

Salesforce Integration



Administration manual for system providers

10/16/2020

Product line neo, version 6.x

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

EVOIPneo

EVOLUTIONneo / XXL / eco

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

Copyright © 2019 ASC Technologies AG. All rights reserved.

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

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

Contents

1	General information	4
2	Introduction	5
3	Preconditions	6
3.1	Licenses	6
3.2	Supported integrations	6
4	Installation	7
4.1	Salesforce App	7
4.2	Install SSL certificate	7
4.2.1	Import customer-specific HTTPS certificate	7
4.2.1.1	Import X.509/Private key	8
4.2.1.2	Import PKCS12	9
5	Configuration.....	12
5.1	System Configuration	12
5.1.1	Start application	12
5.1.2	Configure Web Service API	13
5.1.3	Create user API.....	15
5.1.4	Assign recording resources.....	16
5.1.4.1	Assign extensions to tenants	17
5.1.5	Configure PBX module.....	20
5.1.5.1	Tab PHONEapp Configuration	20
5.1.6	Configure PHONEapp	21
5.1.6.1	Category Default Settings	22
5.1.7	Configure phones	23
5.1.8	Configure additional data	25
5.1.9	Configure Recording Planner	27
5.1.10	Configure Applications module	32
5.2	Configure Salesforce application	33
5.2.1	Assign permission sets	33
5.2.2	Assign page layout.....	35
5.2.3	Configure ASC User Management.....	36
5.2.4	Configure remote site settings	38
	List of figures	40
	List of tables	42
	Glossary	43

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

Salesforce is an international provider of cloud computing solutions for companies. Salesforce offers *Software and Platform as a Service*. Salesforce products and services support multiple tenants and are designed to help companies interconnect their employees, customers, and products.

The Salesforce integration enables you to control the recording. You can link the conversations to the contacts and use them for customer care purposes. In addition, it is possible to use the recordings for analysis by means of transcription and keyword spotting. Within Salesforce App Exchange, you can search for recordings and replay them.

For information about the configuration of the integration refer to the respective administration manual.

To use the application System Configuration with Salesforce, you have to carry out the following configurations in the application:

- Configure server, for information about the configuration refer to the respective administration manual of the integration.
- Activate PBX module [PHONEapp](#), for further information about the PBX configuration refer to the respective administration manual of the integration.
- Configure [PHONEapp](#), see [chapter "Configure PHONEapp", p. 21](#)
- Configure phones, see [chapter "Configure phones", p. 23](#)
- Configure additional data, see [chapter "Configure additional data", p. 25](#)
- Configure and activate integration, for more information refer to the respective administration manual of the integration.
- Create recording profile in the Recording Planner, see [chapter "Configure Recording Planner", p. 27](#)

3 Preconditions

The following conditions must be met to be able to configure and use the Salesforce application:

- The operating system must have been installed according to our specifications, refer to the installation manual *Configuration Windows Server 2012 R2 or Windows Server 2016*.
- The *neo* recording software must have been installed according to our specifications, refer to the installation manual for system providers *Installation recording software of ASC*.
- The integration must have been configured according to our specifications; refer to the administration manual of the respective integration solution.

To use the Salesforce application, you have to additionally carry out the following configurations in the application System Configuration:

- Configure PHONEapp, see Configure ASC PHONEapp module
- Configure phones, see Configure phones
- Configure additional data, see Configure additional data
- Create recording profile in the Recording Planner, see [chapter "Configure Recording Planner", p. 27](#)

3.1 Licenses

License name	Number
PHONEapp universal for recording control per system	1 license per recording system
PHONEapp for Salesforce	1 license per recording system
Recording Control Access system license	1 license per recording system
or	or
Recording Control Access software license	1 license per concurrent user
Search & Replay Access system license	1 license per replay server
Search & Replay Access software license	1 license per concurrent user

Tab. 1: ASC licenses

3.2 Supported integrations

The add-on with the Salesforce application can be used with all integrations supporting the function *Record on demand*.

4 Installation

4.1 Salesforce App

You can download the application from *Salesforce App Exchange*.

1. Open the following URL in a browser:
<https://appexchange.salesforce.com/appxListingDetail?listingId=a0N3A00000EcrSGUAZ>
2. Click on the button *Get It Now*.



Fig. 1: Download application via App Exchange

Alternative installation option

1. If you have a login for *Salesforce.com*, you can download the application by clicking on the following link:
<https://login.salesforce.com/packaging/installPackage.apexp?p0=04t0X0000003Mi1&is-dtp=p1>

Follow the on-screen instructions to download and install the package.

4.2 Install SSL certificate



The *neo* system requires a signed [SSL](#) certificate from a root certifying authority; otherwise it will not be possible to establish a connection between Salesforce and the recording server. The operator of the *neo* must have the certificate issued for the respective DNS name and install it on the recording server with the certificate import tool. The DNS name for the *neo* system for which the certificate has been issued must be used as an end device in the Salesforce configuration.

4.2.1 Import customer-specific HTTPS certificate

If you would like to use a customer-specific certificate, you can import it with the program *certimporter.exe*.

1. Change to the folder *C:\Program Files (x86)\ASC\ASC Product Suite\scripts*.
2. Open the file *certimporter.exe*.
 ⇒ The window Certificate Import Tool appears.

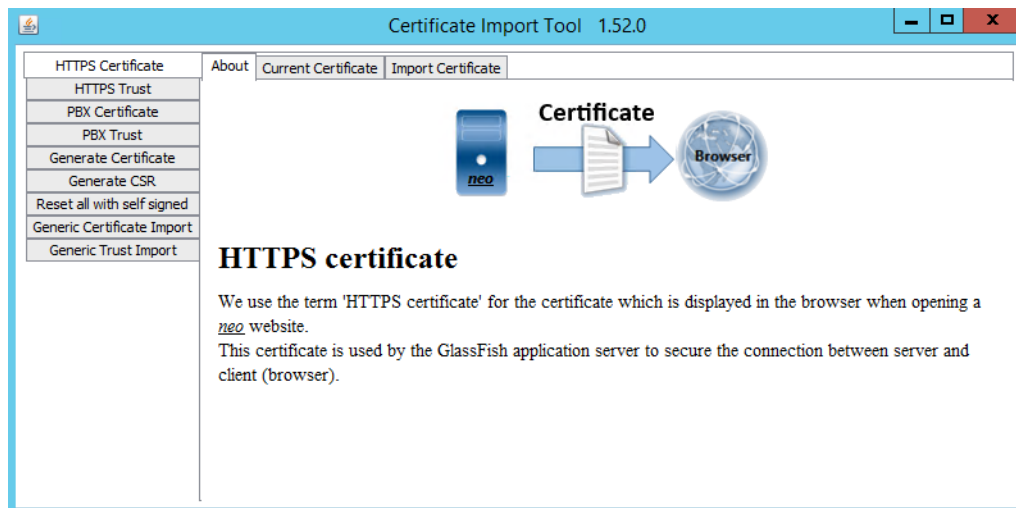


Fig. 2: Certificate Import Tool

The following formats are supported:

- PKCS12
- X.509/Private key

4.2.1.1 Import X.509/Private key

1. Select the menu item *HTTPS Certificate* in the navigation bar.
2. Click on the tab *Import Certificate*.
3. If your certificate is a X.509/Private, select the option *Certificate X.509 (RSA Private key)*.
4. Click on the button next to the field *Certificate X.509* to select your certificate.

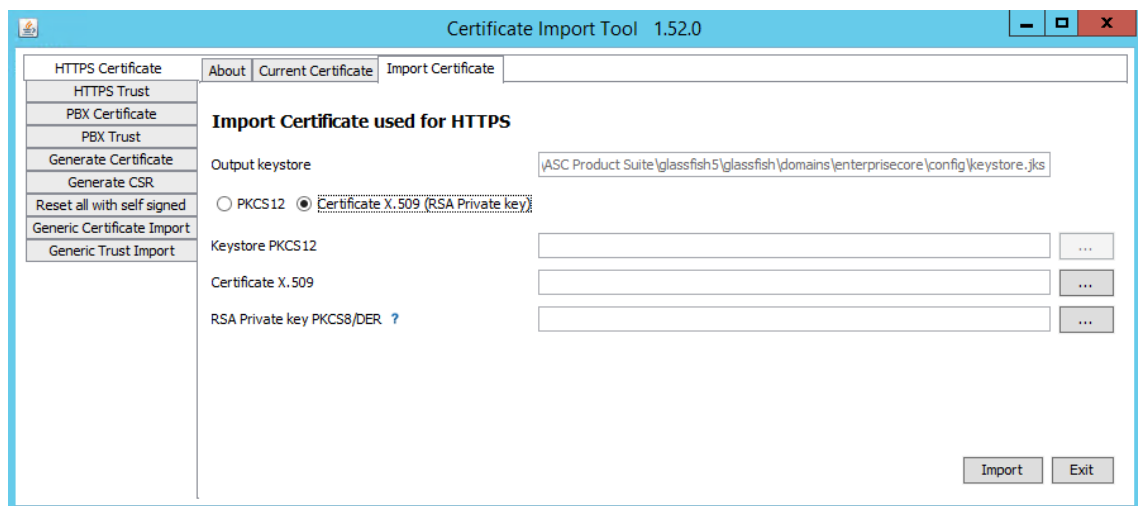


Fig. 3: Import X.509

5. Click on the button *Import*.
⇒ The window to enter the password for the private key appears.

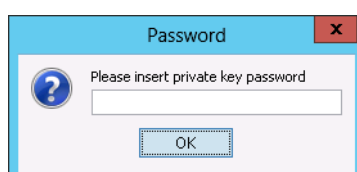


Fig. 4: Enter password for the private key

6. Enter the password for your private key.
If you do not use a password, leave this field empty.
7. Click on the button *OK* to confirm the password.
⇒ A message will inform you about the successful import.

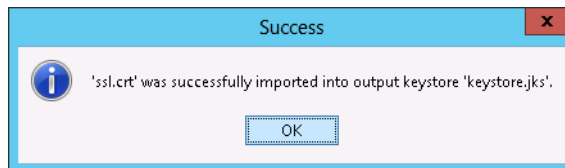


Fig. 5: Message - Successful import

8. Click on the button *OK* to confirm the success message.
9. Click on the button *Exit* to exit the program.
10. Restart the Glassfish server so that the certificate will be applied.
11. In the tab *Current Certificate*, you can check the currently valid certificate.

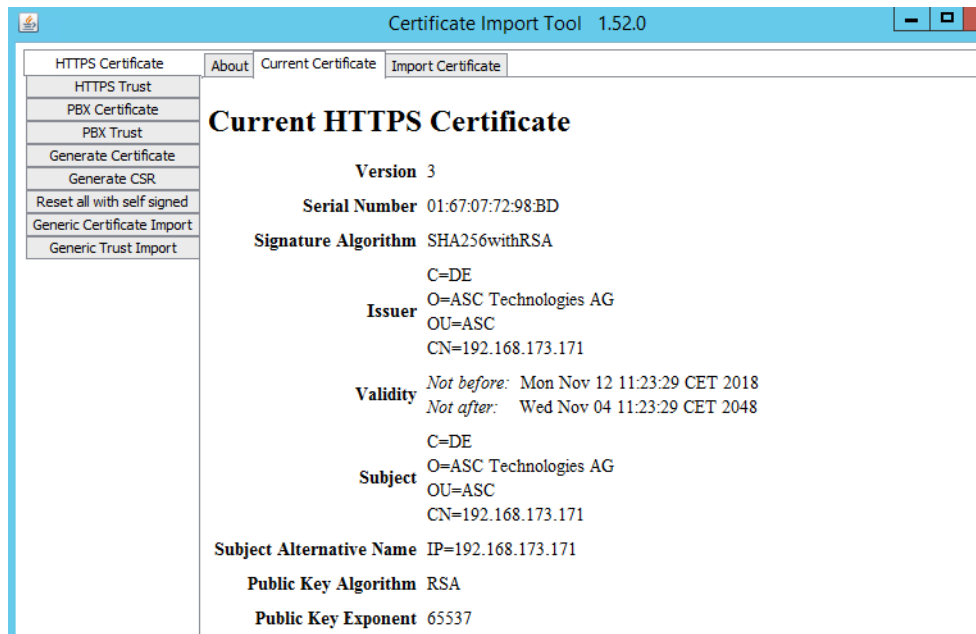


Fig. 6: Check currently valid HTTPS certificate

4.2.1.2 Import PKCS12

1. Select the menu item *HTTPS Certificate* in the navigation bar.
2. Click on the tab *Import Certificate*.
3. If your certificate is a PKCS12 Keystore, select the option *PKCS12*.
4. Click on the button next to the field *Keystore PKCS12* to select your PKCS12 Keystore.

