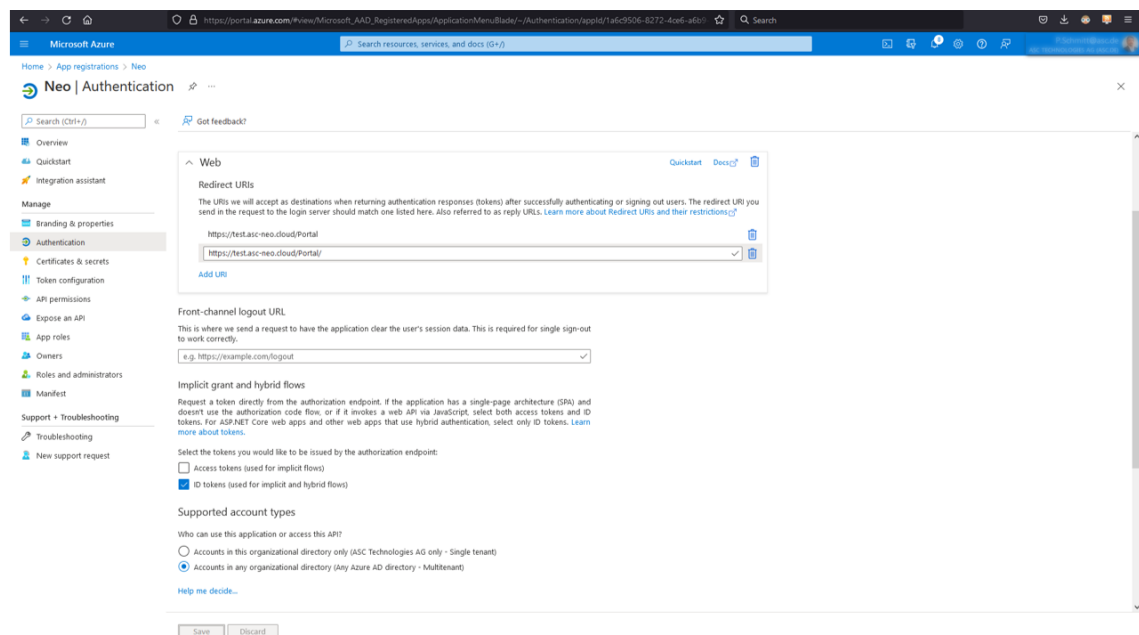


Fig. 48: Enter ID tokens

14. To save the entries, click on the button **Save**.
15. Enter the information in the window *Edit OAuth Provider Settings*, see [chapter "Edit OAuth vendor settings Azure"](#), p. 45.



### Edit OAuth provider settings Google

Edit OAuth Vendor Settings ✕

**General**

OAuth Settings Name*	neo
OAuth vendor	GOOGLE <span style="float: right;">▼</span>
OAuth Flow Type	OPENID <span style="float: right;">▼</span>

**URLs**

Well-known OpenID Configuration URL	<a href="https://accounts.google.com/.well-known/openid-configuration">https://accounts.google.com/.well-known/openid-configuration</a>
-------------------------------------	---

**Settings**

OAuth Client ID*	<input type="text"/>
Redirect URL*	<input type="text"/>

Please configure your application under the following link. Enter the client ID above. As redirect URL use the URL your users will use to access the ASC system. Use HTTPS. In your provider registration, add all the ASC applications that you will be using. e. g.: <https://yourservername/SystemConfiguration/>

<https://console.cloud.google.com/apis/credentials>

Request scope*	openid email profile
User name field*	email
"Login With" image	<a href="#">Upload File</a>
Uploaded image	

OK
Cancel

Fig. 49: Edit OAuth provider settings (example Google)

<i>OAuth Settings Name</i>	Enter the name here under which you have published the application in Google.
<i>OAuth provider</i>	Select the OAuth provider, here: GOOGLE.
<i>OAuth Flow Type</i>	The OAuth Flow Type has been preselected and cannot be changed.
<i>OAuth Client ID</i>	Enter the OAuth Client ID from Google (e. g. ef0129223a2e3bf76e7c3d8422b15b).
<i>Redirect URL</i>	Enter the Neo <a href="#">URL</a> (e. g. <a href="https://serveraddress/">https://serveraddress/</a> ).
<i>Link to Google portal</i>	Click on this link to create the application in Google, see <a href="#">chapter "Create OAuth login data for Google"</a> , p. 50.
<i>Request scope</i>	The request scope has been preselected and cannot be changed.
<i>User name field</i>	The user name field has been preselected and cannot be changed.
<i>"Login with" image</i>	Click on the button <i>Upload File</i> to add an image which is supposed to be displayed on the login screen of the application. <b>NOTICE!</b> The image must have the size of 100x100 pixels.

### Uploaded image

Here, you see a preview of the image that will be displayed on the login screen, if you have uploaded an image.

1. Click on the button *OK* to save the entries.  
Click on the button *Cancel* to discard the entries.

### Create OAuth login data for Google

1. In the window *Edit OAuth Provider Settings*, click on the link <https://console.cloud.google.com/apis/credentials>.
2. Log in to Google:

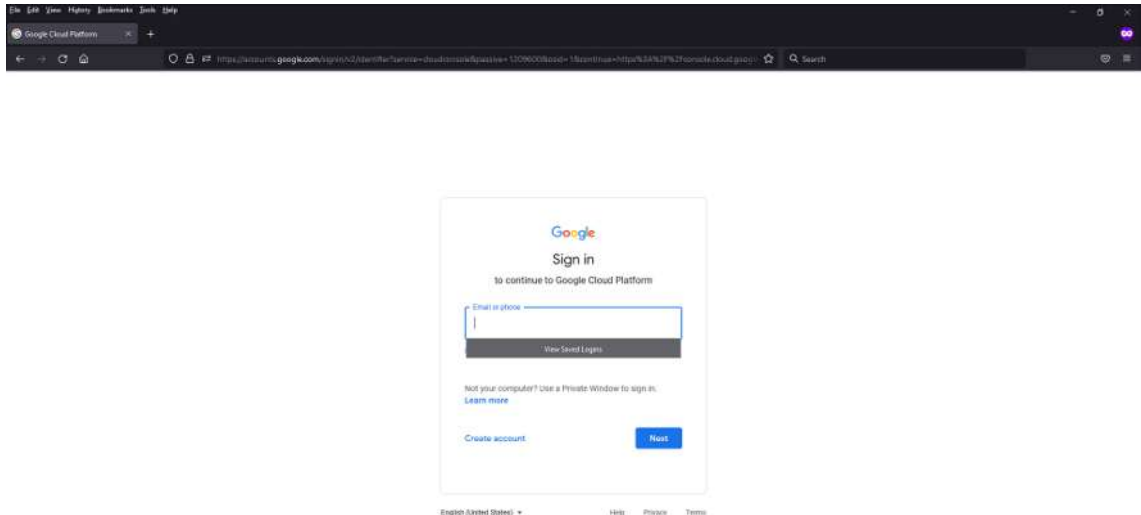


Fig. 50: Google login

3. Select the menu item *Credentials*.

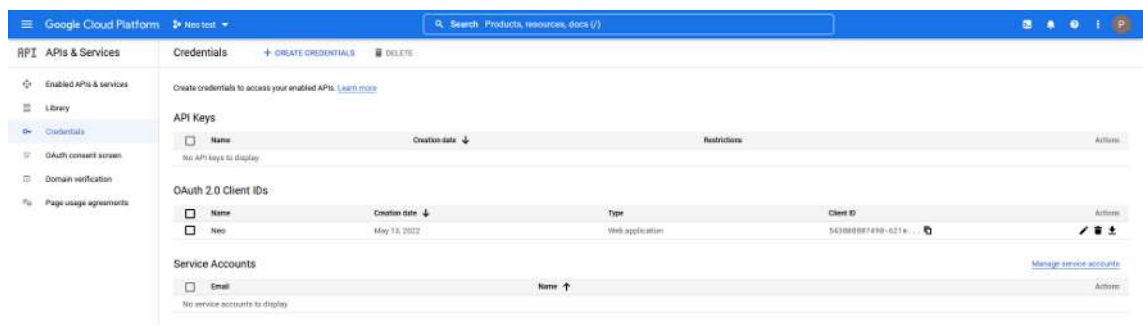


Fig. 51: Credentials

4. Click on the button *+ CREATE CREDENTIALS*.

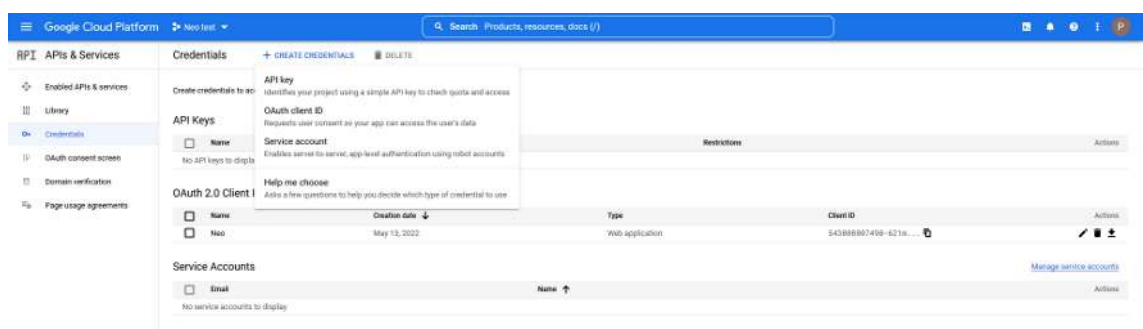


Fig. 52: Create credentials

5. Select the menu item *OAuth client ID*.

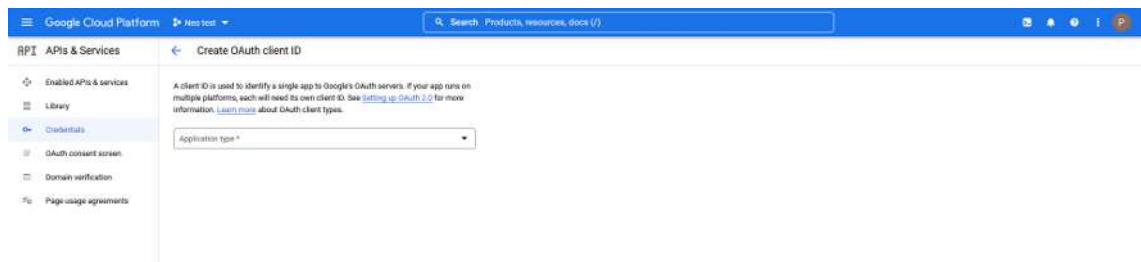


Fig. 53: OAuth client ID

6. Select the application type.

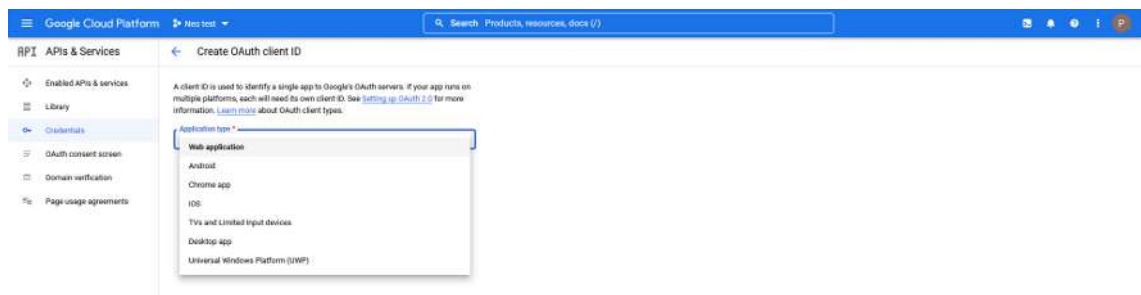


Fig. 54: Select application type

7. In this case *Web application*.

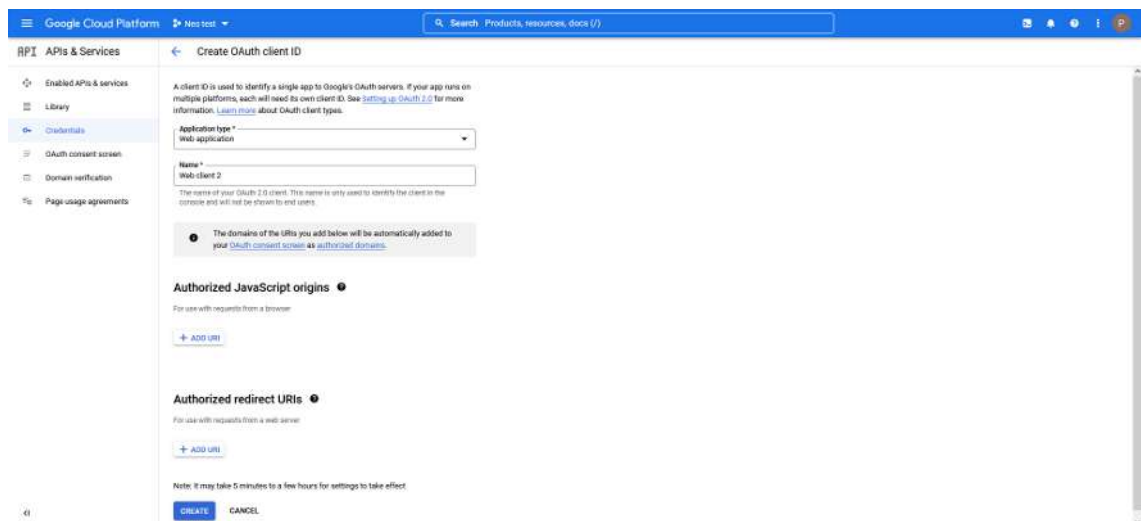
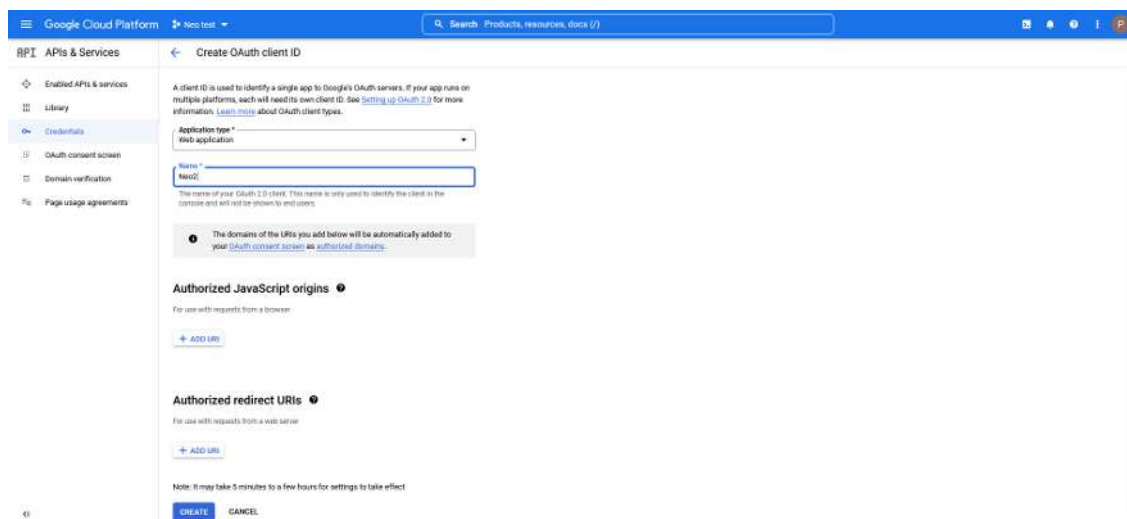


Fig. 55: Application type Web application

8. Enter the name.



Google Cloud Platform

APIs & Services

Create OAuth client ID

Application type: Web application

Name: Neo2

The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized JavaScript origins

Authorized redirect URIs

Note: It may take 5 minutes to a few hours for settings to take effect.

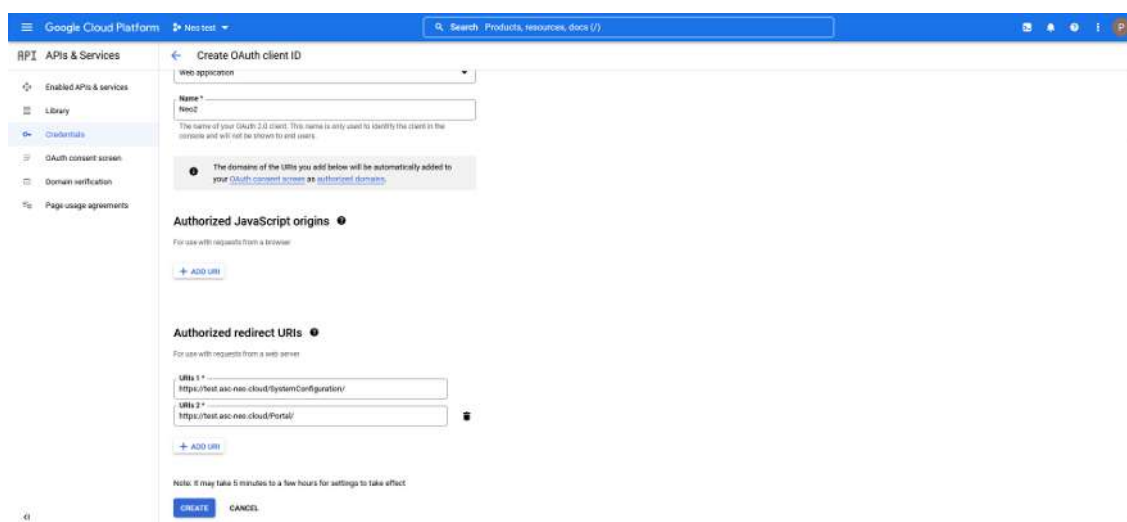
CREATE CANCEL

Fig. 56: Enter name

- Under *Authorized redirect URIs*, enter the URIs of **all** web applications which are supposed to support the OAuth login.



The URI must finish in a "/".



Google Cloud Platform

APIs & Services

Create OAuth client ID

Application type: Web application

Name: Neo2

The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized JavaScript origins

Authorized redirect URIs

URI 1: https://test.asc-mac.cloud/systemConfigurations/

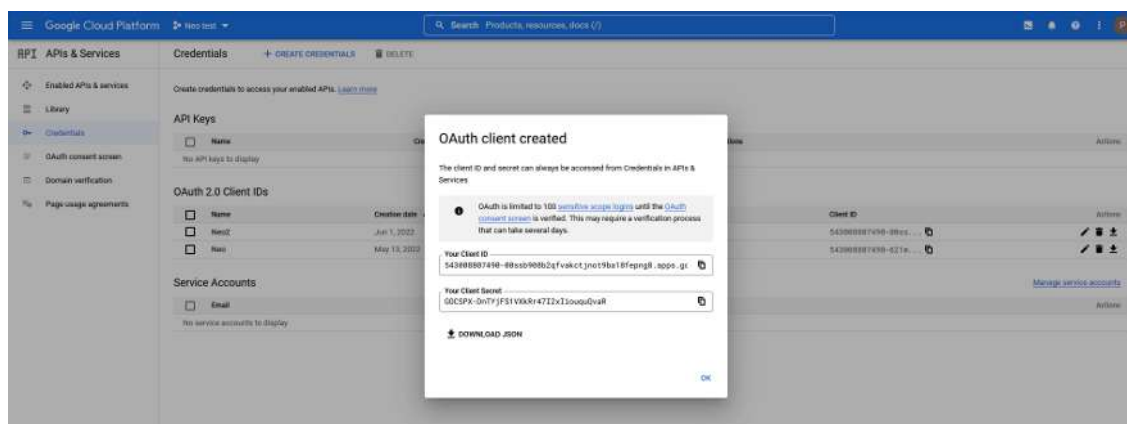
URI 2: https://test.asc-mac.cloud/Portal/

Note: It may take 5 minutes to a few hours for settings to take effect.

CREATE CANCEL

Fig. 57: Enter URI

- Save the entries.
- Copy your created credentials or download them as JSON file.



Google Cloud Platform

APIs & Services

Credentials

CREATE CREDENTIALS DELETE

API Keys

OAuth 2.0 Client IDs

Service Accounts

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth is limited to 100 [lifetime access tokens](#) until the [OAuth consent screen](#) is verified. This may require a verification process that can take several days.

Your Client ID: 543988887498-8950990b2f70kctjnc19ba18fcpng8.apps.googleusercontent.com

Your Client Secret: GDCSPX-0n7rJf51V0kR147IZx13oouq2vull

DOWNLOAD JSON

Fig. 58: OAuth client created

12. Enter the information in the window *Edit OAuth Provider Settings*, see [chapter "Edit OAuth provider settings Google"](#), p. 49.

### Edit OAuth provider settings Mitel

Edit OAuth Vendor Settings
✕

**General**

---

OAuth Settings Name\*

OAuth vendor

MITEL ▼

OAuth Flow Type

PROVIDED\_CODE ▼

**URLs**

---

Token URL

https://authentication.api.mitel.io/20

**Settings**

---

OAuth Client ID\*

Redirect URL\*

Request scope\*

gauth

User name field\*

login

OK

Cancel

Fig. 59: Edit OAuth provider settings (example Mitel)

<i>OAuth Settings Name</i>	Enter the name here under which you have published the application in Mitel.
<i>OAuth provider</i>	Select the OAuth provider, here: MITEL.
<i>OAuth Flow Type</i>	The OAuth Flow Type has been preselected and cannot be changed.
<i>Token URL</i>	The token URL has been preselected and cannot be changed.
<i>OAuth Client ID</i>	Enter the OAuth Client ID of Mitel (e. g. ef0129223a2e3bf76e7c3d8422b15b).
<i>Redirect URL</i>	Enter the Neo <a href="#">URL</a> (e. g. https://serveraddress/).
<i>Request scope</i>	The request scope has been preselected and cannot be changed.
<i>User name field</i>	The user name field has been preselected and cannot be changed.


- Click on the button *OK* to save the entries.  
Click on the button *Cancel* to discard the entries.

#### 4.2.9.5 Group field Miscellaneous Settings

**Miscellaneous Settings** ▼

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

Fig. 60: Configure miscellaneous settings

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

#### 4.2.9.6 Group field Terms of Use

**Terms of Use** ▼

Terms of use  
(max. 4000 characters)

Fig. 61: 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](#)).

 **SYSTEM PROVIDER**  
Letzte Anmeldung 18.02.2019 09:04:52

System ✕

< Passwörter
Allgemeine Einstellungen\*
LDAP-Verbindungsdaten\*
Web S >

Serveradresse	Port
192.168.170.173	389

Hinzufügen
Bearbeiten
Löschen

Speichern

Zurücksetzen

Fig. 62: Tenants module - tab LDAP Authentication

<b>Add</b>	Opens a window in which you can add a new <a href="#">LDAP</a> connection (see <a href="#">chapter "Edit LDAP connection data", p. 56</a> ).
<b>Edit</b>	Opens the selected entry for editing (see <a href="#">chapter "Edit LDAP connection data", p. 56</a> ).
<b>Delete</b>	Deletes the selected entry from the list.

## 4.2.10.1 Edit LDAP connection data

Server address	Port
159.159.159.159	46611
123.123.123.123	4711

Add Edit Delete

Fig. 63: LDAP Connection Data

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

Edit Connection Data

Server address\*

123.123.123.123

Port\*

4711

Use SSL

☐

User DN

CN=Johnson Jim:OU=

Password

•••••

Check LDAP Connection

OK

Cancel

Fig. 64: Edit LDAP connection data (example)

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

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

## 4.2.11 Tab Web Service

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

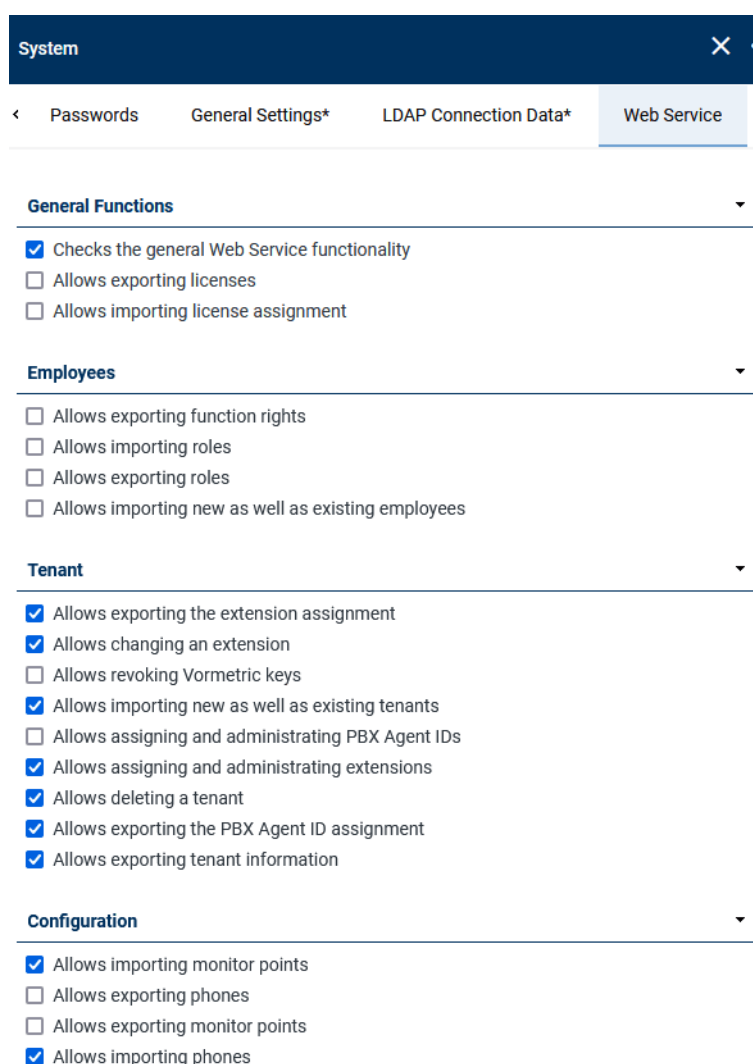


In this tab, you can select which of the functionalities that are generally provided for Web Service are allowed to be used in your recording system. The respective functionalities are released for each tenant individually. Which functionalities are generally available and displayed in the tab depends 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*.



**System** [Close] [Menu]

< Passwords General Settings\* LDAP Connection Data\* **Web Service**

**General Functions** [Expand]

- ☒ Checks the general Web Service functionality
- ☐ Allows exporting licenses
- ☐ Allows importing license assignment

**Employees** [Expand]

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

**Tenant** [Expand]

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

**Configuration** [Expand]

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

Fig. 65: 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.