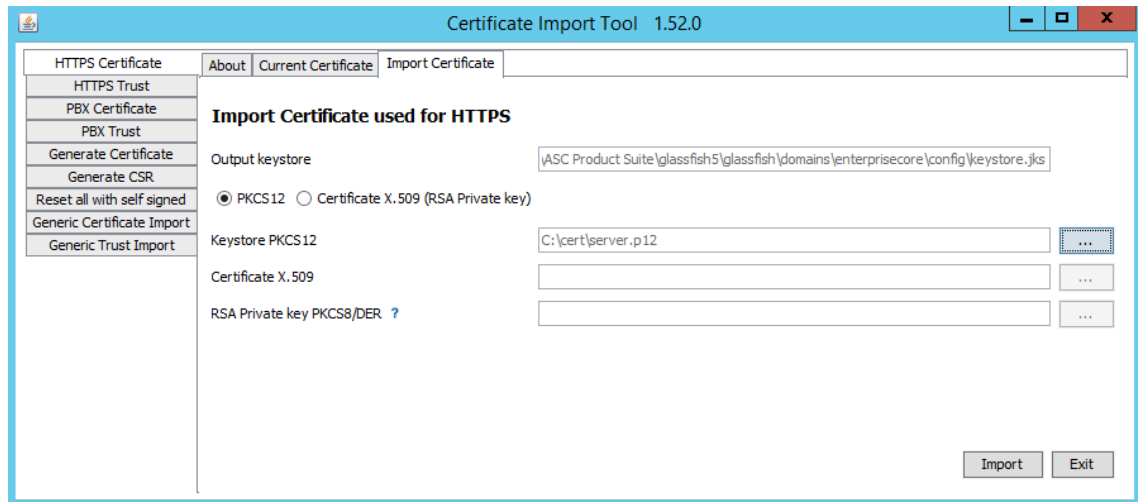


Fig. 7: Import PKCS12 Keystore

5. Click on the button *Import*.
 - ⇒ The window to enter the alias for the PKCS12 Keystore appears.

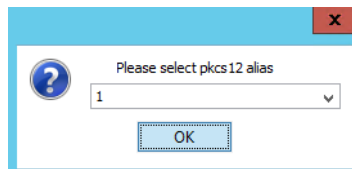


Fig. 8: Confirm alias

6. Click on the button *OK* to confirm the alias.
 - ⇒ The window to enter the password appears.

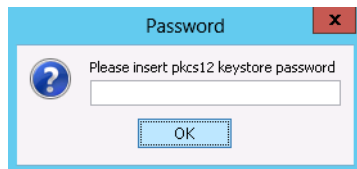


Fig. 9: Enter password for PKCS12 Keystore

7. Enter the password for your PKCS12 Keystore.
If you do not use a password, leave this field empty.
8. Click on the button *OK* to confirm the password.
9. Click on the button *Exit* to exit the program.
10. Restart the Glassfish server so that the certificate will be applied.
11. In the tab *Current Certificate*, you can view the currently valid certificate.

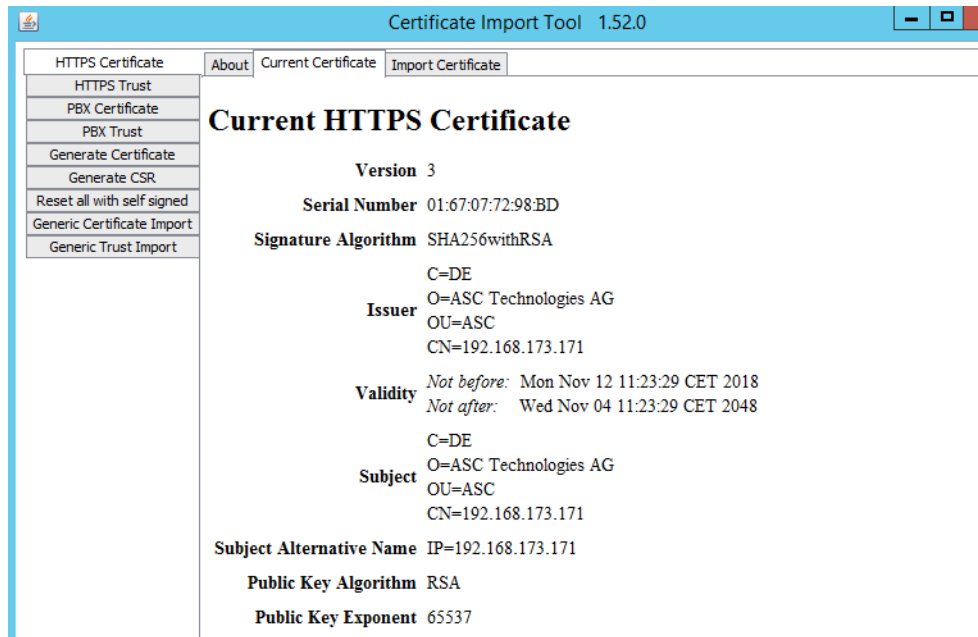


Fig. 10: Check currently valid HTTPS certificate

5 Configuration

5.1 System Configuration



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

5.1.1 Start application

During the installation routine, shortcuts for the *neo* programs are created on your desktop.

1. To start the application directly on the server, double-click on the shortcut System Configuration.

To access the application from a computer via the web, enter the following URL in the address bar:

https://<System-IP>/SystemConfiguration.

If you have configured customer-specific ports, you have to include the port in the URL:

https://<System-IP>:<Port>/SystemConfiguration.

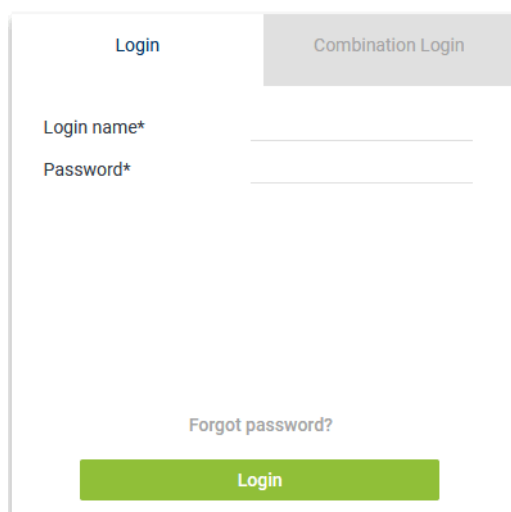


Fig. 11: System Configuration - web interface

To install and configure the recording solutions, you have to log in as system provider.

Login data for the administrator of the system provider:

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

Tab. 2: Login data - system provider

2. Log in to the web interface.
 - ⇒ The main window System Configuration appears.

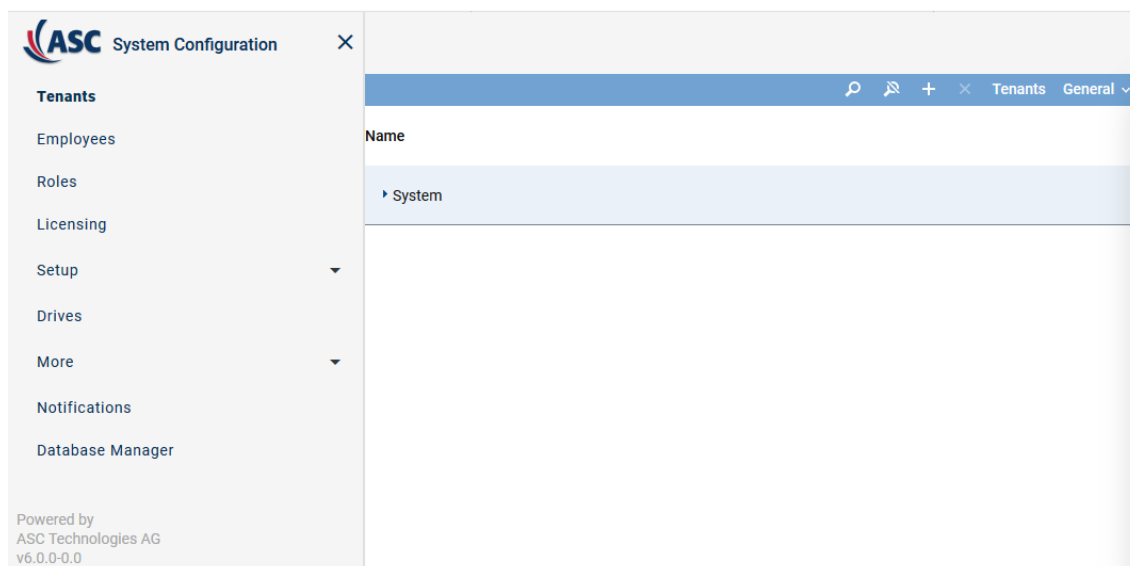


Fig. 12: System Configuration - main view:

5.1.2 Configure Web Service API

To enable tenants to use the Web Service to search for and replay recordings, you as system administrator must configure this option for each tenant.

1. Select the menu item *Tenants* in the navigation bar.
2. In the main view, select the account of the tenant for which you would like to adjust the settings.
3. Click on the tab *Web Service* to configure this option for the tenant.

SYSTEM PROVIDER
Last login Dec 2, 2019 10:15:25 AM

1st-tenant ✕

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

General Functions ▼

☒ Checks the general web service functionality.

Employees ▼

☐ Allows exporting employees
☐ Allows importing new as well as existing employees

Conversation ▼

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

Tenant ▼

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

Conversations Export Server ▼

Export server

API-01

+
-

Save

Reset

Fig. 13: Web service functionalities for the tenant

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

Group field General Functions

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

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

Group field Conversation

In this group field, you can configure the functions for the search and for the export of 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>Allows exporting conversations</i>	Activate the check box if you would like to allow the tenant to export conversations via the Web Service. NOTICE! When activating this function, you have to enter an export server in the group field <i>Conversations Export Server</i> .

Allows searching for conversations via Web Service Activate the check box if you would like to allow the tenant to search conversations via the Web Service.

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*.

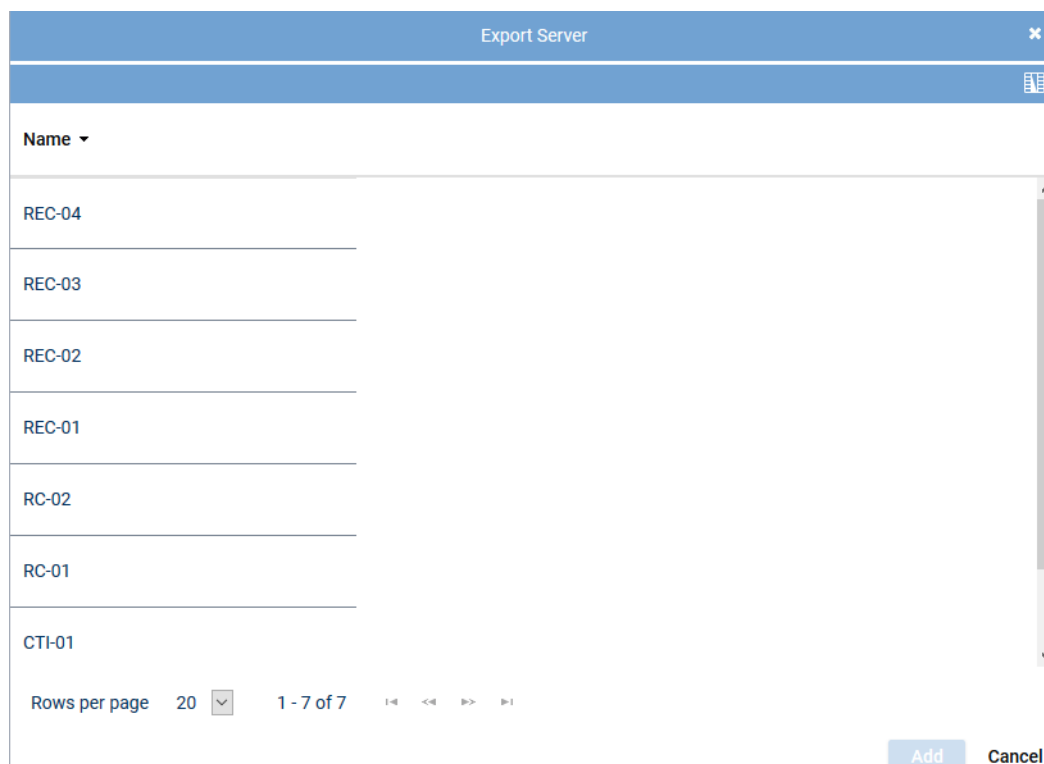


Fig. 14: Select export server

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*.

3. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

5.1.3

Create user API

For external recording control and the access to the applications, it is important that the user is a technical user whose password cannot expire.

Therefore, create a new superuser as tenant for the [API](#) interface.



The following configuration has to be carried out as the administrator of the tenant.

1. Select the menu item *Employees* in the navigation bar to create a new user.

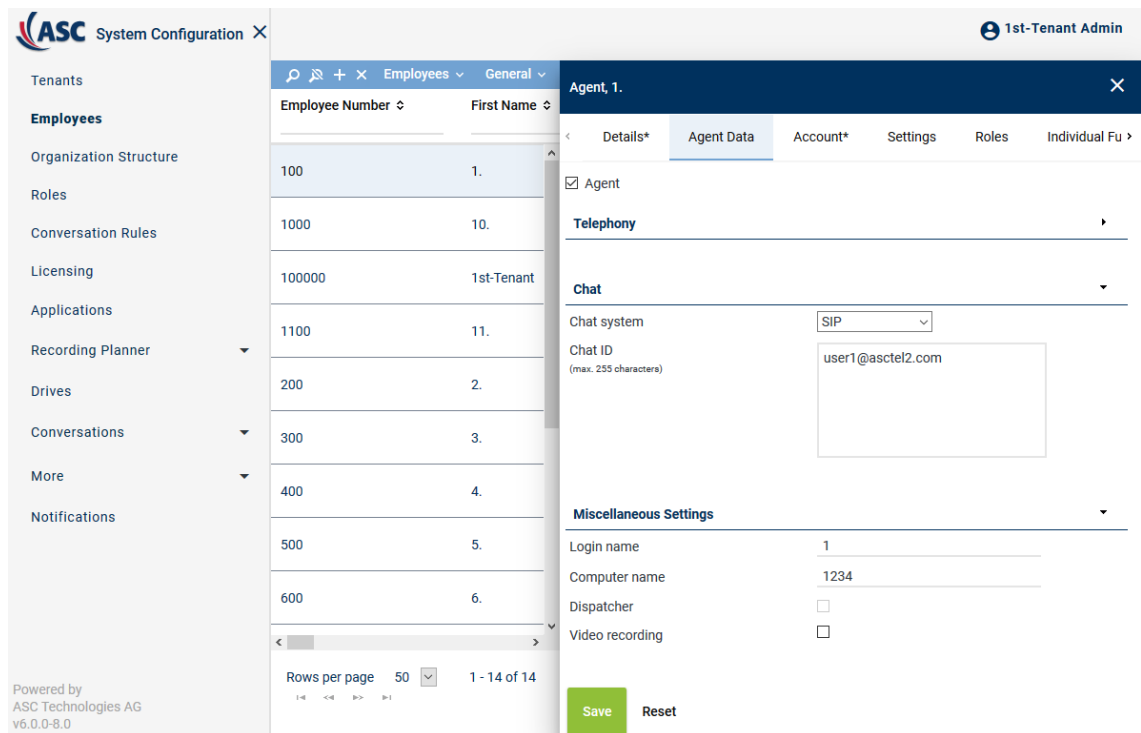



Fig. 15: Employees module - main view

2. Click on the icon  (Add) in the toolbar.
⇒ In the tab Details, the entry fields for the new user appear.
3. Enter *API* as the first name and the last name of the user.
4. Click on the tab *Account* and enter the login data for this user.
5. Click on the button *Save* so that the tab *Settings* becomes active.
6. Click on the tab *Settings*.
7. Give the user the right *Superuser*

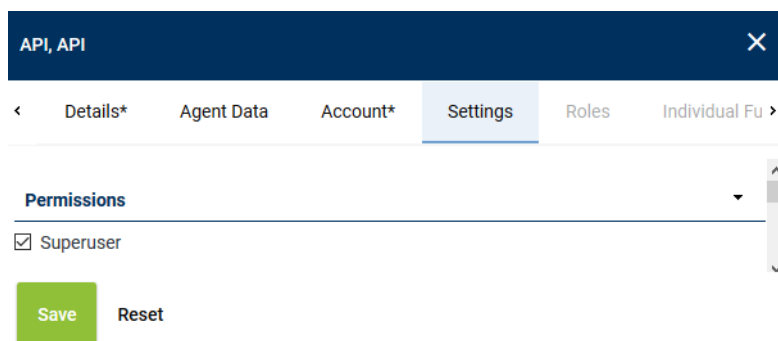


Fig. 16: Configure user API as superuser

8. Click on the button *Save* to apply the settings.



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

5.1.4 Assign recording resources

In multi-tenant systems, you have to assign each tenant its own recording resources.

Depending on the recording type, agents can be assigned to the recording resource via the extension, via the PBX Agent ID or via the chat ID. Within one tenant, you can configure all three possibilities.

5.1.4.1 Assign extensions to tenants

If you would like to make an assignment based on extensions, you can assign the respective tenant the extension designated for recording in the Tenants module.



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.

1. Select the menu item *Tenants* in the navigation bar.

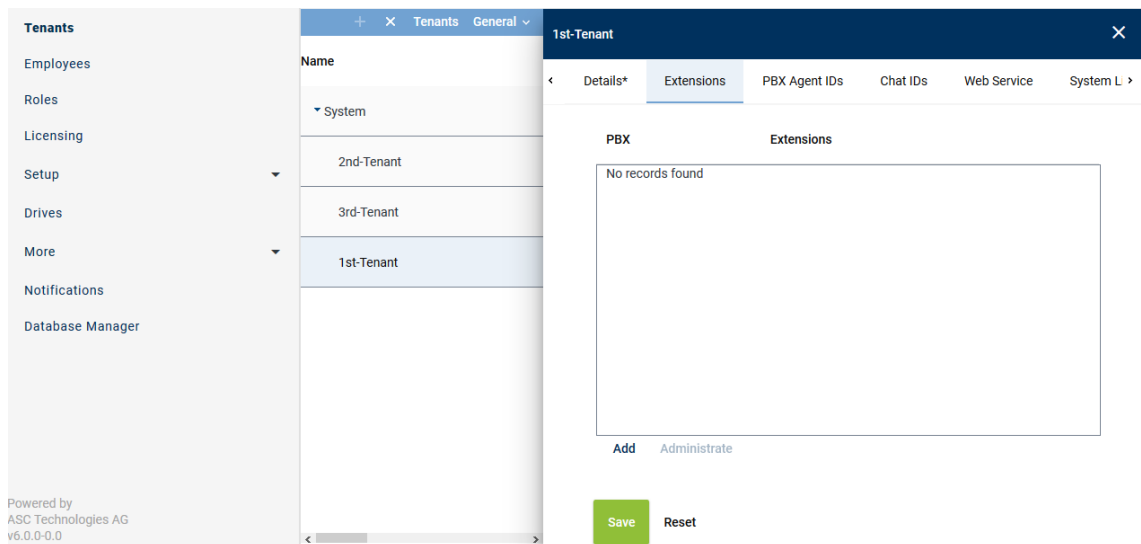


Fig. 17: Tenants - main view - tab Extensions

5.1.4.1.1 Add extensions

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

Add Extensions ✕

PBX PBX

☐ File import

☐ File contains a headline

File name ...

☒ Manual entry

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

6000-6999

☐ Replace existing list of extensions

Add
Cancel

Fig. 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"> • ZIP • TXT • CSV <p>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.</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"> • Click on the button ... behind the field <i>File name</i>. • Click on the button <i>Choose File</i>. • Select the respective file in the Explorer and click on the button <i>Open</i>. • Click on the button ↗ <i>Upload File</i>.
<i>Manual entry</i>	<p>Select this option to enter extensions or extension ranges manually.</p>

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.

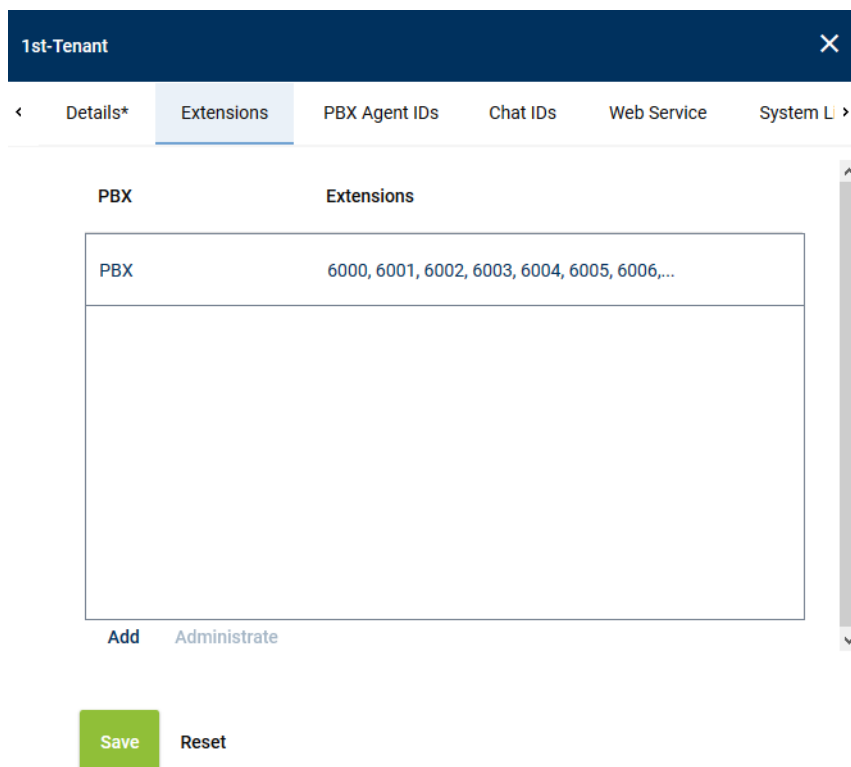
☒ = Function has been activated; the entry replaces the extensions of the selected PBX.

☐ = 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.

5.1.4.1.2 Remove extensions

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



The screenshot shows a configuration window for '1st-Tenant'. The 'Extensions' tab is active, displaying a table with two columns: 'PBX' and 'Extensions'. The first row shows 'PBX' and a list of extensions: '6000, 6001, 6002, 6003, 6004, 6005, 6006,...'. Below the table, there are buttons for 'Add' and 'Administrate'. At the bottom of the window, there are buttons for 'Save' and 'Reset'.

Fig. 19: Remove extensions

2. Click the button *Administrate*.

- 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

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

5.1.5 Configure PBX module

In the PBX module, you have to activate the PHONEapp configuration.

- Select the menu item *Setup > PBX* in the navigation bar.
⇒ The following window appears:



Fig. 21: Create new PBX

5.1.5.1 Tab PHONEapp Configuration

- Click on the tab PHONEapp Configuration.

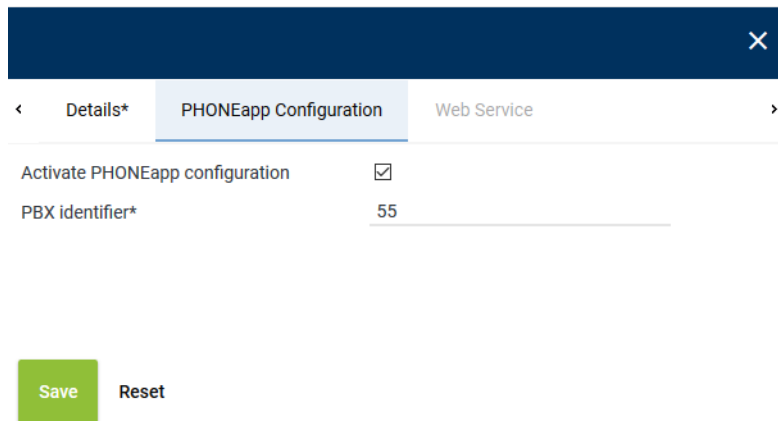


Fig. 22: Activate PHONEapp configuration

2. Enter the following parameters:

Activate PHONE <u>app</u> configuration	Tick the check box to activate the PHONE <u>app</u> . Once the PHONE <u>app</u> has been activated here, you can proceed with the configuration in the PHONEapp module and in the Phones module.
PBX identifier	Enter the identifier of the PBX. The identifier allows the PBX to connect with the PHONE <u>app</u> . This identifier is specified during the installation of the PBX. Only use letters, numbers, and underscores.

3. In the detail view, click on the button *Save* to apply the changes in the tab *PHONEapp Configuration*.

5.1.6 Configure PHONEapp

In the PHONEapp module, you can adjust the basic settings for the phone applications and configure phone types.