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

<i>Allows exporting licenses</i>	Activate the check box if you would like to allow exporting licenses.
<i>Allows importing license assignment</i>	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.

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

<i>Allows exporting the extension assignment</i>	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
<i>Allows changing an extension</i>	Activate the check box if you would like to allow the tenant to change an extension via the Web Service.
<i>Allows revoking Vormetric keys</i>	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
<i>Allows importing new as well as existing tenants</i>	Activate the check box if you would like to be able to add tenants and overwrite the data of existing tenants via the Web Service.
<i>Allows assigning and administrating PBX Agent IDs</i>	Activate the check box if you would like to allow the tenant to assign and administrate Agent PBX IDs via the Web Service.
<i>Allows assigning and administrating extensions</i>	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
<i>Allows deleting a tenant</i>	Activate the check box if you would like to allow the tenant to delete a tenant via the Web Service.
<i>Allows exporting the PBX Agent ID assignment</i>	Activate the check box if you would like to allow the tenant to export the PBX Agent ID assignment via the Web Service.
<i>Allows exporting tenant information</i>	<p>Activate the check box if you would like to be able to export tenant information via the Web Service.</p> <p>Tenant information are e. g. tenant name, the used default language, employee ID, first name, last name or the e-mail address.</p>

### Group field Configuration

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

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

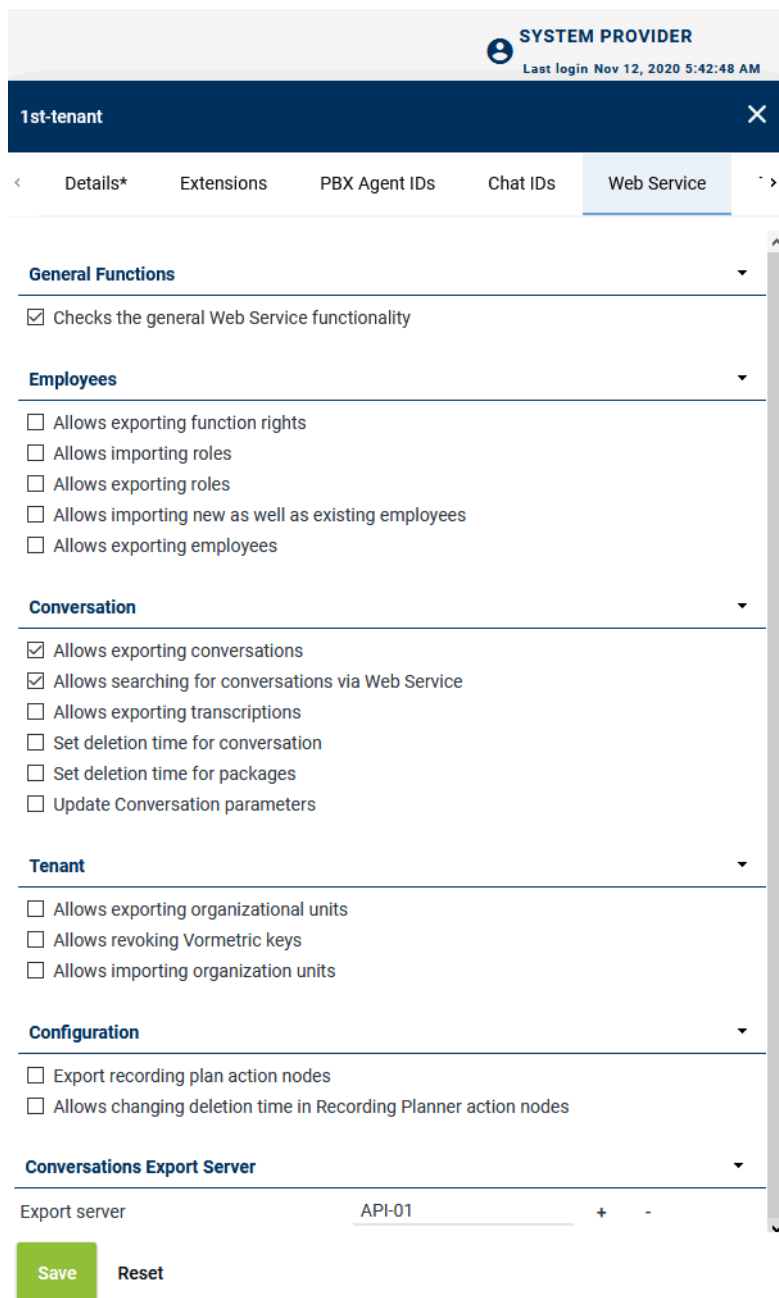
*Allows exporting monitor points*

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*.



The screenshot shows the 'Web Service' configuration page for a tenant named '1st-tenant'. The page is part of the 'SYSTEM PROVIDER' interface, with a last login timestamp of 'Nov 12, 2020 5:42:48 AM'. The 'Web Service' tab is selected among other tabs like 'Details\*', 'Extensions', 'PBX Agent IDs', and 'Chat IDs'. The configuration is organized into several sections, each with a dropdown arrow:

- General Functions:**
  - ☒ Checks the general Web Service functionality
- Employees:**
  - ☐ Allows exporting function rights
  - ☐ Allows importing roles
  - ☐ Allows exporting roles
  - ☐ Allows importing new as well as existing employees
  - ☐ Allows exporting employees
- Conversation:**
  - ☒ Allows exporting conversations
  - ☒ Allows searching for conversations via Web Service
  - ☐ Allows exporting transcriptions
  - ☐ Set deletion time for conversation
  - ☐ Set deletion time for packages
  - ☐ Update Conversation parameters
- Tenant:**
  - ☐ Allows exporting organizational units
  - ☐ Allows revoking Vormetric keys
  - ☐ Allows importing organization units
- Configuration:**
  - ☐ Export recording plan action nodes
  - ☐ Allows changing deletion time in Recording Planner action nodes
- Conversations Export Server:**
  - Export server: API-01

At the bottom, there are two buttons: 'Save' (green) and 'Reset'.

Fig. 66: 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.

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

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

### Group field Conversation

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

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

### Group field Tenant

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


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

### Group field Configuration

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

### 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*.

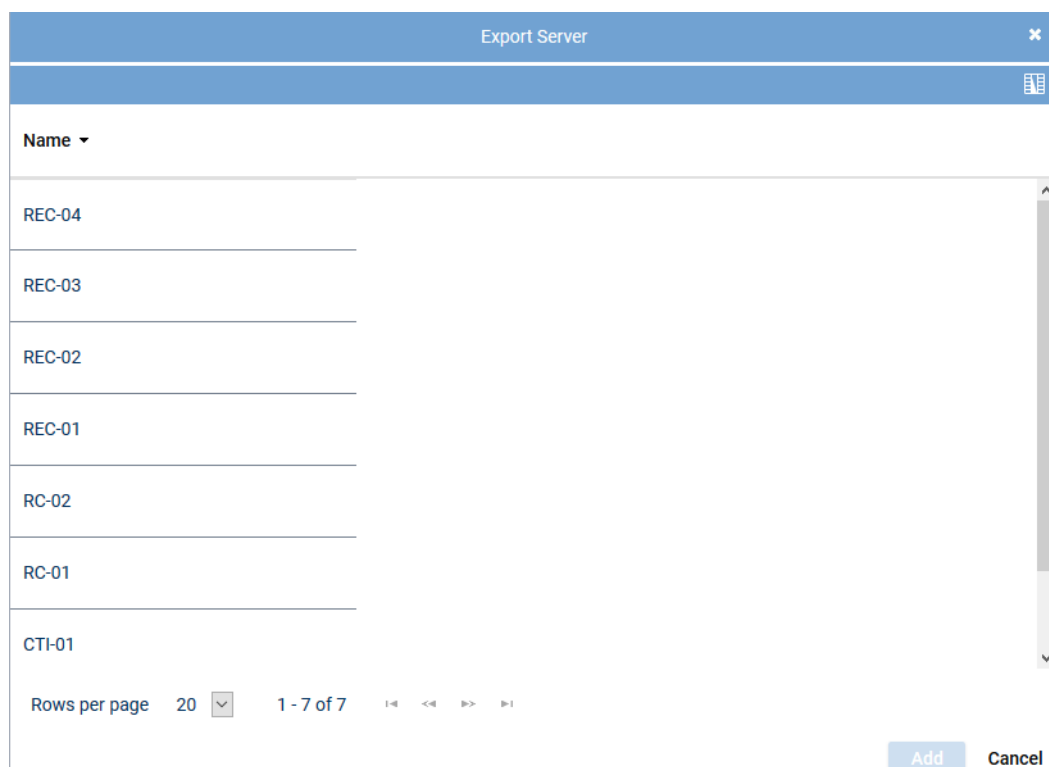


Fig. 67: Select export server

**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. 68: Assign server

2. Select the appropriate server from the list.

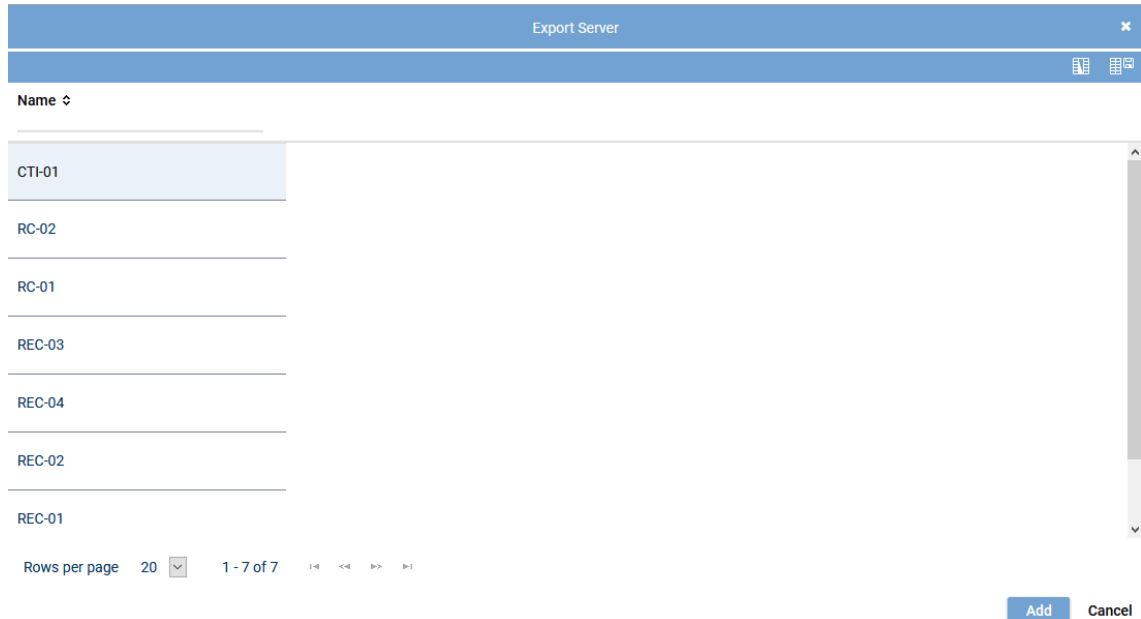


Fig. 69: Select server (example)

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.

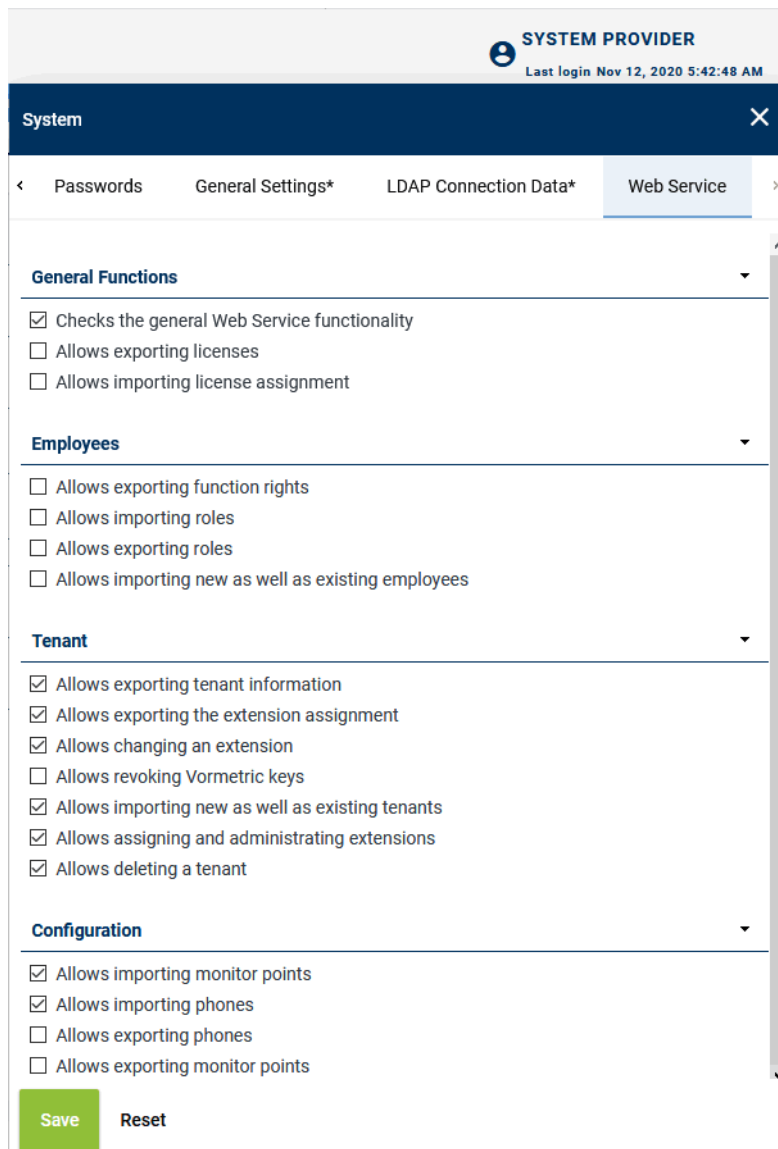
#### Return value

- 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*.



**SYSTEM PROVIDER**  
Last login Nov 12, 2020 5:42:48 AM

**System** [X]

← Passwords General Settings\* LDAP Connection Data\* **Web Service** →

**General Functions**

- ☒ Checks the general Web Service functionality
- ☐ Allows exporting licenses
- ☐ Allows importing license assignment

**Employees**

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

**Tenant**

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

**Configuration**

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

**Save** **Reset**

Fig. 70: 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.

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

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



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

### Group field Tenant

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

<i>Allows exporting tenant information</i>	Activate the check box if you would like to be able to export tenant information via the Web Service.  Tenant information are e. g. tenant name, the used default language, employee ID, first name, last name or the e-mail address.
<i>Allows exporting the extension assignment</i>	Activate the check box if you would like to be able to export the extensions assigned to a tenant via the Web Service.
<i>Allows assigning and administering extensions</i>	Activate the check box if you would like to be able to assign extensions to the tenants via the Web Service.
<i>Allows deleting a tenant</i>	Activate the check box if you would like to be able to delete the tenant via the Web Service.
<i>Allows changing an extension</i>	Activate the check box if you would like to be able to change the extension via the Web Service.
<i>Allows revoking Vormetric keys</i>	Activate the check box if you would like to allow the tenant to revoke Vormetric keys via the Web Service.
<i>Allows importing new as well as existing tenants</i>	Activate the check box if you would like to be able to add tenants and overwrite the data of existing tenants via the Web Service.

### Group field Configuration

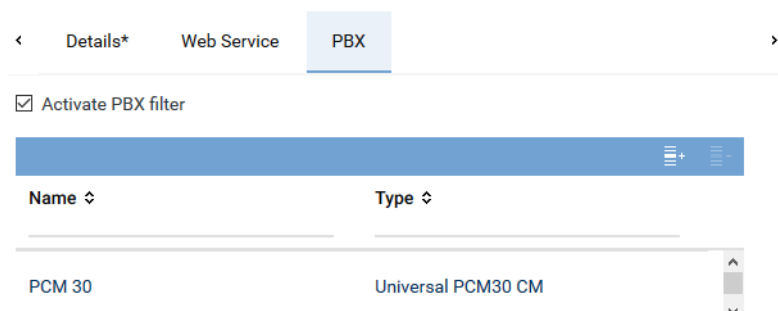
In this group field, you can configure the functions for the configuration of the tenants.

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

#### 4.2.12

### Tab PBX

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



Name	Type
PCM 30	Universal PCM30 CM

Fig. 71: 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. 65](#).
- To remove the assignment of a PBX to a reseller, proceed as described in [chapter "Remove PBX assignment", p. 65](#).

**4.2.12.1 Assign PBX**

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

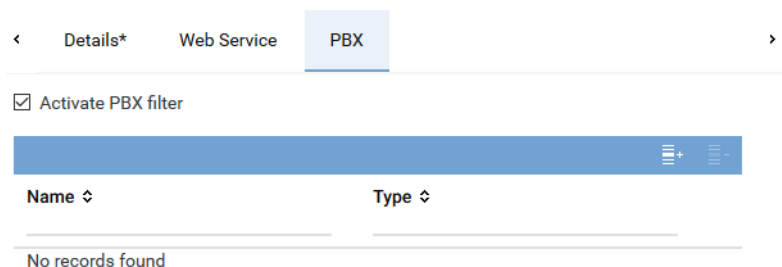


Fig. 72: Assign PBX

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.

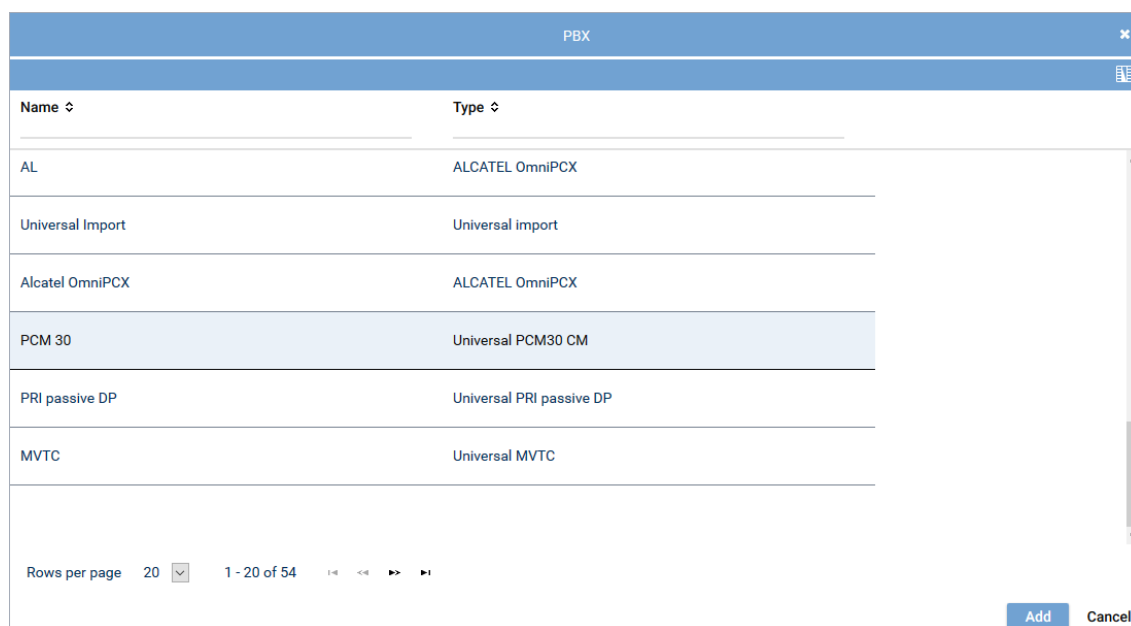


Fig. 73: Add PBX

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.

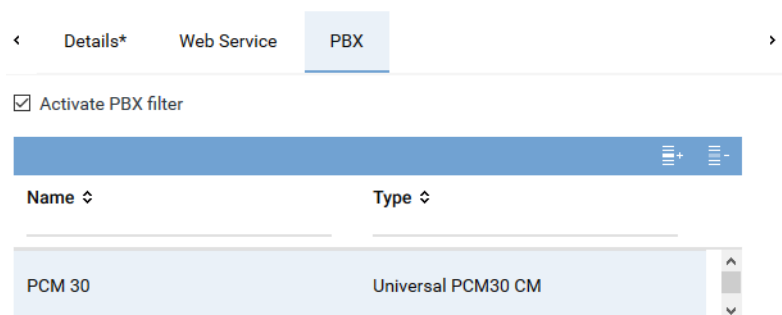


Fig. 74: Remove PBX assignment

- 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.

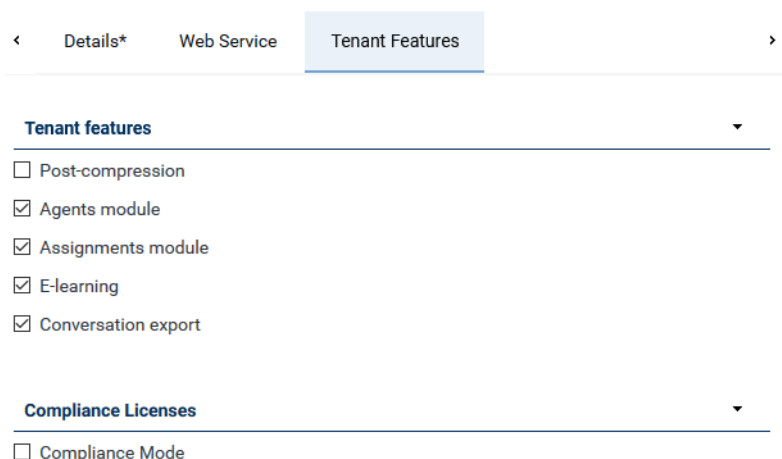


Fig. 75: Tab Tenant Features

#### 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  $\mu$ -law).

	<p><b>NOTICE!</b> 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.</p> <p><b>NOTICE!</b> 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.</p> <p><b>NOTICE!</b> Recordings are compressed from the moment on that post-compression is activated. Recordings which have already been transferred to the storage expansion are <b>not</b> compressed retroactively.</p> <p><b>NOTICE!</b> The drives must be configured for post-compression. For further information refer to the administration manual <i>System Configuration - Configuration drives</i>. Post-compression applies for all drives for which post-compression has been activated.</p>
<i>Agents module</i>	<p>Select whether the Agents module is supposed to be activated.</p> <p><input checked="" type="checkbox"/> = Agents module has been activated.</p> <p><input type="checkbox"/> = Agents module has not been activated.</p>
<i>Assignments module</i>	<p>Select whether the Assignments module is supposed to be activated.</p> <p><input checked="" type="checkbox"/> = Assignments module has been activated.</p> <p><input type="checkbox"/> = Assignments module has not been activated.</p>
<i>E-learning</i>	<p>Select whether the E-Learning module is supposed to be activated.</p> <p><input checked="" type="checkbox"/> = E-Learning module has been activated.</p> <p><input type="checkbox"/> = E-Learning module has not been activated.</p>
<i>Conversation export</i>	<p>Select whether the export of conversations is supposed to be activated.</p> <p><input checked="" type="checkbox"/> = Export of conversations has been activated.</p> <p><input type="checkbox"/> = Export of conversations has not been activated.</p>

### Group field Compliance Licenses



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

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

## 4.3

### Create new tenants manually

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

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

Fig. 76: Tenants module - main view (example)

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

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

- In the detail view, make all necessary settings within the tabs.  
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button **Save** to save the settings.  
To discard the entries, click on the button **Reset**.

1st-tenant

<

Details\*

Extensions

PBX Agent IDs

Chat IDs

Web Service

>

Help

Tenant name\*

1st-tenant

Customer ID

Style

ASC (blue)

Default language

Englisch (US)

Employee number

200000

First name\*

1st-Tenant

Last name\*

Admin

E-mail

Login\*

1st-Tenant-Admin

Password\*

.....

Confirm password\*

.....

Lock account

☐

Time zone

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

System Availability (via Browser)

Address

Contact Person

Save

Reset

Fig. 77: Save tenant

#### 4.4

#### Edit tenants manually

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

1st-tenant
✕

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

[? Help](#)

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

System Availability (via Browser) ▶

Address ▶

Contact Person ▶


Save

Reset

Fig. 78: Save changes

## 4.5

### Delete tenant

- 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.
- Click on the icon  (Delete) in the toolbar.
- To really delete the selected tenant, confirm the security prompt.

## 5 Employees module

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

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

You have the possibility to assign a user role rights which can be defined in the Roles module. In addition or optionally, you can assign the user individual function rights.



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



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



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

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

### 5.1 Main view

All saved employees are displayed in the main view.

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

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

Fig. 79: 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.

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

## 5.1.1

## Toolbar

The toolbar offers the following functions.

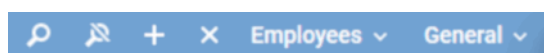







Fig. 80: Employees module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see <a href="#">chapter "Search", p. 74</a> .  The icon  (Search) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new employee (see <a href="#">chapter "Create new employee", p. 88</a> ).
	<i>Delete</i>	Deletes the selected employee (see <a href="#">chapter "Delete employee", p. 89</a> ).
<i>Employees</i>	<i>Summary</i>	Lists all function rights of the selected employee (see <a href="#">chapter "Show summary", p. 73</a> ).
	<i>Show Locked Employees/Show All Employees</i>	Lists only the locked employees in the main view (see <a href="#">chapter "Show locked employees", p. 73</a> ).
	<i>Make Employee Visible or Not Visible</i>	Function which makes the selected employee visible or not visible for others (see <a href="#">chapter "Make employee visible or not visible", p. 74</a> ).
	<i>Export User Data</i>	Exports the user data of the employee of the current tenant in XML format.
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> </ul>



	<ul style="list-style-type: none"> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



For detailed 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.

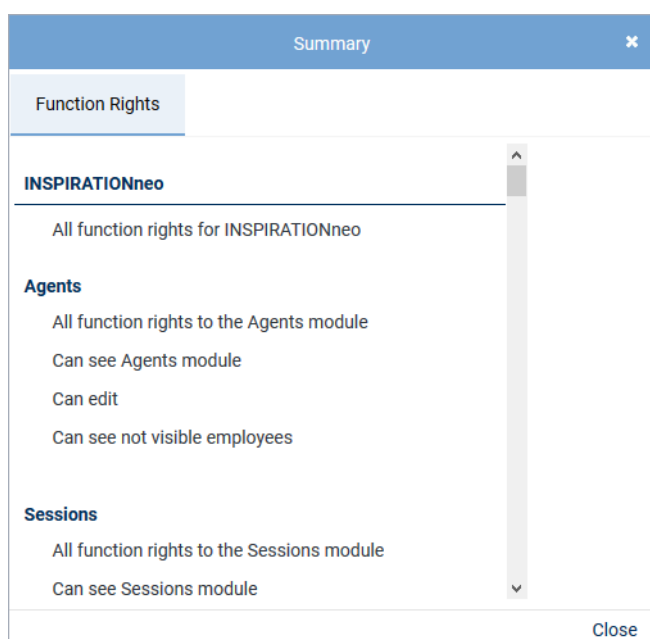




Fig. 81: Summary of the function rights

	Function right has been assigned individually.
	Function right has been assigned via a role. <b>NOTICE!</b> 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. 80](#).