1. In the navigation bar, select the menu item *Setup > PHONEapp*.

⇒ The following window appears:

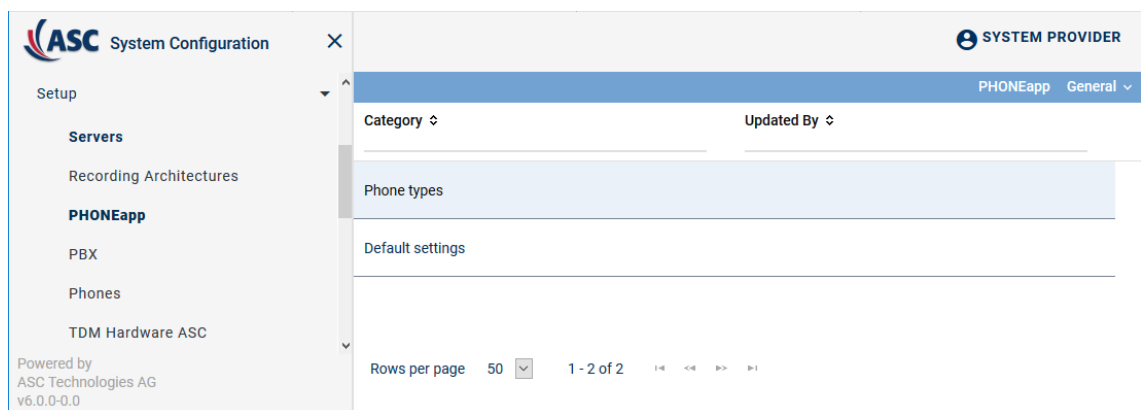


Fig. 23: PHONEapp - main view:

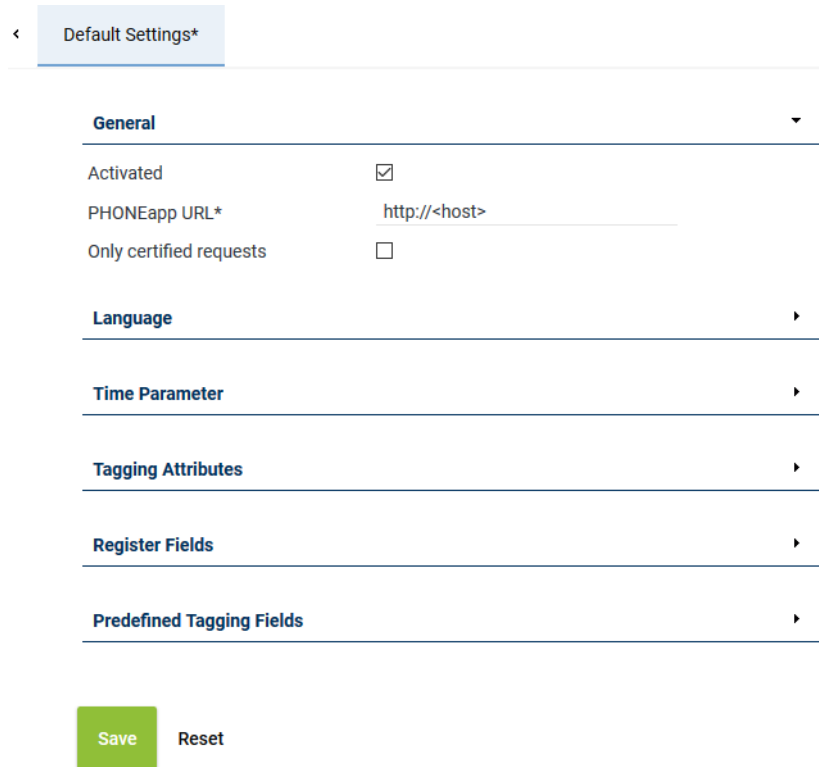
In the category *Phone types*, you can display the properties of the supported end devices and add additional phone types.

To configure the function keys you have to create a new phone type in the category *Phone types*.

5.1.6.1 Category Default Settings

In this category, you define the values for the general settings of your PBX. The default settings are divided into different group fields.

1. In the main view of *Setup > PHONEapp*, select the category *Default Settings*.
⇒ Different group fields are displayed in the detail view.



< Default Settings*

General

Activated ☒

PHONEapp URL*

Only certified requests ☐

Language

Time Parameter

Tagging Attributes

Register Fields

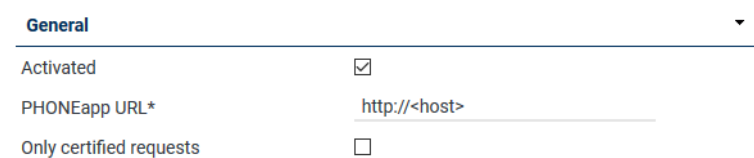
Predefined Tagging Fields

Save Reset

Fig. 24: Detail view Default settings

5.1.6.1.1 Group field General

1. Enter the following parameters:



General

Activated ☒

PHONEapp URL*

Only certified requests ☐

Fig. 25: Group field General

General	Here, you have to enter the address of the <u>PHONEapp</u> and activate it.
• Activated	Activates the recording control by means of the <u>PHONEapp</u> .
• PHONEapp URL	<p>Enter the URL under which the <u>PHONEapp</u> is supposed to be accessible. Enter the IP address of the application server instead of <i><host></i>.</p> <p>Enter the additional port, if it differs from default (port 80 for <i>http</i> or port 443 for <i>https</i>), e. g. <i>http://<core_ip>:90</i>.</p> <p>The end device will establish a connection with this URL. The <u>PHONEapp</u> transfers the data provided by the URL to the display of the end device.</p>

When using a load balancer, enter the IP address and the port of the load balancer here.

- *Only certified requests*

If the check box has been activated, certificate-based authentication of the client (end device) on the server is required. To be able to do so, the client certificate must be imported in the certificate key store of the server.

5.1.6.1.2 Save configuration

1. To save the settings, click on the button *Save*.
To discard the settings, click on the button *Reset*.

5.1.7 Configure phones

The phones are configured in the menu item *Phones* of the Setup module of the application System Configuration.

1. Select the menu item *Setup > Phones* in the navigation bar.

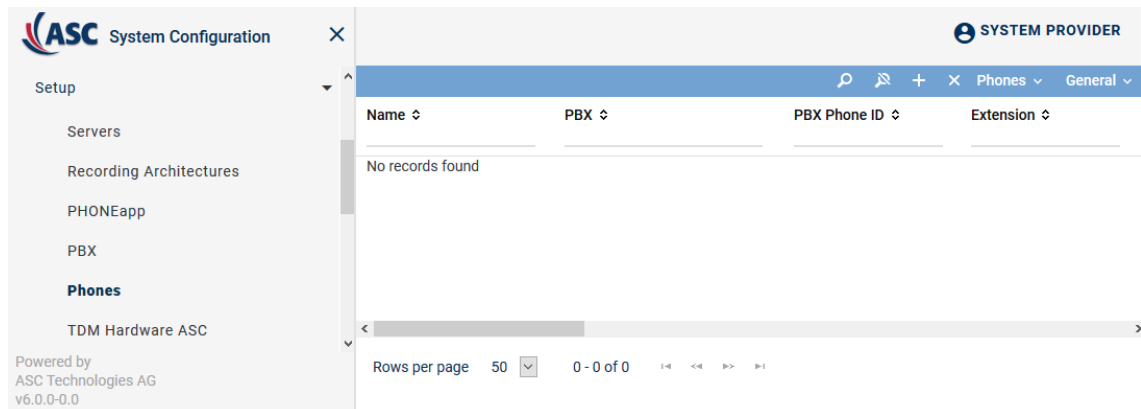

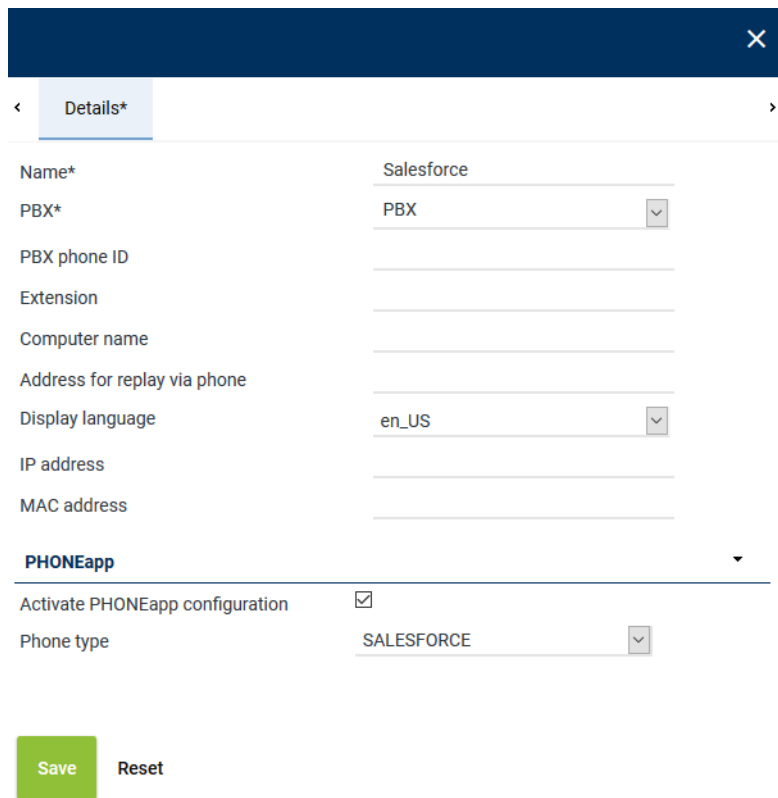


Fig. 26: Setup - Phones

2. To add a new phone, click on the icon  (Create).
3. Select the option *IP Phone*.
4. Click on the tab *Details* in the detail view.



Configure the type of the end device that you would like to use for the Salesforce application.



Details*

Name* Salesforce

PBX* PBX

PBX phone ID

Extension

Computer name

Address for replay via phone

Display language en_US

IP address

MAC address

PHONEapp

Activate PHONEapp configuration ☒

Phone type SALESFORCE

Save Reset

Fig. 27: Tab Details (example)

Enter the following parameters:

<i>Name</i>	Enter the name of your phone.
<i>PBX</i>	Select your already configured PBX.
<i>PBX phone ID</i>	Enter the ID of the end device of the PBX. This field is a mandatory field if you use shared lines.
<i>Extension</i>	Enter the extension of the end device. This field is a mandatory field when entering no <i>PBX phone ID</i> .
<i>Computer name</i>	Enter the name of your computer if you would like to use the feature <i>Free Seating</i> .
<i>Address for replay via phone</i>	Enter the IP address or the phone number of the end device which allows a SIP addressing of the end device.
<i>Display language</i>	Select the language which is supposed to be used on the display of the end device.
<i>IP address</i>	Enter the IP address of the end device. This field is a mandatory field if you would like to start the PHONEapp automatically.
<i>MAC address</i>	Enter the MAC address of the end device if the IP address is not available.
<i>Activate PHONEapp configuration</i>	Activate the check box to activate the PHONEapp on the end device. This option is only available if the PHONEapp has been activated in the PBX module.
<i>Phone type</i>	Select the phone type SALESFORCE. The phone type is only available if you have installed the license PHONEapp for Salesforce.

Alternatively, you can import the phone configuration. To do so, upload a file containing the information about the phones. Supported file types are: ZIP, XML or CSV.



For information about importing phone configurations refer to the administration manual for system providers *Import of phone configurations*.

5. In the detail view, click on the button *Save* to apply the changes in the tab *Details*.

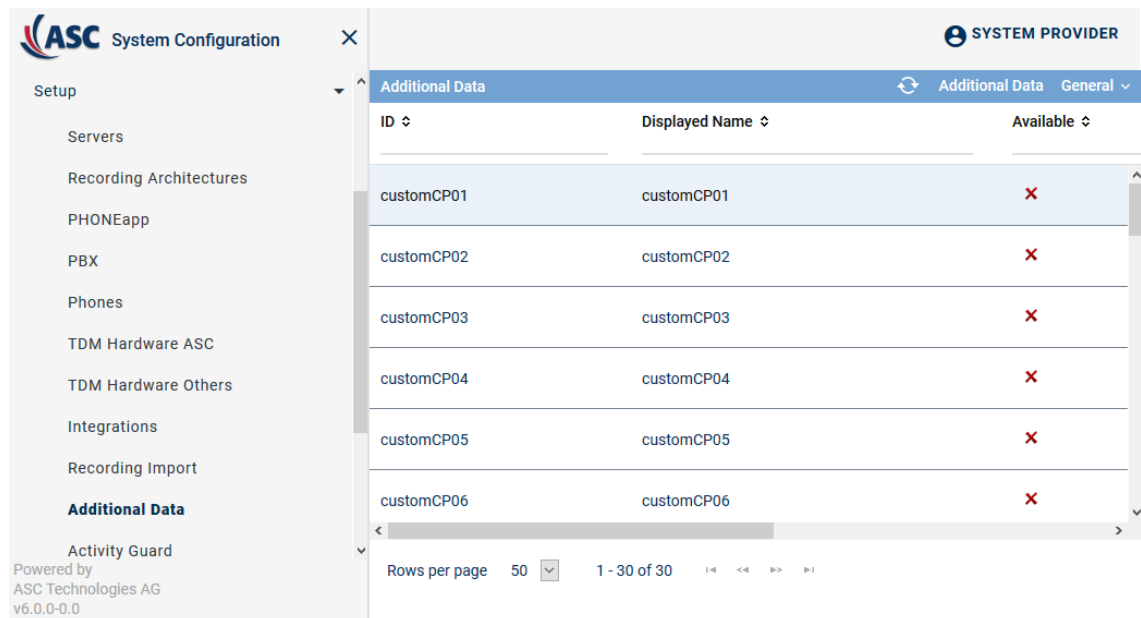
⇒ The recently created phone is displayed in the main view.

5.1.8 Configure additional data

In the Additional Data module, you can configure the additional data which is delivered for a conversation by the add-on.

For selection fields to appear in the drop-down list when mapping them in the [CTI](#) configuration in the integration, they have to be configured in the Additional Data module.

1. Select the menu item *Setup > Additional Data* in the navigation bar.



The screenshot shows the ASC System Configuration interface. On the left is a navigation menu with items like Servers, Recording Architectures, PHONEapp, PBX, Phones, TDM Hardware ASC, TDM Hardware Others, Integrations, Recording Import, **Additional Data**, and Activity Guard. The main area displays the 'Additional Data' module with a table of configuration items. The table has columns for ID, Displayed Name, and Available. There are 6 rows, each with a customCP ID and name, and an 'Available' status marked with a red 'X'. At the bottom, there is a pagination bar showing 'Rows per page 50' and '1 - 30 of 30'.

ID	Displayed Name	Available
customCP01	customCP01	X
customCP02	customCP02	X
customCP03	customCP03	X
customCP04	customCP04	X
customCP05	customCP05	X
customCP06	customCP06	X

Fig. 28: Additional Data module - main view

2. Select the set of data you would like to configure.

⇒ The detail view displays the information you can configure.

customCP01

Details

ID

customCP01

Description

Change Display Name

Availability

Save

Reset

Fig. 29: Configure additional data

Group field Change display name







Change Display Name		
Language	Content	
ar_SA	customCP01	
bg_BG	customCP01	
de_DE	Universal Call ID	
en_GB	customCP01	
en_US	Universal Call ID	 

Fig. 30: Group field Change display name

1. To change the display name, click on the pen in the line of the language you would like to change.
2. Enter a display name and click on the check mark at the end of the line to confirm the entry.

Group field Availability

Availability	
Available	<input checked="" type="checkbox"/>
Editable	<input checked="" type="checkbox"/>
External recording control	<input checked="" type="checkbox"/>

Fig. 31: Group field Availability

<i>Available</i>	Activate the check box to make the data field available to the entire system.
<i>Editable</i>	Activate the check box to allow the data field to be edited in the search and replay applications later on.
<i>External Recording Control</i>	Activate the check box to be able to use the data field for external recording control.

1. Click on the button *Save* to save the settings.



For further information about the configuration of the additional data refer to the administration manual *Additional Data module*.

5.1.9

Configure Recording Planner



The following configuration has to be carried out as the administrator of the tenant.

In the Recording Planner module of the application System Configuration, you can configure recording plans for automated recording or external recording control.

1. Log in to the application System Configuration as system administrator of the tenant (*1st-tenant-admin*).
2. Select the menu item *Recording Planner > Compliance*.
⇒ The main view appears.

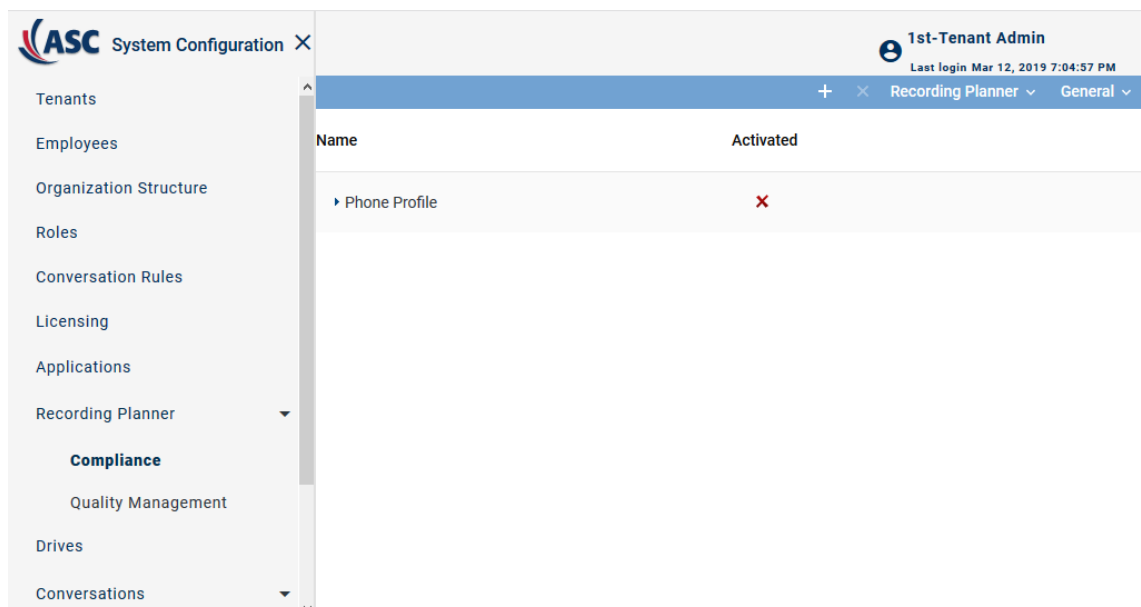



Fig. 32: Recording Planner - main view

3. A phone profile has been configured and activated by default. Delete or deactivate this profile so that it does not interfere with the new recording profile.
4. In the main view, click on the icon  (Create/Duplicate profile) to create a new profile.

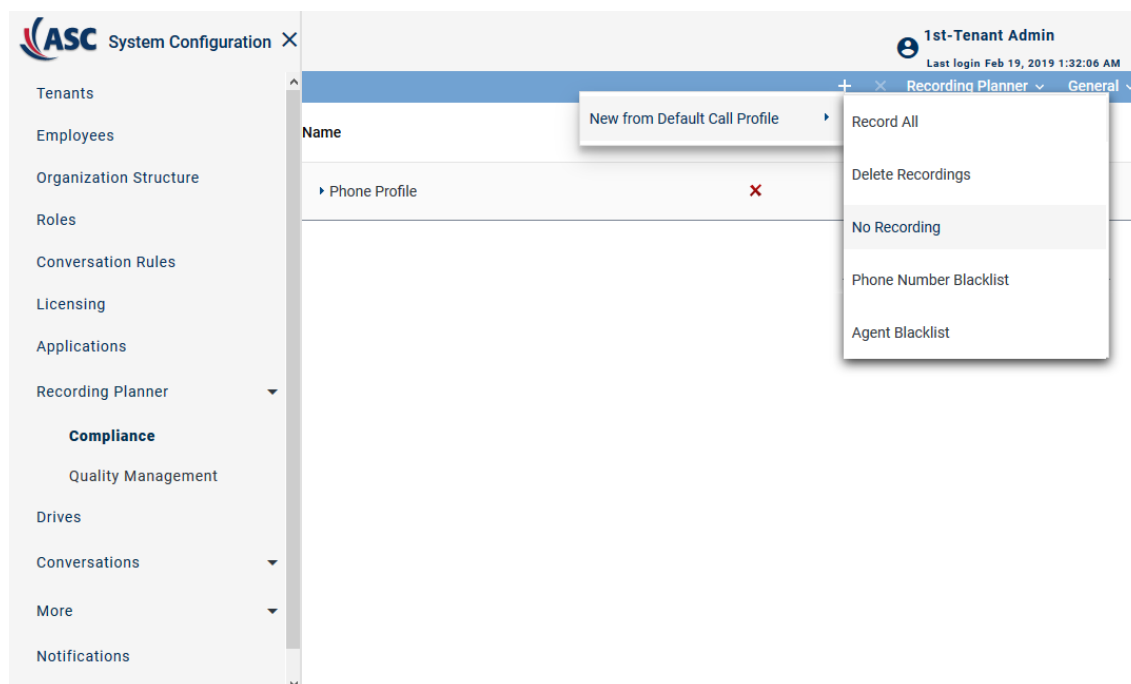


Fig. 33: Create new profile

5. Select the option *New from Default Call Profile > No Recording*. That way, you can enable external recording control by configuring the action node.

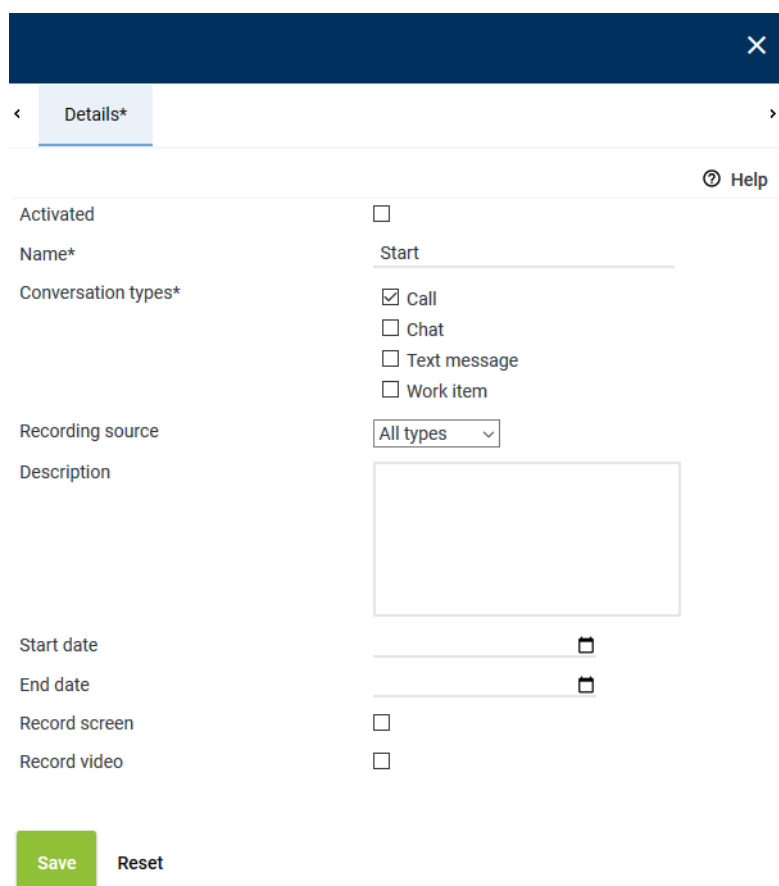


Fig. 34: Configure parameters for the recording profile

6. Enter the following parameters:

<i>Activated</i>	Do not activate the check box before you have configured the action node.
<i>Name</i>	Enter a name for the recording profile.
<i>Conversation types</i>	Select the option <i>Call</i> .
<i>Recording source</i>	Select the entry <i>AllTypes</i> from the drop-down list.

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

⇒ The profile now appears in the main view.

8. Click on the arrow in the line of the profile.

⇒ Below the profile, a default action node appears.

When creating a new profile, the action node *Default* always appears. This action node cannot be changed. To configure a user-defined recording, you have to create a new action node and replace the default action node with the new action node.

9. Select the action node and click on the menu item *Recording Planner > Create/Edit Action Node Configuration* in the toolbar.

10. Select the menu item *New > Don't Record*.

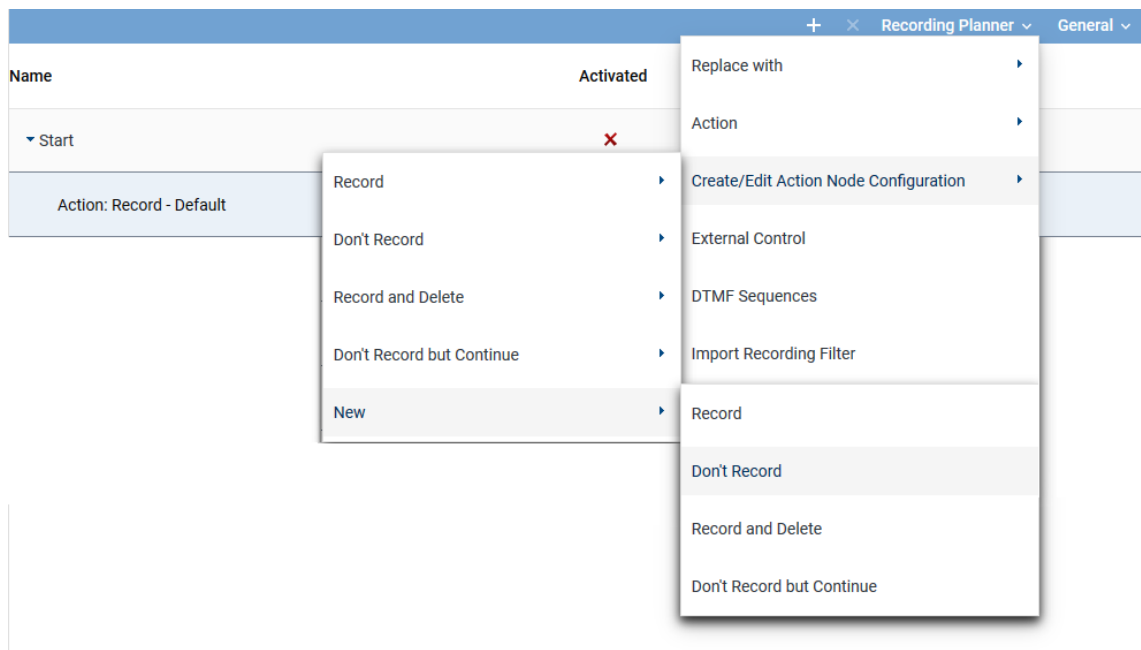


Fig. 35: Create action node

11. In the detail view, enter the parameters which enable external recording control.

Configuration

Details*

Type

Don't record

Name*

Start

Keep recordings when stream is recognized

☐

External Recording Control

Allowed clients

☒ API
☒ CLIENTcommand
☐ DTMF sequences
☐ Function keys
☒ PHONEapp
☐ SCREENrec

Allowed Actions

Start recordings

☒

Stop recordings

☒

Created recordings

☒ Keep, if not externally deleted
☐ Delete, if not externally kept

Keep recordings

☐

Delete recordings

☐

Suppress recordings

☐

Unsuppress recordings

☐

Wrap-up time

0 Minute(s)

0 Second(s)

Delete recordings

☐ Never
☒ After

1 Year(s)

Save

Cancel

Fig. 36: Enter parameters for the action node

Name Enter a name for the action node.