### 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.

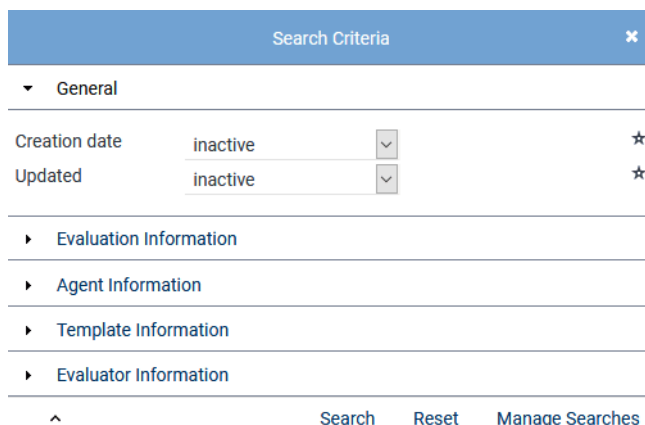





Fig. 82: Window Search Criteria (example)

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.

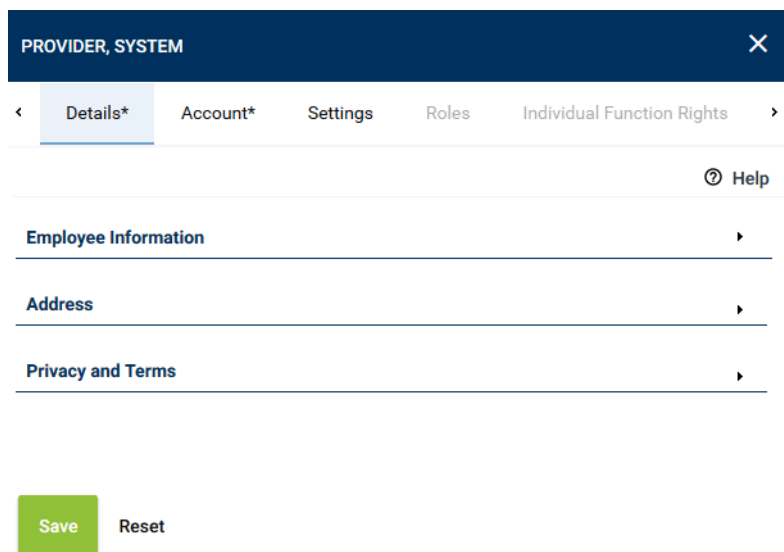


Fig. 83: Employees module - detail view

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. 75](#).
- *Account*  
Here, you can display and edit the employee's login data.  
See [chapter "Tab Account", p. 80](#).
- *Settings*  
Here, you can display and edit the employee's rights and logging settings.  
See [chapter "Tab Settings", p. 83](#).
- *Roles*  
Here, you can display the roles which have been assigned to the employee and edit the role assignment.  
See [chapter "Tab Roles", p. 85](#).
- *Individual Function Rights*  
Here, you can display and assign the employee's individual function rights.  
See [chapter "Tab Individual Function Rights", p. 86](#).

### 5.2.1 Tab Details

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

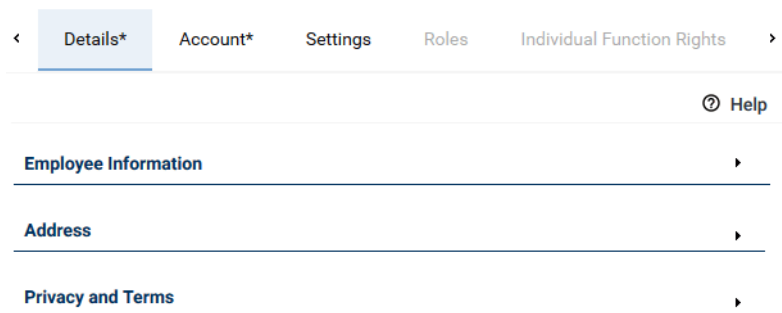



Fig. 84: Employees module - tab Details



Entering an address is optional.



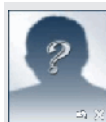
Upon opening a group field for optional information, you have to complete the mandatory fields in this group field to be able to save the changes. If you do not want to enter the optional information, you have to close the group field by clicking on the icon  in the respective title bar.

### 5.2.1.1 Group field Employee Information

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



Fig. 85: Edit employee information





Placeholder for the employee's photo.

See [chapter "Upload or delete image", p. 78](#).

<i>Employee number</i>	ID of the employee.
<i>First name</i>	First name of the employee.
<i>Last name</i>	Last name of the employee.
<i>Date of birth</i>	Date of birth of the employee. You can enter the date directly via the keyboard or via the icon.
<i>E-mail</i>	E-mail address of the employee.
<i>Date of entry</i>	Day on which the employee was hired. You can enter the date directly via the keyboard or via the icon.
<i>Comment</i>	Comment on the employee information.

<i>Address for replay via phone</i>	<p>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:</p> <ul style="list-style-type: none"> <li>• Extension if it has been configured in the PBX for replay via phone.</li> <li>• Complete phone number, e. g. <i>06021 5001 1015</i> if the PBX is connected to the public telephone network.</li> <li>• IP address if it has been configured.</li> <li>• MAC address if it has been configured.</li> <li>• SIP address, e. g. <i>Extension@IP-Address</i>.</li> </ul>
<i>Import key</i>	<p>Key to unambiguously identify an employee imported from an external source.</p> <p>When importing the employee information for the first time, the import key is entered here automatically. Upon each new import, this import key is checked to determine whether the employee has already been imported before.</p> <p>In addition, the import key is used when transferring (export/import) recordings from a Neo system to another Neo system to map the recordings to the agents. If the employee does not have an automatically created import key, you can enter an import key manually for this mapping.</p> <p><b>NOTICE!</b> If you change an import key manually, the employee will not be recognized as an already imported employee upon the next import of employee data. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordings.</p>
<i>Extended import key</i>	<p>Extended key to unambiguously identify employees imported from an external source.</p> <p>The extended import key is used whenever the standard import key is not sufficient for an unambiguous identification.</p> <p>An example where the extended import key is used is during the import of calls from the application Recording Insights. Here, the import key alone is not sufficient as the users come from different <a href="#">LDAP</a> systems and several attributes are compiled in an extended import key for unambiguous identification.</p> <p>When the employee's data is imported for the first time, the import key is entered here automatically. With every new import, this import key is checked to determine whether the employee has already been imported.</p> <p>In addition, the import key is used during the export/import of recordings from one Neo system to another Neo system to map the recordings to the agents. If the employee does not have an automatically generated import key, you can enter an import key manually for this purpose.</p> <p><b>NOTICE!</b> If you change an import key manually, the employee will not be recognized as having been imported before already. Furthermore, it will not be possible to map the recordings correctly upon the next import of recordings.</p>
<i>Time zone</i>	<p>Shows the time zone in which the conversations are supposed to be displayed in the replay applications. The settings which have been configured for the respective employee prevail over the default settings in the Tenants module</p>

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.

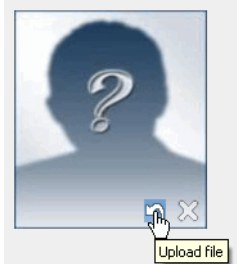


Fig. 86: Upload image

⇒ The window *Upload File* appears.

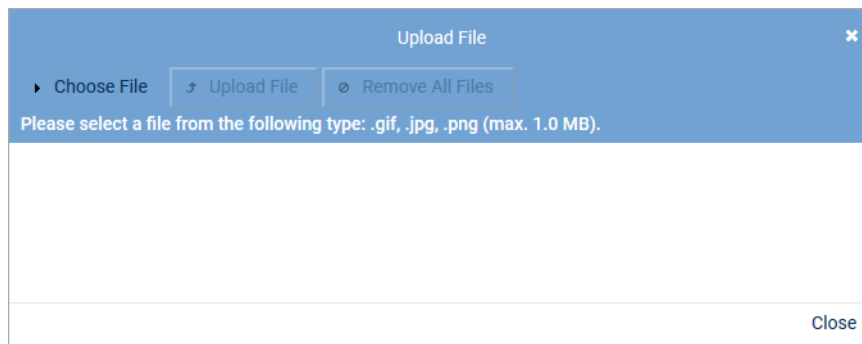



Fig. 87: Upload File

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.

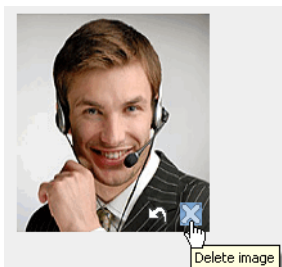


Fig. 88: Delete image (example)

⇒ 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. 89: Add address

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

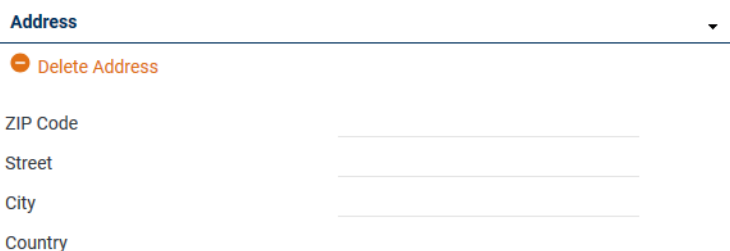



Fig. 90: Add address


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. 91: 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.

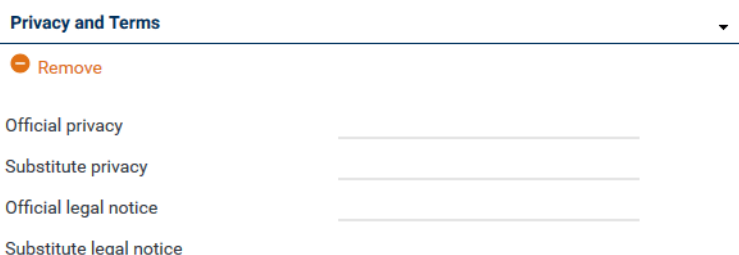



Fig. 92: Add privacy statement and terms

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

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.

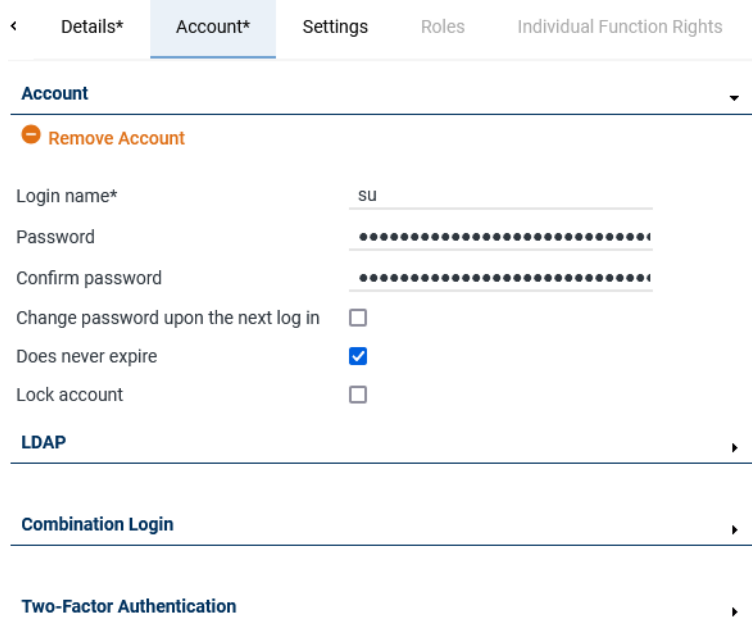


Fig. 93: Employees module - tab Account




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. 94: Add account

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

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



	<b>NOTICE!</b> If you use the function <i>Last Call Repeat</i> , you must use exclusively digits here.
<i>Confirm password</i>	Enter the password of the employee again.
<i>Change password upon the next login</i>	Activate this option if the employee is supposed to change the password upon logging in the next time.
<i>Does never expire</i>	Activate this option if the password is never supposed to expire.
<i>Lock account</i>	This option allows locking the employee's account. In the main view, you can filter for this criterion, see <a href="#">chapter "Show locked employees"</a> , p. 73.

- If you would like to remove the account, click on the button  *Remove account* in the title bar of the group field.
- To activate the authentication via [LDAP](#) for the employee, see [chapter "Authentication via LDAP"](#), p. 81.
- To assign the employee a combination user, see [chapter "Assign combination user"](#), p. 81.
- To activate two-factor authentication for the employee, see [chapter "Two-factor authentication"](#), p. 82.

#### 5.2.2.1 Authentication via LDAP

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



Fig. 95: Activate authentication via LDAP

- Enter the complete Distinguished Name (DN) of the user in the field *LDAP DN*.
- If you would like to deactivate the authentication via LDAP again, deactivate the check box *LDAP authentication*.  
☒ = Authentication via [LDAP](#) has been activated.  
☐ = Authentication via [LDAP](#) has not been activated.