Group field External Recording Control

Allowed Clients Activate the options

- API
- CLIENTcommand
- PHONEapp

Group field Allowed Actions

Start/Stop recordings	Allows starting and stopping the recording manually for all clients which have been activated in <i>External recording control</i> .
Created recordings	Select the option which is supposed to be carried out if no decision has been made externally. <input checked="" type="radio"/> <i>Keep, if not externally deleted</i>
Delete recordings	Select the option <input checked="" type="radio"/> After and enter the period of time after which the saved recordings are supposed to be deleted in general, e. g. 5 days.

- Click on the button **Save**.
⇒ The action node *Default* can be replaced with the action node *Start*.
- Select the menu item *Recording Planner > Action > Don't Record > Start* in the toolbar.

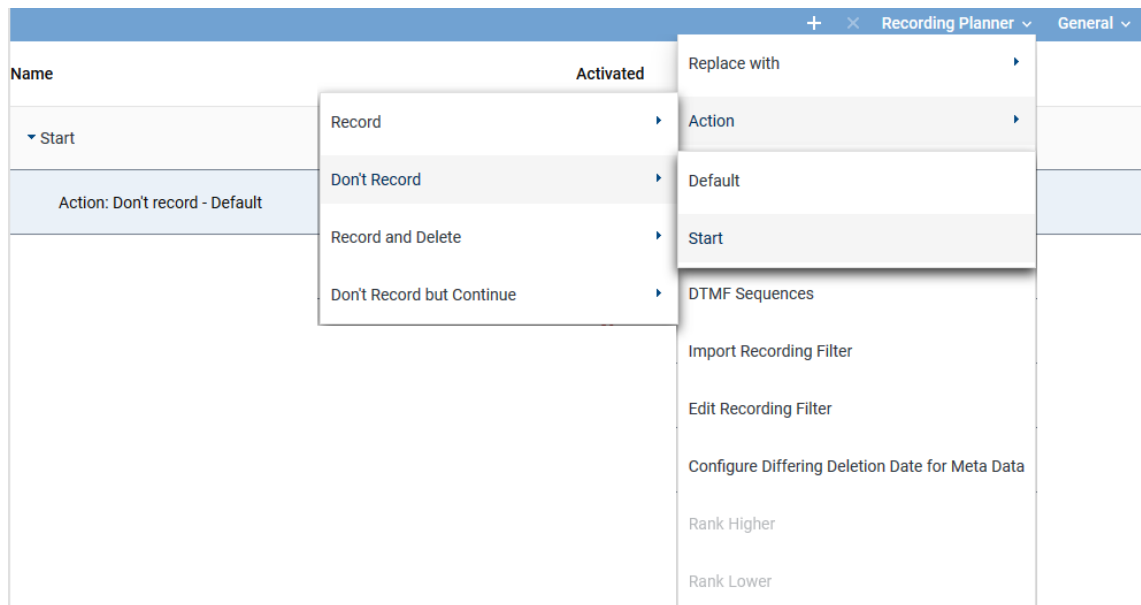


Fig. 37: Replace action node

The action node with the start configuration appears in the main view.

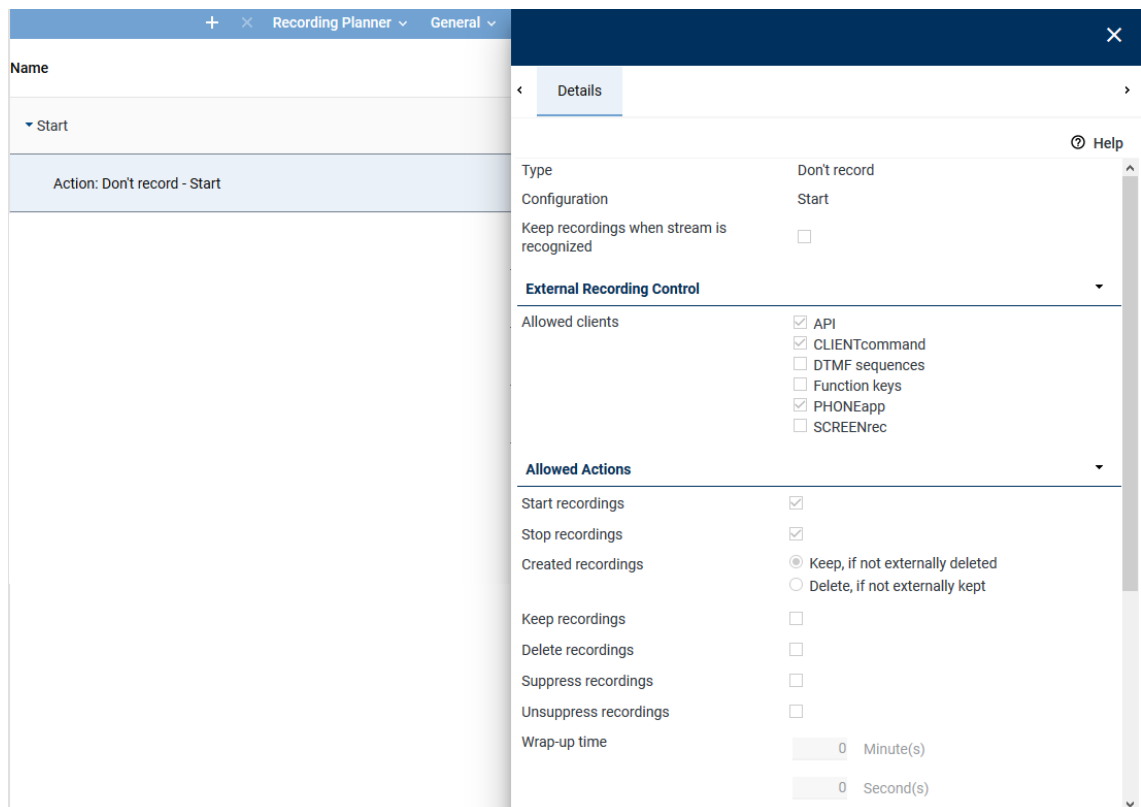


Fig. 38: Action node - KSK start

- Select the recording profile *Start* in the main view.
- Activate the check box *Activated* in the detail view so that the profile can be used for recording.

+ × Recording Planner ▾ General ▾	
Name	Activated
▾ Start	✓
Action: Don't record - Start	

Fig. 39: Activate recording profile



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

5.1.10

Configure Applications module

To enable the recording server to communicate with the Salesforce application, you must configure the connection data in the Applications module.



The following configuration has to be carried out as the administrator of the tenant.

1. Log in to the application System Configuration as system administrator of the tenant (*1st-tenant-admin*).
2. Select the menu item *Applications* in the navigation bar.
⇒ The main view appears.



 System Configuration ×		 1st-Tenant Admin	
Tenants Employees Organization Structure Roles Conversation Rules Licensing Applications Recording Planner ▾ Drives Conversations ▾ More ▾ Notifications SCREENminer Rules		Settings General ▾	
		Name ↕	
		Teleopti Info	
		Salesforce	
		POWERplay Go	
		Audio analysis	
		CLIENTcommand	
		POWERplay Instant	
		POWERplay Web for Xpert	

Fig. 40: Applications module - main view

3. In the main view, select the entry *Salesforce*.
4. Enter the connection data in the tab *General Settings*.

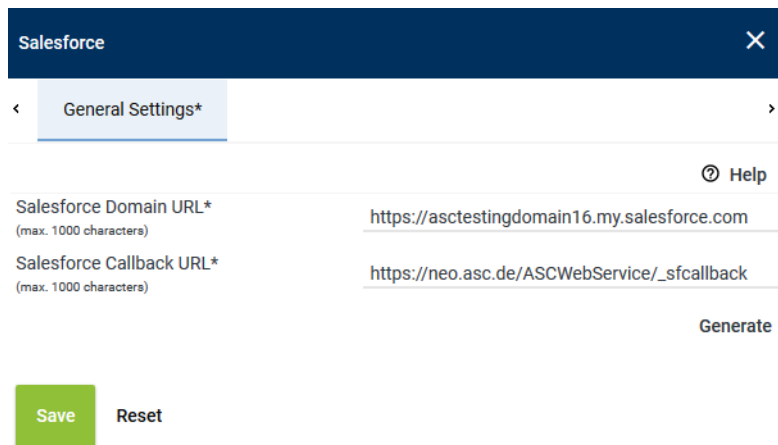


Fig. 41: Configure general settings for the connection to the Salesforce app

The two components communicate via the two URLs.

Salesforce Domain URL	Enter the URL to the Salesforce application. The URL contains the name of the tenant to authenticate in the Salesforce app. The login request is sent via this URL. e. g. https://asctestingdomain16.my.salesforce.com
Salesforce Callback URL	Enter the URL of the Web Service of the recording server with the addition <code>ASCWebService/_sfcallback</code> . The Salesforce app uses this URL for its response. e. g. https://neo.asc.de/ASCWebService/_sfcallback

The recording server send an authentication request with the login data to the Salesforce app. The Salesforce app responds via the configured callback URL.

5. Click on the button *Save* to save the entries.
 - ⇒ The button *Generate* becomes active.
6. Click on the button *Generate*.
 - ⇒ A window appears to enter the login data for the Salesforce application.
7. To be able to establish a connection, you must enter the user name and the password of the tenant once.

5.2 Configure Salesforce application

To be able to use the application, the user ASC must receive a permission set and a page layout.

1. Log in to the Salesforce interface in the browser as the administrator of the tenant of ASC.
2. Within the icon *Settings* in the top right corner, select the menu item *Setup*.

5.2.1 Assign permission sets

1. Use the quick search to search for the entry *permission sets*.

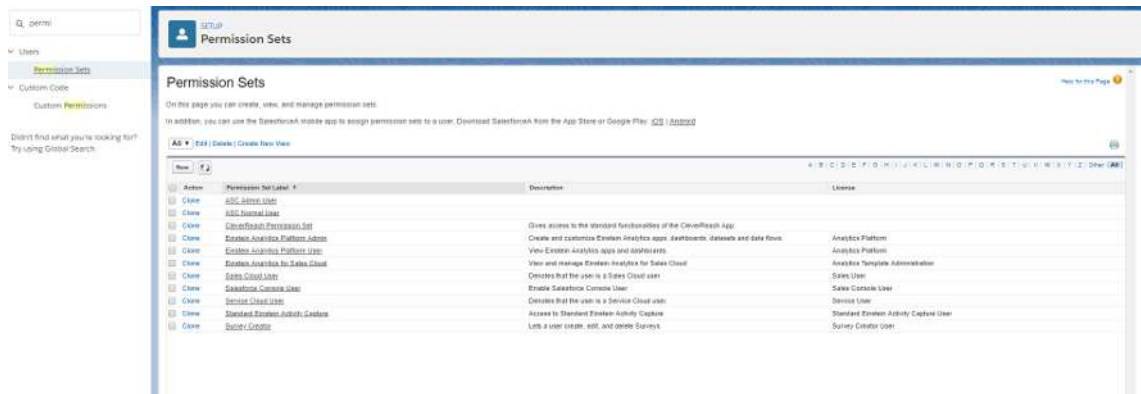


Fig. 42: Setup - user - permission sets

2. Select the permission set *ASC Admin User*.

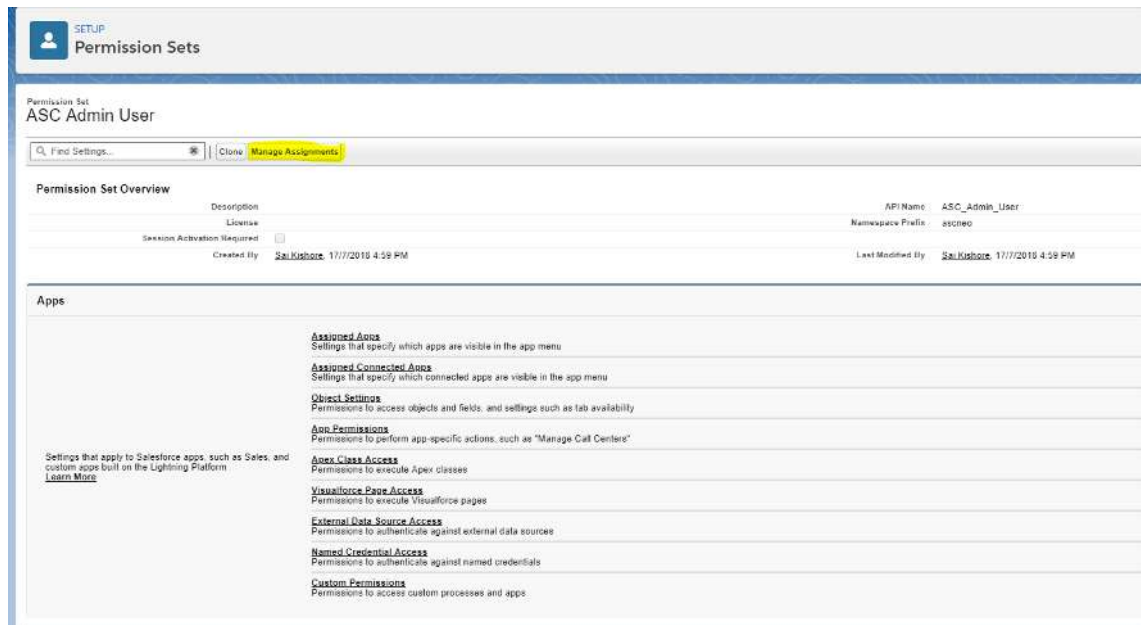


Fig. 43: Permission sets - Manage Assignments

3. Click on the button *Manage Assignments*.
⇒ The window to select the *user* appears.



Fig. 44: Permission sets - Add Assignments

4. Click on the button *Add Assignments*.




Fig. 45: Add Assignments

5. Activate the check box in front of the respective user to assign a permission.

6. Click on the button *Assign*.

⇒ A notification confirming the successful assignment appears.