#### 5.2.2.2 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.

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

Combination Login

Last Name ▾ First Name ▾

No records found

Fig. 96: Assign combination user

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

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


Rows per page 20 ▾ 1 - 13 of 13 < << >> >

Add Cancel

Fig. 97: Add combination user

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

### 5.2.2.3 Delete combination user assignment

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

Combination Login

Last Name ▾ First Name ▾

Agent 5.

Fig. 98: Delete combination user assignment

### 5.2.2.4 Two-factor authentication

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

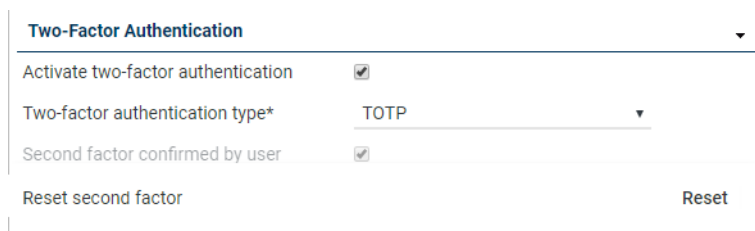


Fig. 99: Activate two-factor authentication

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

### 5.2.3 Tab Settings

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

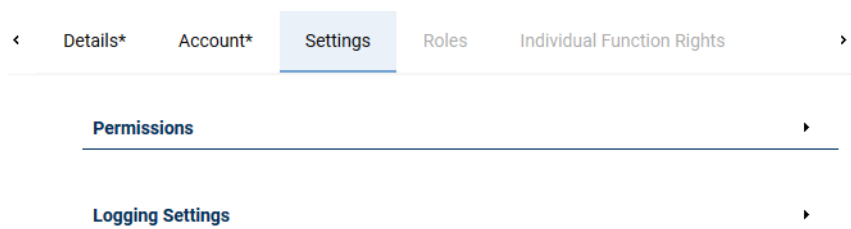


Fig. 100: Employees module - tab Settings

#### 5.2.3.1 Group field Permissions

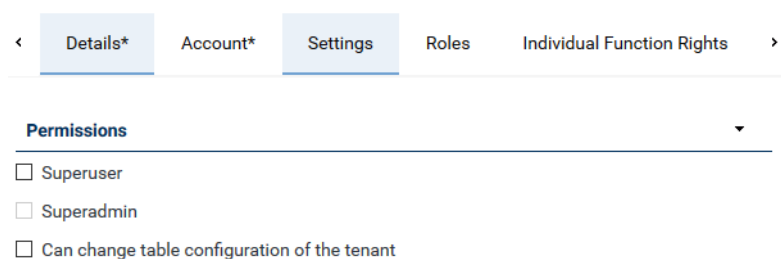


Fig. 101: Configure permissions

<i>Superuser</i>	<p>This right assigns all function rights in the system to the user if their licenses are available.</p> <p><input checked="" type="checkbox"/> = Right has been activated.</p>
------------------	---

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



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

### 5.2.3.2

#### Group field Logging Settings

**Logging Settings** ▼

---

Logging following activities of the user

☐ Access control

☐ Configuration activities

Fig. 102: Configure logging

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

☒ = Logging has been activated.

☐ = Logging has been deactivated.

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

*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.

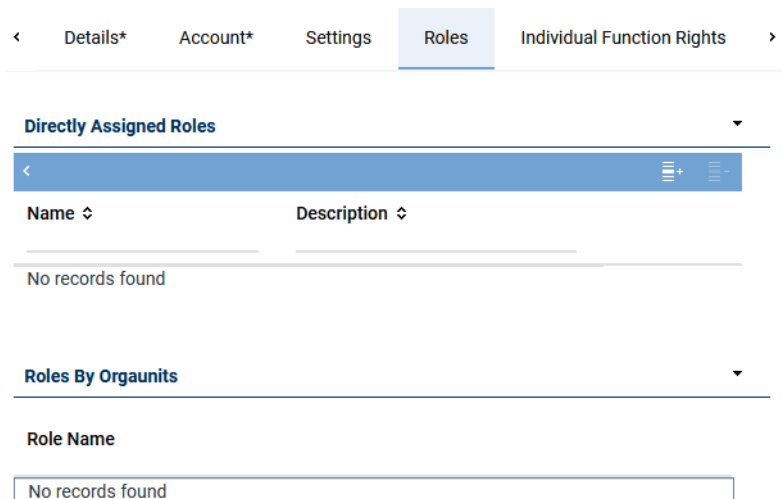


Fig. 103: Employees module - tab Roles

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).

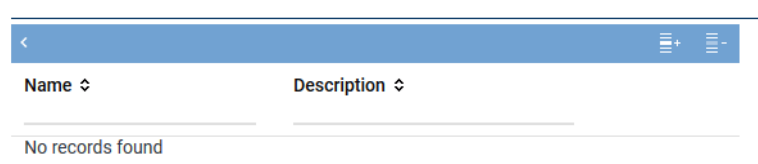
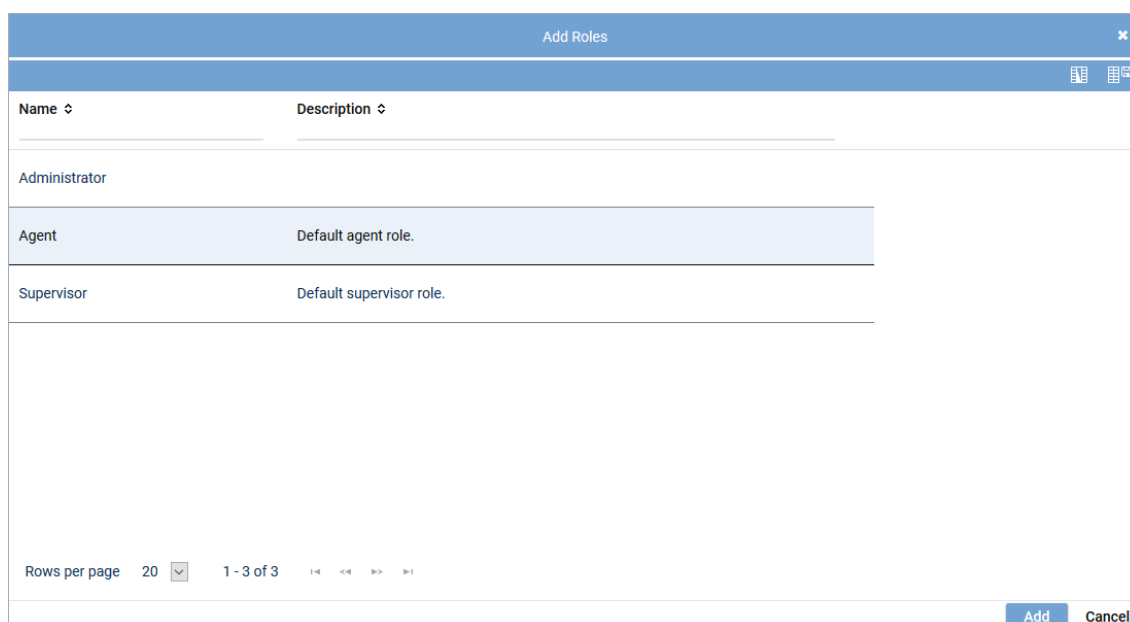


Fig. 104: Assign roles

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



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


Rows per page 20 1 - 3 of 3

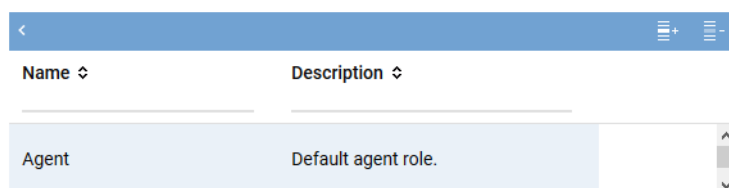
Add Cancel

Fig. 105: Add role

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

#### 5.2.4.2 Delete role assignment

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



Name	Description
Agent	Default agent role.

Remove

Fig. 106: 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.

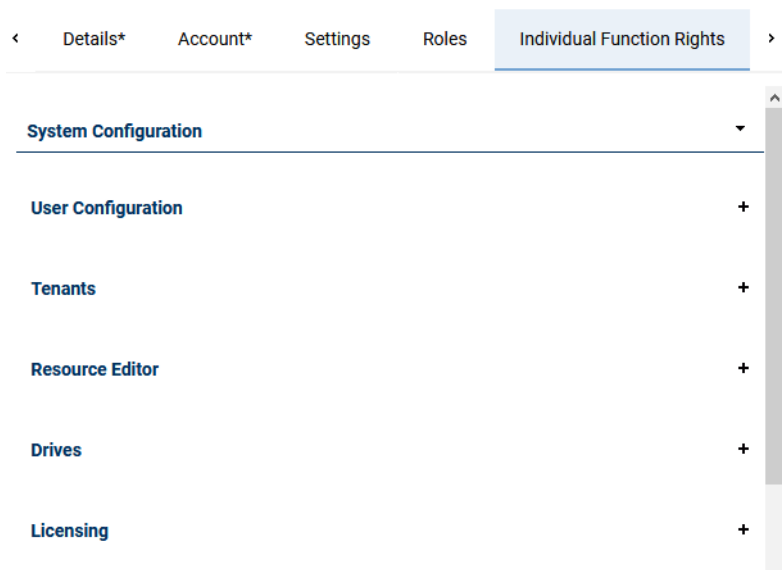


Fig. 107: Employees module - tab Individual Function Rights (example)

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.

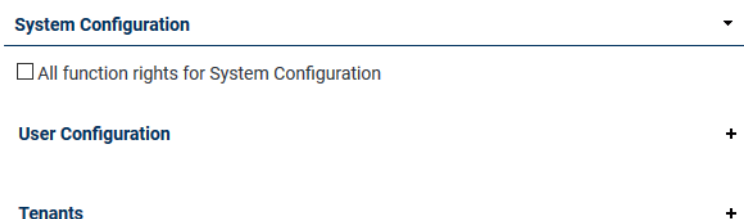


Fig. 108: Function rights - display sections (example)

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.

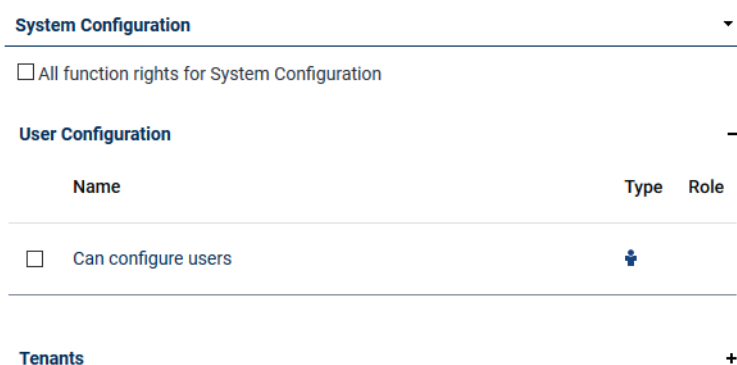





Fig. 109: Function rights - Display function rights


1st column)	Shows whether the function right has been assigned individually. <input checked="" type="checkbox"/> = individual function right <input type="checkbox"/> = no individual function right
<b>Name</b>	Description of the function right.
<b>Type</b>	Shows which license is required for this right.  = agent license  = supervisor license  = basic license (without agent or supervisors rights)
<b>Role</b>	Shows whether the function right has been assigned to the user via a role (role right). no mark = no role right <input checked="" type="checkbox"/> = role right  <b>NOTICE!</b> In the window <i>Summary</i> , you can see via which role the function right has been assigned, see <a href="#">chapter "Show summary", p. 73</a> .

Tab. 3: Function rights

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

### 5.3

#### Create new employee

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

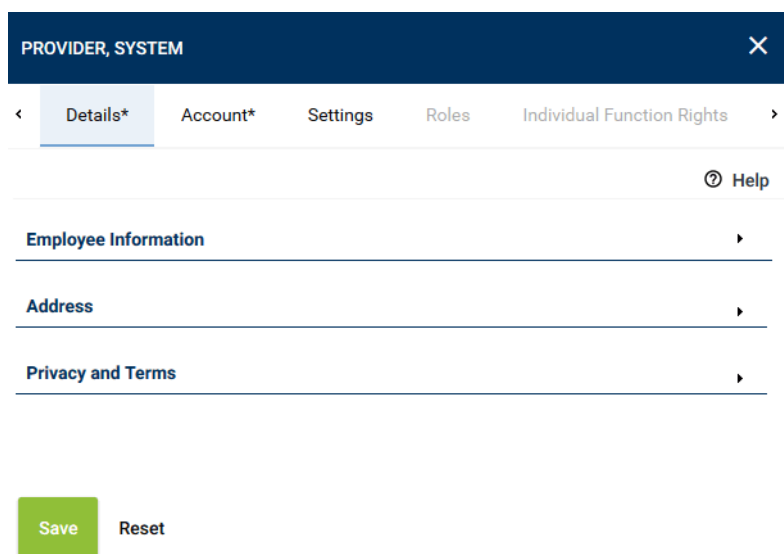


Fig. 110: Save employee

### 5.4

#### Edit employee

- In the main view, select the employee for whom you would like to edit the data.



2. Make all necessary changes in the tabs of the detail view.  
You can change tabs without buffering without risking the loss of your settings.
3. Once you have finished adjusting the settings, click on the button *Save* to save the settings.  
To discard the entries, click on the button *Reset*.