Full Name	Username	User License	Message
Sal Kishore	sal.kishore@asc.co.uk	Solutions	Success

Fig. 46: Assigned permission

7. Click on the button *Done*.

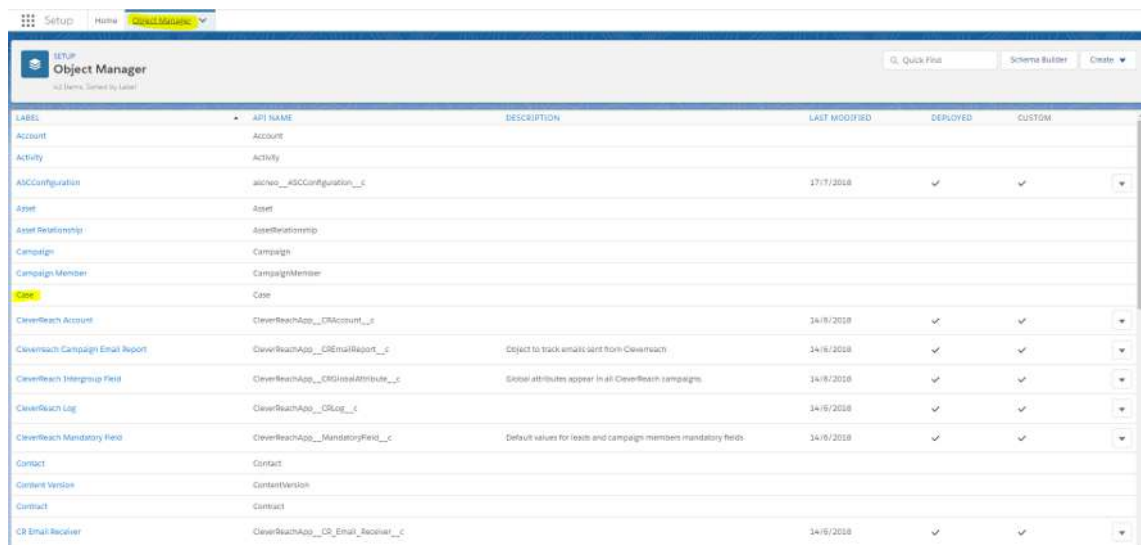
⇒ The user appears in the list for the assigned permissions.

5.2.2

Assign page layout

1. Click on the tab *Object Manager*.

2. Select the menu item *Case* in the navigation bar.

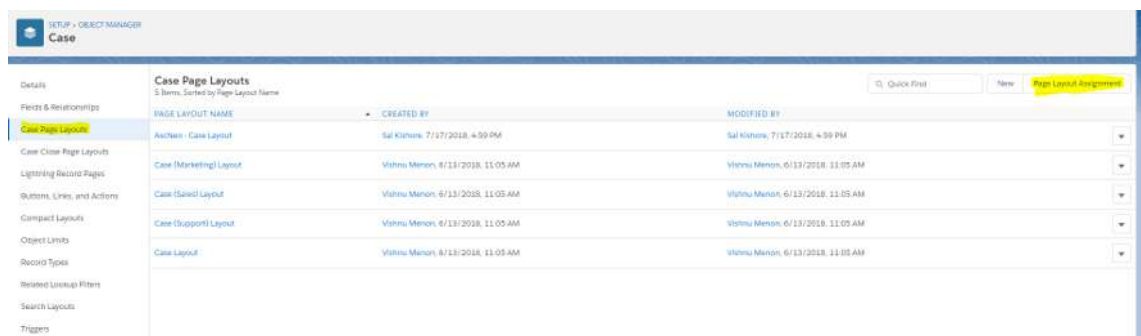


LABEL	API NAME	DESCRIPTION	LAST MODIFIED	DEPLOYED	CUSTOM
Account	Account				
Activity	Activity				
ASCConfiguration	asc_config__c		17/7/2018	✓	✓
Asset	Asset				
Asset Relationship	AssetRelationship				
Campaign	Campaign				
Campaign Member	CampaignMember				
Case	Case				
CleverReach Account	CleverReachApp__CRMAccount__c		14/6/2018	✓	✓
CleverReach Campaign Email Report	CleverReachApp__CEReport__c	Object to track emails sent from CleverReach	14/6/2018	✓	✓
CleverReach Intergroup Field	CleverReachApp__CIGroupAttribute__c	Group attributes appear in all CleverReach campaigns	14/6/2018	✓	✓
CleverReach Log	CleverReachApp__CLog__c		14/6/2018	✓	✓
CleverReach Mandatory Field	CleverReachApp__MandatoryField__c	Default values for leads and campaign members mandatory fields	14/6/2018	✓	✓
Contact	Contact				
Content Version	ContentVersion				
Contract	Contract				
CR Email Receiver	CleverReachApp__CR_Email_Receiver__c		14/6/2018	✓	✓

Fig. 47: Object Manager - Case

3. Select the menu item *Case Page Layouts* in the navigation bar.

⇒ A list with *page layouts* appears.



WIDE LAYOUT NAME	CREATED BY	MODIFIED BY
AvCen - Case Layout	Sal Kishore, 7/17/2018, 4:59 PM	Sal Kishore, 7/17/2018, 4:59 PM
Case (Marketing) Layout	Vishnu Menon, 6/13/2018, 11:05 AM	Vishnu Menon, 6/13/2018, 11:05 AM
Case (Sales) Layout	Vishnu Menon, 6/13/2018, 11:05 AM	Vishnu Menon, 6/13/2018, 11:05 AM
Case (Support) Layout	Vishnu Menon, 6/13/2018, 11:05 AM	Vishnu Menon, 6/13/2018, 11:05 AM
Case Layout	Vishnu Menon, 6/13/2018, 11:05 AM	Vishnu Menon, 6/13/2018, 11:05 AM

Fig. 48: Case - page layouts - assign page layouts

4. Click on the button *Page Layout Assignment* in the top right corner.

⇒ The list displays the already assigned page layouts.

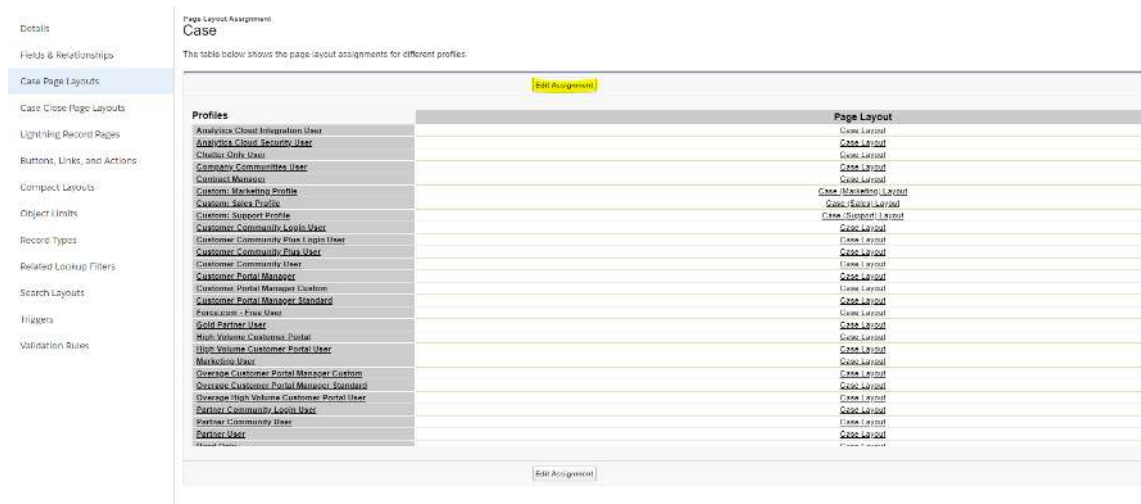


Fig. 49: Page layouts - Edit Assignment

5. Click on the button *Edit Assignment*.
 ⇒ A list containing profiles appears.

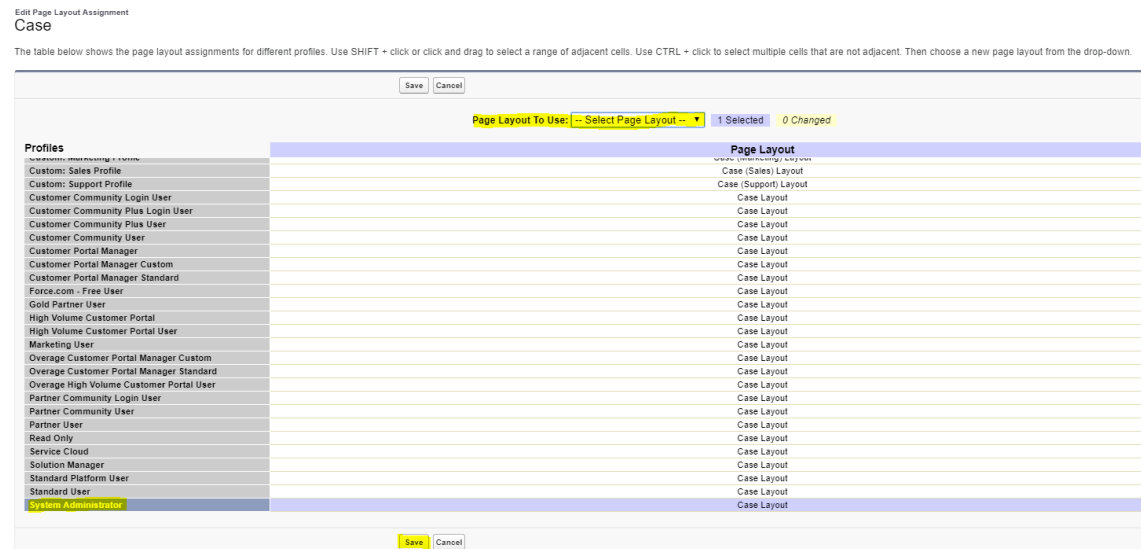



Fig. 50: Assign page layout

6. Select the respective profile, e. g. System Administrator.
7. In the drop-down list, select the page layout which is supposed to be used.
8. Click on the button *Save*.
 ⇒ The profile and the page layout of the user now appear in the list.