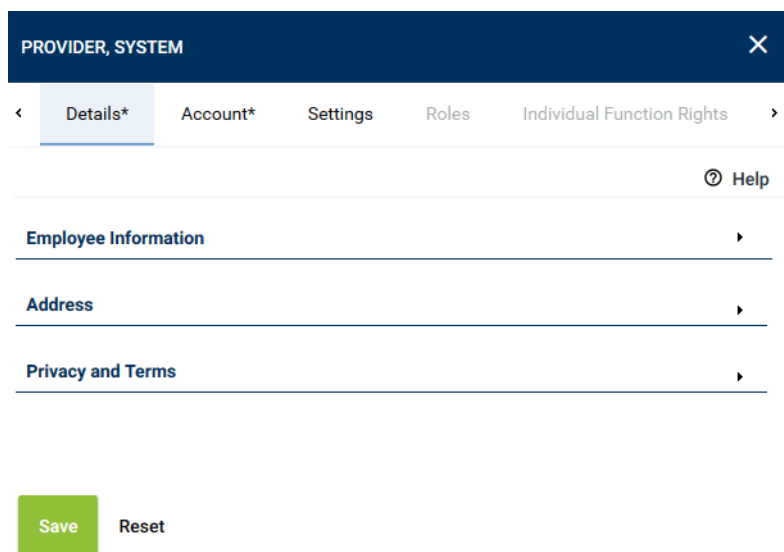



Fig. 111: Save changes

### 5.5 Delete employee

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



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



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

## 6 Roles module

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

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



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



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

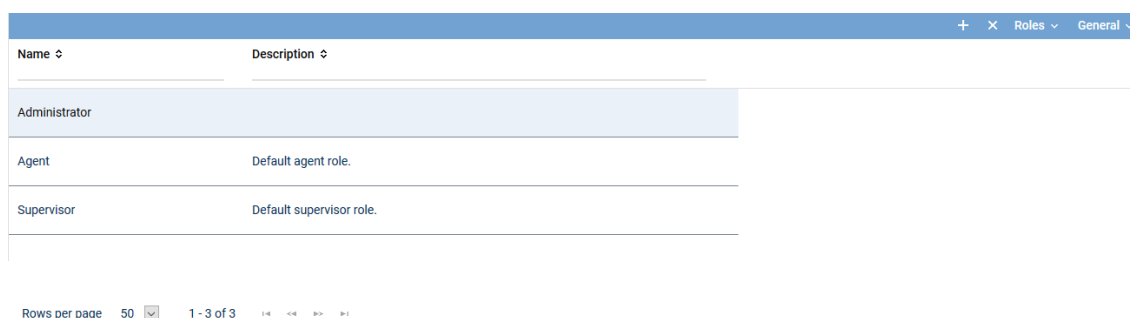


You can import configuration data from existing [LDAP](#) structures, too. The import is configured in the Configuration Import module. For further information refer to the administration manual *Import of configuration data*.

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

### 6.1 Main view

In the main view, all saved roles are displayed.



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

Rows per page 50 1 - 3 of 3

Fig. 112: Roles module - main view

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







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

#### 6.1.1 Toolbar

The toolbar offers the following functions.



Fig. 113: Roles module - toolbar

	<i>Search</i>	Opens the window of the search function. The search function allows searching systematically for sets of data which meet certain criteria, see <a href="#">chapter "Search", p. 74</a> .
		The icon  ( <i>Search</i> ) is displayed whenever the search has been adjusted by means of a filter.
	<i>Reset Search</i>	Resets all manually entered search criteria. The search is started without manual filter settings.
	<i>Create</i>	Creates a new role (see <a href="#">chapter "Create new role", p. 95</a> ).
	<i>Delete</i>	Deletes the selected role (see <a href="#">chapter "Delete role", p. 96</a> ).
<i>Roles</i>	<i>Duplicate with Employees</i>	Creates a copy of the selected role with the assigned employee, see <a href="#">chapter "Duplicate role", p. 95</a> .
	<i>Duplicate Without Employees</i>	Creates a copy of the selected role without the assigned employee, see <a href="#">chapter "Duplicate role", p. 95</a> .
<i>General</i>	<i>Print</i>	Prints the table of the main view.
	<i>Adjust Table</i>	Opens a window in which you can adjust the following settings for the main view: <ul style="list-style-type: none"> <li>• Displayed information</li> <li>• Order of the displayed columns</li> <li>• Number of rows per page</li> </ul>
	<i>General Help</i>	By clicking on the menu item <i>General Help</i> , a description of the application you are currently viewing is opened.
	<i>Module Help</i>	By clicking on the menu item <i>Module Help</i> , a description of the module you are currently viewing is opened.



For detailed 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.

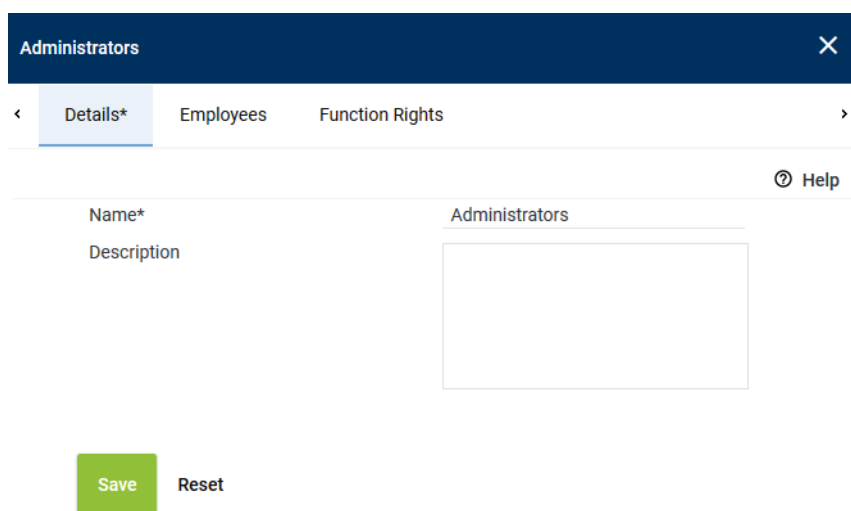


Fig. 114: Roles module - detail view

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. 92](#).

- *Employees*

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

See [chapter "Tab Employees", p. 92](#).

- *Function Rights*

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

See [chapter "Tab Function Rights", p. 93](#)

### 6.2.1 Tab Details

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

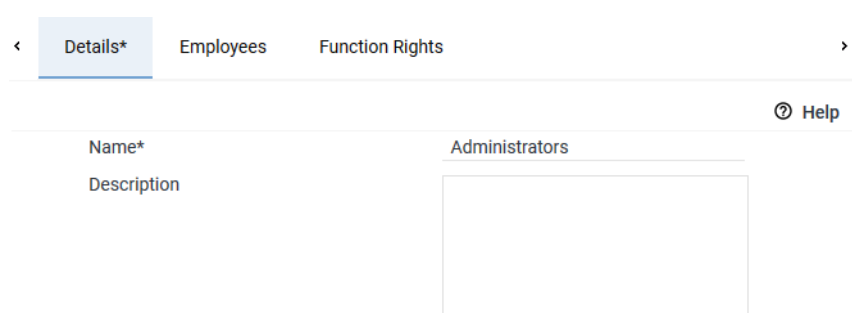


Fig. 115: Roles module - tab Details

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

### 6.2.2 Tab Employees

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

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

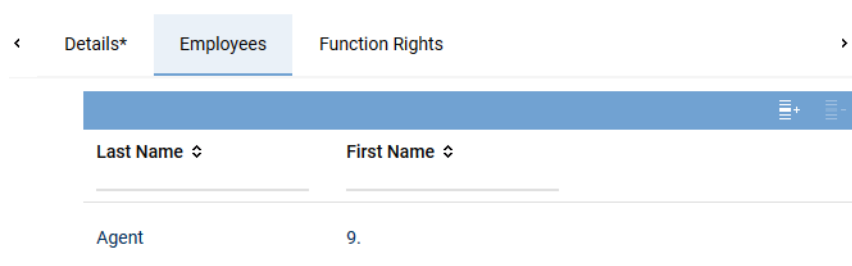


Fig. 116: Roles module - tab Employees



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).

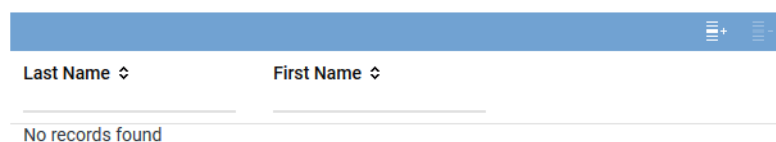
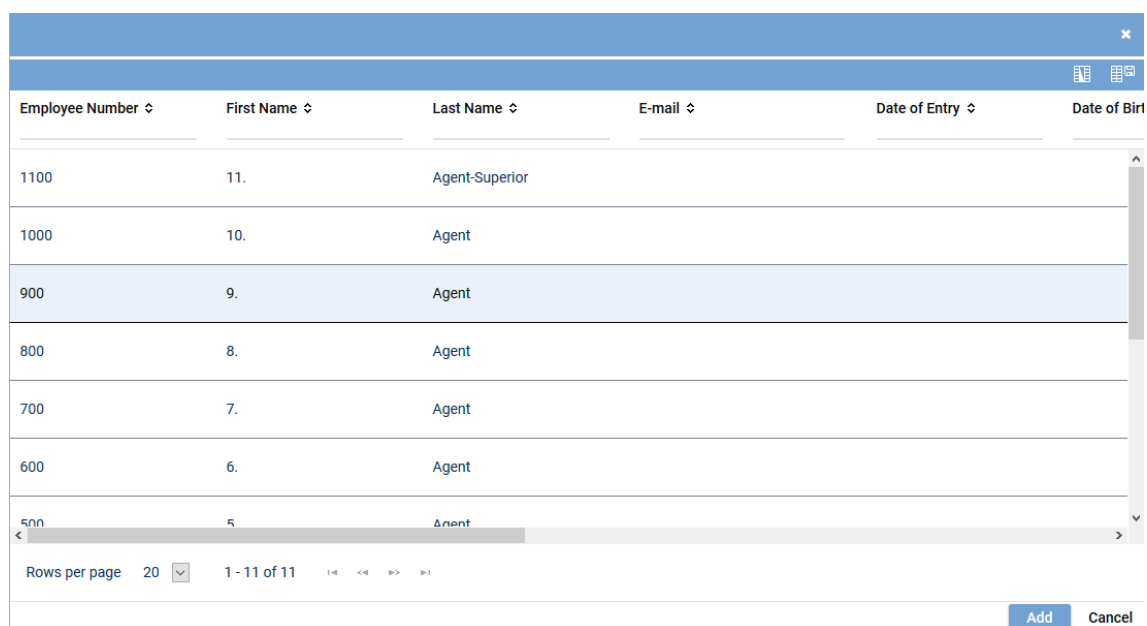


Fig. 117: Assign users

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




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

Fig. 118: 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*).

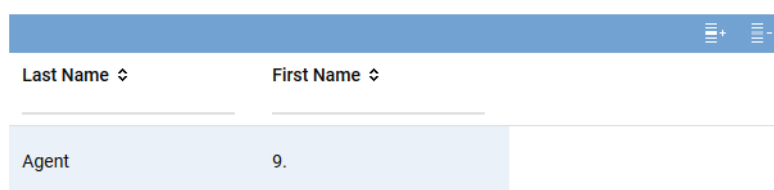


Fig. 119: Delete user assignment

### 6.2.3 Tab Function Rights

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



Fig. 120: Roles module - tab Function Rights (example)

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

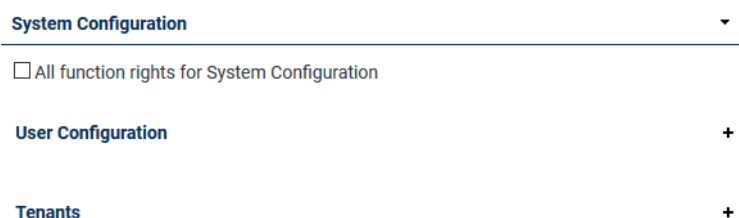


Fig. 121: Function rights - display sections (example)

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



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

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

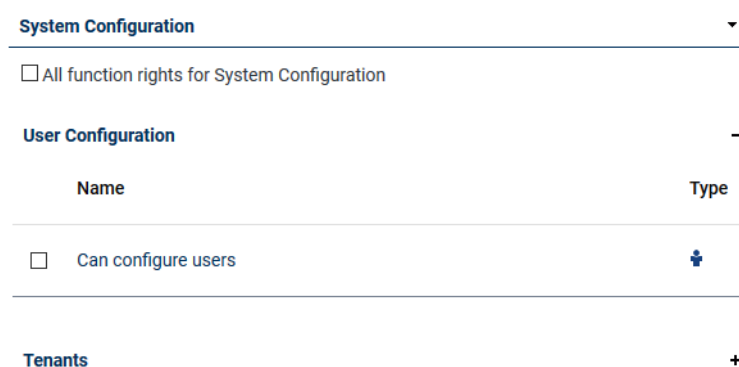





Fig. 122: Function rights - Display function rights

1st column)	Shows whether the function right has been assigned individually. <input checked="" type="checkbox"/> = individual function right <input type="checkbox"/> = no individual function right
Name	Description of the function right.
Type	Shows which license is required for this right.