5.2.3 Configure ASC User Management

1. Click on the icon for all applications  in the task bar in the top right corner.
2. The window *App Launcher* opens.

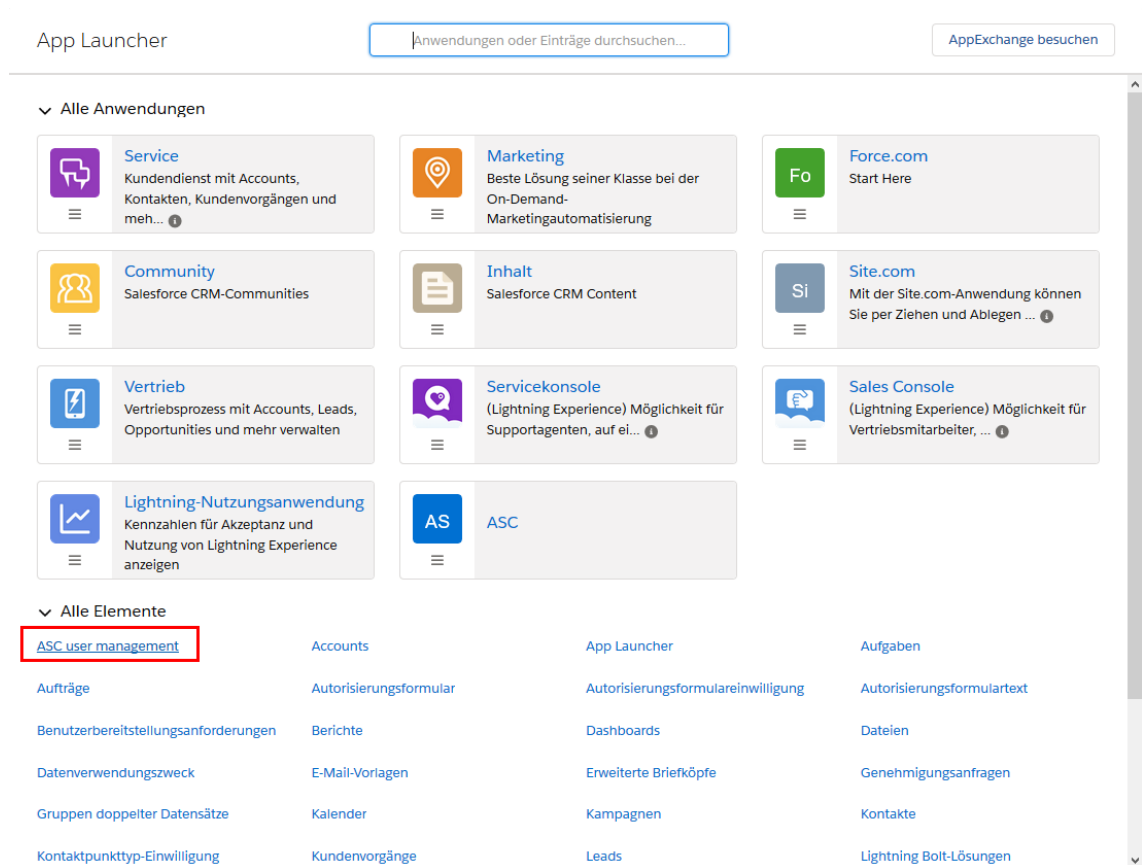


Fig. 51: App Launcher - Call up ASC User Management

3. In the group field *Alle Elemente* (all elements), click on the menu item *ASC user management*.

⇒ The following window appears:

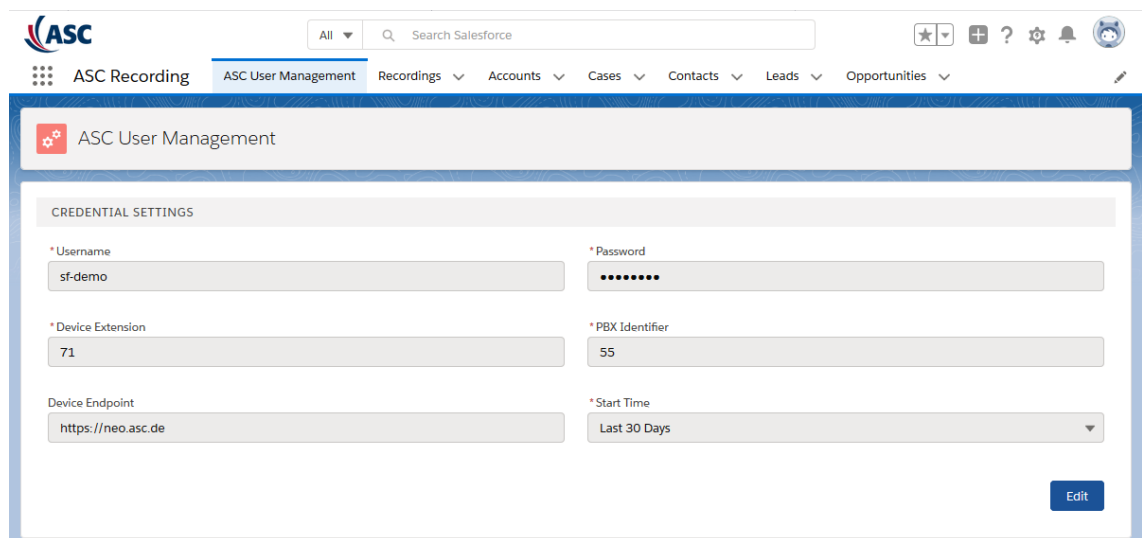


Fig. 52: Configure ASC User Management

4. Click on the button *Edit* to edit the parameters.
5. Enter the following parameters:

Username	Enter the user name of the tenant for which the Salesforce integration has been set up on the server.
Password	Enter the password to access the ASC recording server.

<i>Device Extension</i>	Enter the extension of the recording server.
<i>PBX Identifier</i>	Enter the PBX Identifier which has been configured for the recording server in the ASC application System Configuration in the PHONEapp module, see chapter "Tab PHONEapp Configuration" , p. 20.
<i>Device Endpoint</i>	Enter the URL which allows calling up the application. You can use the IP address or an DNS name, e. g. <code>//www.neo.asc.de</code> .
<i>Start Time</i>	Enter the period of time from which you would like to display conversations from the application.



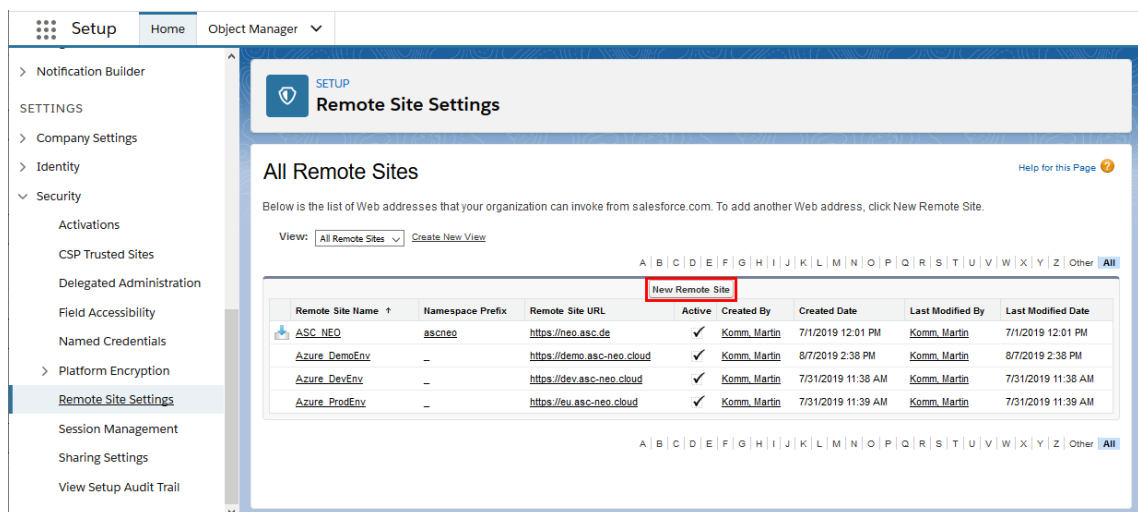
The *neo* system requires a signed [SSL](#) certificate from a root certifying authority; otherwise it will not be possible to establish a connection between Salesforce and the recording server. The operator of the *neo* must have the certificate issued for the respective DNS name and install it on the recording server with the certificate import tool. The DNS name for the *neo* system for which the certificate has been issued must be used as an end device in the Salesforce configuration.

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

5.2.4 Configure remote site settings

To enable Salesforce to access the recording server, you must configure the remote site settings in the Salesforce app.

- Within the icon *Settings* in the top right corner, select the menu item *Setup*.
- Search for *Remote site*
⇒ The window *All Remote Sites* opens.



Remote Site Name	Namespace Prefix	Remote Site URL	Active	Created By	Created Date	Last Modified By	Last Modified Date
ASC_NEO	ascneo	https://neo.asc.de	✓	Komm. Martin	7/1/2019 12:01 PM	Komm. Martin	7/1/2019 12:01 PM
Azure_DemoEnv	-	https://demo.asc-neo.cloud	✓	Komm. Martin	8/7/2019 2:38 PM	Komm. Martin	8/7/2019 2:38 PM
Azure_DevEnv	-	https://dev.asc-neo.cloud	✓	Komm. Martin	7/31/2019 11:38 AM	Komm. Martin	7/31/2019 11:38 AM
Azure_ProdEnv	-	https://eu.asc-neo.cloud	✓	Komm. Martin	7/31/2019 11:39 AM	Komm. Martin	7/31/2019 11:39 AM

Fig. 53: All remote sites

- Click on the button *New Remote Site*.
⇒ The window *Remote Sites Details* opens.

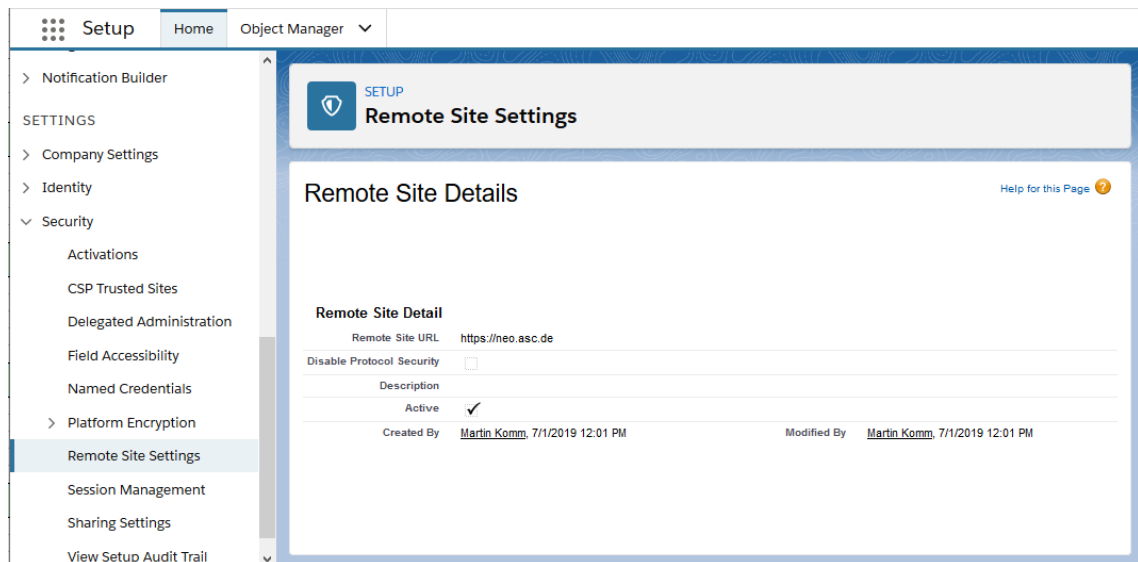


Fig. 54: Configure remote site

4. Enter the following parameters

Remote Site URL	Enter the URL of the recording server.
Description	You can enter an optional description.
Active	<p>This parameter allows activating or deactivating the connection.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> activated <input type="checkbox"/> deactivated <p>Activate the check box if the connection for this recording server is supposed to be activated.</p>

List of figures

Fig. 1	Download application via App Exchange	7
Fig. 2	Certificate Import Tool	8
Fig. 3	Import X.509	8
Fig. 4	Enter password for the private key	8
Fig. 5	Message - Successful import	9
Fig. 6	Check currently valid HTTPS certificate	9
Fig. 7	Import PKCS12 Keystore	10
Fig. 8	Confirm alias	10
Fig. 9	Enter password for PKCS12 Keystore	10
Fig. 10	Check currently valid HTTPS certificate	11
Fig. 11	System Configuration - web interface	12
Fig. 12	System Configuration - main view:	13
Fig. 13	Web service functionalities for the tenant	14
Fig. 14	Select export server	15
Fig. 15	Employees module - main view	16
Fig. 16	Configure user API as superuser	16
Fig. 17	Tenants - main view - tab Extensions	17
Fig. 18	Assign extensions to tenants	18
Fig. 19	Remove extensions	19
Fig. 20	Select extensions	20
Fig. 21	Create new PBX	20
Fig. 22	Activate PHONEapp configuration	21
Fig. 23	PHONEapp - main view:	21
Fig. 24	Detail view Default settings	22
Fig. 25	Group field General	22
Fig. 26	Setup - Phones	23
Fig. 27	Tab Details (example)	24
Fig. 28	Additional Data module - main view	25
Fig. 29	Configure additional data	26
Fig. 30	Group field Change display name	26
Fig. 31	Group field Availability	27
Fig. 32	Recording Planner - main view	27
Fig. 33	Create new profile	28
Fig. 34	Configure parameters for the recording profile	28
Fig. 35	Create action node	29
Fig. 36	Enter parameters for the action node	30
Fig. 37	Replace action node	31
Fig. 38	Action node - KSK start	31
Fig. 39	Activate recording profile	32
Fig. 40	Applications module - main view	32
Fig. 41	Configure general settings for the connection to the Salesforce app	33

Fig. 42	Setup - user - permission sets	34
Fig. 43	Permission sets - Manage Assignments	34
Fig. 44	Permission sets - Add Assignments.....	34
Fig. 45	Add Assignments	34
Fig. 46	Assigned permission	35
Fig. 47	Object Manager - Case	35
Fig. 48	Case - page layouts - assign page layouts	35
Fig. 49	Page layouts - Edit Assignment	36
Fig. 50	Assign page layout.....	36
Fig. 51	App Launcher - Call up ASC User Management	37
Fig. 52	Configure ASC User Management.....	37
Fig. 53	All remote sites.....	38
Fig. 54	Configure remote site.....	39

List of tables

Tab. 1	ASC licenses	6
Tab. 2	Login data - system provider	12

Glossary

API

Application Programming Interface

CTI

Computer Telephony Integration

PBX

Private Branch Exchange

SSL

Secure Socket Layer

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)