-  = agent license
-  = supervisor license
-  = basic license (without agent or supervisors rights)

Tab. 4: Function rights

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

### 6.3

#### Create new role

- Click on the icon  (*Create*) in the toolbar.
- Adjust all settings in the tabs of the detail view as described in the respective chapters (see [chapter "Detail view", p. 91](#)).  
You can change tabs without buffering without risking the loss of your settings.
- Once you have finished adjusting the settings, click on the button *Save* to save the settings.  
To discard the entries, click on the button *Reset*.

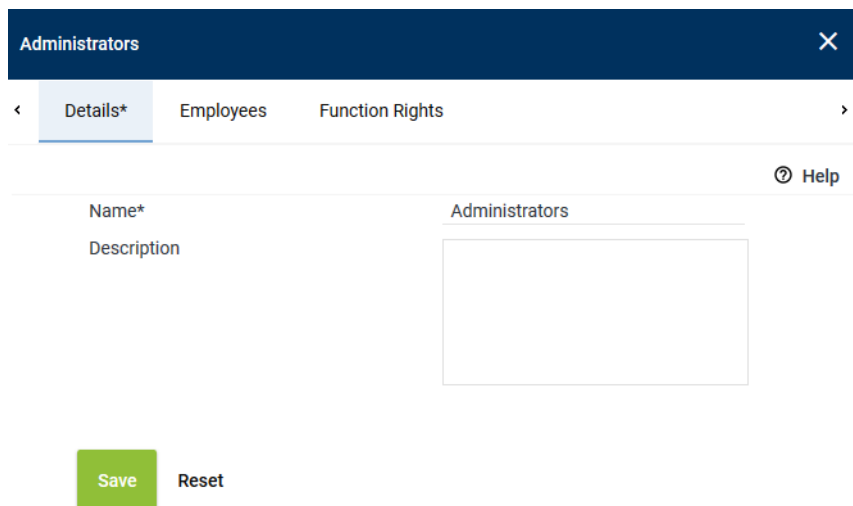


Fig. 123: Save role

### 6.4

#### Duplicate role

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

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

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

6. Adjust all settings in the tabs of the detail view as described in the respective chapters (see [chapter "Detail view", p. 91](#)).  
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**.

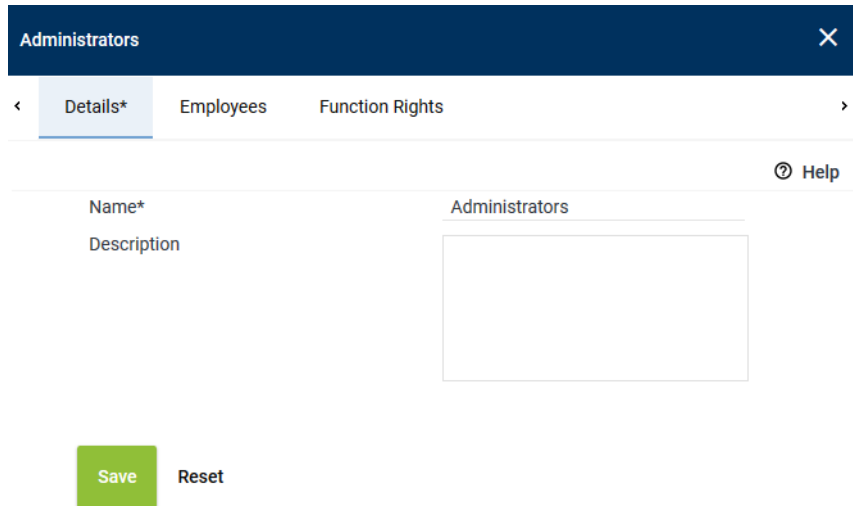


Fig. 124: Save role

## 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. 91](#).  
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**.

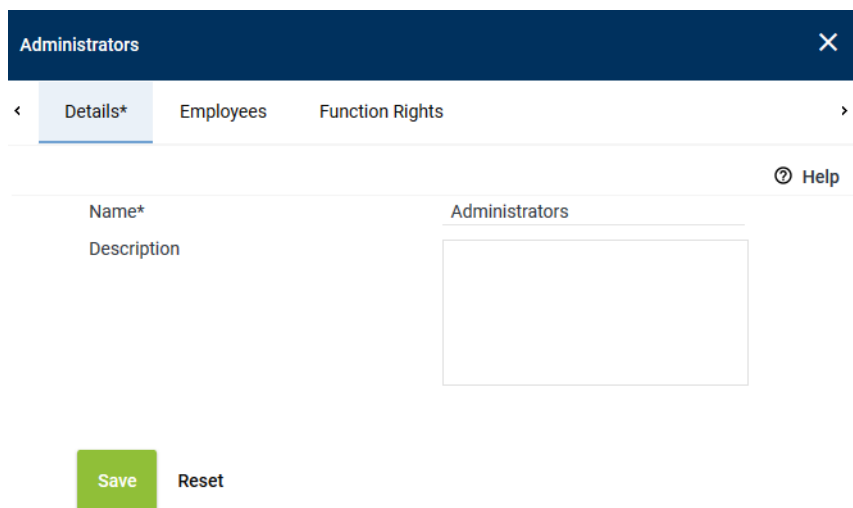



Fig. 125: Save changes

## 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.

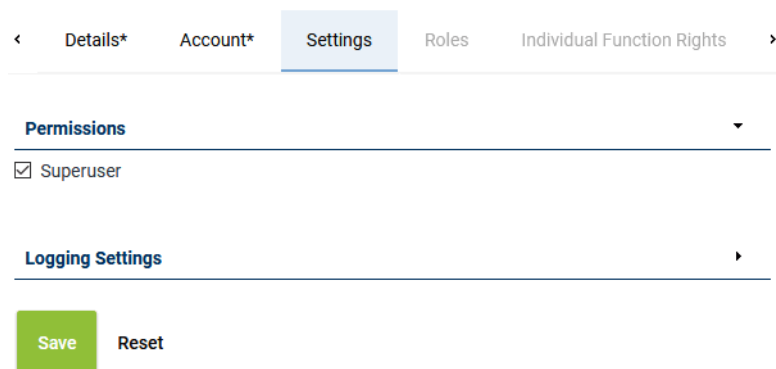
A superadmin has limited superuser function rights in the system.

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*.



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

Permissions: ☒ Superuser

Logging Settings

Buttons: Save, Reset

Fig. 126: Create superuser

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

## 7.2

## Create superadmin

1. Open the Employees module.
2. In the main view, select the user whom you would like to assign superadmin rights.
3. Click on the tab *Settings* in the detail view.
4. Open the group field *Permissions*.
5. Activate the check box in front of *Superuser*.
6. Activate the check box in front of *Superadmin*.  
**NOTICE!** The option *Superadmin* is only displayed if there is the respective license in the system.

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

**Permissions** ▼  
☒ Superuser  
☒ Superadmin

**Logging Settings** ►

Fig. 127: Create superadmin

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

## List of figures

Fig. 1	Tenants module - main view .....	12
Fig. 2	Tenants module - toolbar .....	12
Fig. 3	Tenants module - detail view for the tenant "System" .....	13
Fig. 4	Tenants module - detail view for normal tenants .....	14
Fig. 5	Tenants module - detail view for resellers .....	16
Fig. 6	Tenants module - detail view for normal tenants .....	17
Fig. 7	Add time zone .....	18
Fig. 8	The displayed entries in the table are filtered for ber (example).....	19
Fig. 9	Add time zone .....	19
Fig. 10	System Availability (via Browser).....	19
Fig. 11	System Availability (via Browser).....	20
Fig. 12	Configure system availability .....	20
Fig. 13	Add address.....	21
Fig. 14	Add address.....	21
Fig. 15	Add contact person.....	21
Fig. 16	Add contact person.....	21
Fig. 17	Tenants module - tab Extensions .....	22
Fig. 18	Assign extensions to tenants .....	23
Fig. 19	Remove extensions .....	24
Fig. 20	Select extensions.....	25
Fig. 21	Tenants module - tab PBX Agent ID.....	26
Fig. 22	Assign PBX Agent IDs to tenants .....	26
Fig. 23	Select PBX Agent IDs.....	28
Fig. 24	Tenants module - tab Chat IDs.....	29
Fig. 25	Assign chat IDs to tenants .....	29
Fig. 26	Select chat IDs.....	31
Fig. 27	Tenants module - tab Passwords .....	31
Fig. 28	Define password length .....	32
Fig. 29	Define mandatory characters.....	33
Fig. 30	Configure password security .....	34
Fig. 31	Define forbidden passwords .....	35
Fig. 32	Define advanced password settings .....	36
Fig. 33	Edit entry in the list .....	36
Fig. 34	Tenants module - tab General Settings .....	36
Fig. 35	Configure user activity .....	37
Fig. 36	SMTP account .....	37
Fig. 37	SMTP account .....	38
Fig. 38	Add SMTP account.....	38
Fig. 39	Group field SNMP Agent (examples).....	39
Fig. 40	Configure login settings .....	41
Fig. 41	Edit OAuth provider settings (example Custom).....	44

Fig. 42	Edit OAuth provider settings (example Azure).....	45
Fig. 43	Azure login.....	46
Fig. 44	New registration.....	46
Fig. 45	Register application .....	47
Fig. 46	Application (client) ID / OAuth Client ID .....	47
Fig. 47	Enter URI .....	48
Fig. 48	Enter ID tokens .....	48
Fig. 49	Edit OAuth provider settings (example Google) .....	49
Fig. 50	Google login.....	50
Fig. 51	Credentials.....	50
Fig. 52	Create credentials.....	50
Fig. 53	OAuth client ID.....	51
Fig. 54	Select application type.....	51
Fig. 55	Application type Web application.....	51
Fig. 56	Enter name .....	52
Fig. 57	Enter URI .....	52
Fig. 58	OAuth client created .....	52
Fig. 59	Edit OAuth provider settings (example Mitel) .....	53
Fig. 60	Configure miscellaneous settings.....	54
Fig. 61	Configure terms of use .....	55
Fig. 62	Tenants module - tab LDAP Authentication.....	55
Fig. 63	LDAP Connection Data.....	56
Fig. 64	Edit LDAP connection data (example).....	56
Fig. 65	Web service functionalities for the system provider.....	57
Fig. 66	Web Service functions for the tenant.....	59
Fig. 67	Select export server.....	61
Fig. 68	Assign server .....	62
Fig. 69	Select server (example).....	62
Fig. 70	Web service functionalities for the reseller .....	63
Fig. 71	Tenants module - tab PBX.....	64
Fig. 72	Assign PBX.....	65
Fig. 73	Add PBX .....	65
Fig. 74	Remove PBX assignment.....	66
Fig. 75	Tab Tenant Features .....	66
Fig. 76	Tenants module - main view (example).....	68
Fig. 77	Save tenant.....	69
Fig. 78	Save changes .....	70
Fig. 79	Employees module - main view.....	71
Fig. 80	Employees module - toolbar .....	72
Fig. 81	Summary of the function rights .....	73
Fig. 82	Window Search Criteria (example).....	74
Fig. 83	Employees module - detail view .....	75

Fig. 84	Employees module - tab Details .....	76
Fig. 85	Edit employee information .....	76
Fig. 86	Upload image.....	78
Fig. 87	Upload File.....	78
Fig. 88	Delete image (example).....	78
Fig. 89	Add address.....	79
Fig. 90	Add address.....	79
Fig. 91	Add privacy statement and terms .....	79
Fig. 92	Add privacy statement and terms .....	79
Fig. 93	Employees module - tab Account .....	80
Fig. 94	Add account.....	80
Fig. 95	Activate authentication via LDAP.....	81
Fig. 96	Assign combination user.....	82
Fig. 97	Add combination user.....	82
Fig. 98	Delete combination user assignment.....	82
Fig. 99	Activate two-factor authentication .....	83
Fig. 100	Employees module - tab Settings .....	83
Fig. 101	Configure permissions .....	83
Fig. 102	Configure logging.....	84
Fig. 103	Employees module - tab Roles .....	85
Fig. 104	Assign roles .....	85
Fig. 105	Add role .....	86
Fig. 106	Delete role assignment .....	86
Fig. 107	Employees module - tab Individual Function Rights (example).....	87
Fig. 108	Function rights - display sections (example) .....	87
Fig. 109	Function rights - Display function rights .....	87
Fig. 110	Save employee .....	88
Fig. 111	Save changes.....	89
Fig. 112	Roles module - main view.....	90
Fig. 113	Roles module - toolbar.....	90
Fig. 114	Roles module - detail view .....	91
Fig. 115	Roles module - tab Details.....	92
Fig. 116	Roles module - tab Employees.....	92
Fig. 117	Assign users .....	93
Fig. 118	Add user .....	93
Fig. 119	Delete user assignment .....	93
Fig. 120	Roles module - tab Function Rights (example).....	94
Fig. 121	Function rights - display sections (example) .....	94
Fig. 122	Function rights - Display function rights.....	94
Fig. 123	Save role.....	95
Fig. 124	Save role.....	96
Fig. 125	Save changes .....	96

---

Fig. 126 Create superuser .....	98
Fig. 127 Create superadmin .....	99

### List of tables

Tab. 1	Login data - system provider .....	7
Tab. 2	Login data - 1st tenant .....	7
Tab. 3	Function rights .....	88
Tab. 4	Function rights .....	94



## 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

### JSON

JavaScript Object Notation

### 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 Socket Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.

---

### **URL**

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

---

### **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.