

Deployment Guide

Release 2303 – March 2023

maiConnect
for SAP S4/HANA®

cxAddOns



Global AddOn specialist for Enterprise Software.

Table of contents

1	System landscape	3
2	Deployment steps	4
2.1	Synchronization checklist.....	6
3	Cloud Connector Setup	7
3.1	Download & Installation.....	7
3.2	First steps after installation.....	7
3.3	Adding a subaccount.....	7
3.4	System Mapping.....	9
3.5	Determination of resources	11
3.6	Providing communication information	12
4	SAP System Settings	13
4.1	Communication User	13
4.2	Activating the required OData Services	13
4.3	Define activity types	15
4.4	Activate & assign events	16
4.5	Setting up the RFC connection	17
4.6	Customizing for the Synchronization of Contacts	20
5	Exchange Server Settings	25
5.1	Enable EWS and local authentication	25
5.1.1	Local Exchange Server.....	25
5.1.2	Office 365.....	25
5.2	Setting up mailbox access.....	26
5.2.1	Dedicated service user	26
5.2.2	Authorization via OAuth (Office 365)	28
5.2.3	Note about the Azure API permissions.....	36
5.3	Exchange Throttling Policy.....	37
5.4	Connection between Exchange and SAP BTP	38
6	List of Figures	40

1 System landscape

maiConnect@S4 is hosted on the SAP Business Technology Platform (SAP BTP). For data exchange between SAP S/4HANA onPrem and Microsoft Exchange (incl. Office 365), it uses the standard SAP and Microsoft interfaces.

Communication from SAP S/4HANA to SAP BTP is done via an RFC connection. If an object is created/changed/deleted in SAP S/4HANA, an event is triggered and a customized maiConnect@Cloud URL is called.

From the direction of SAP BTP, maiConnect communicates with standard OData services via a SAP cloud connector. Additional OData services required by maiConnect are imported into the S/4HANA system via a transport.

The user also communicates with the Microsoft Exchange Server via the Microsoft Outlook Client and thus receives all appointments, tasks and contacts.

Due to the direct communication of maiConnect@S4 with the Microsoft Exchange Server, it is also possible that appointments, tasks and contacts are made available directly on all Exchange-compatible end devices such as iPhone or tablet.

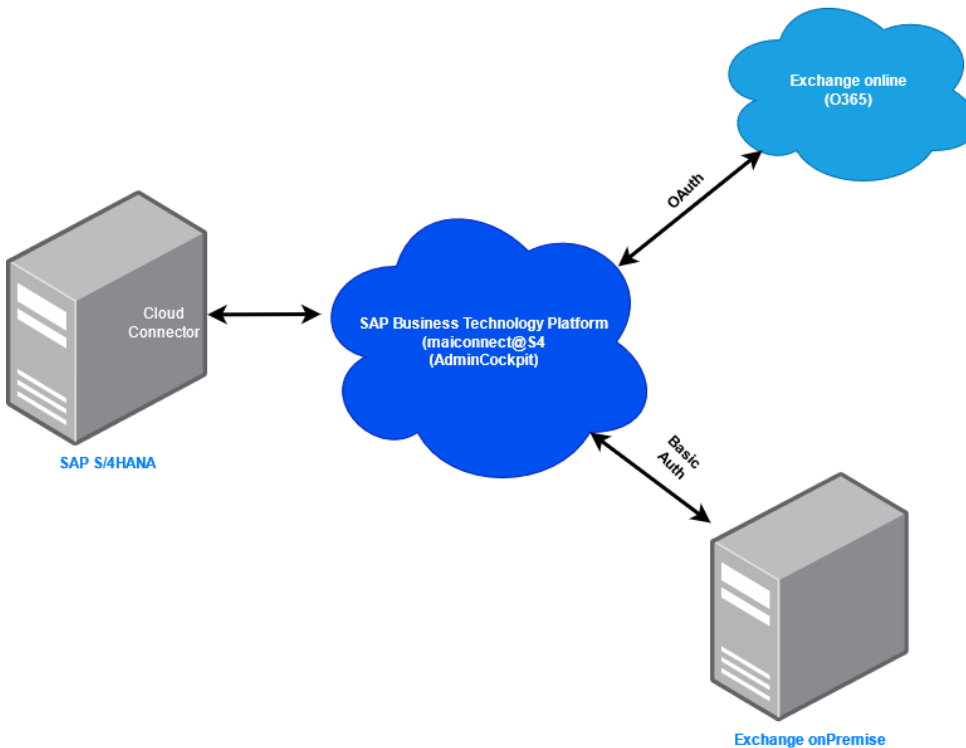


Figure 1: System landscape

2 Deployment steps

This chapter describes the basic steps for a maiConnect@S4 deployment. Here is an overview of the individual steps and their sequence.

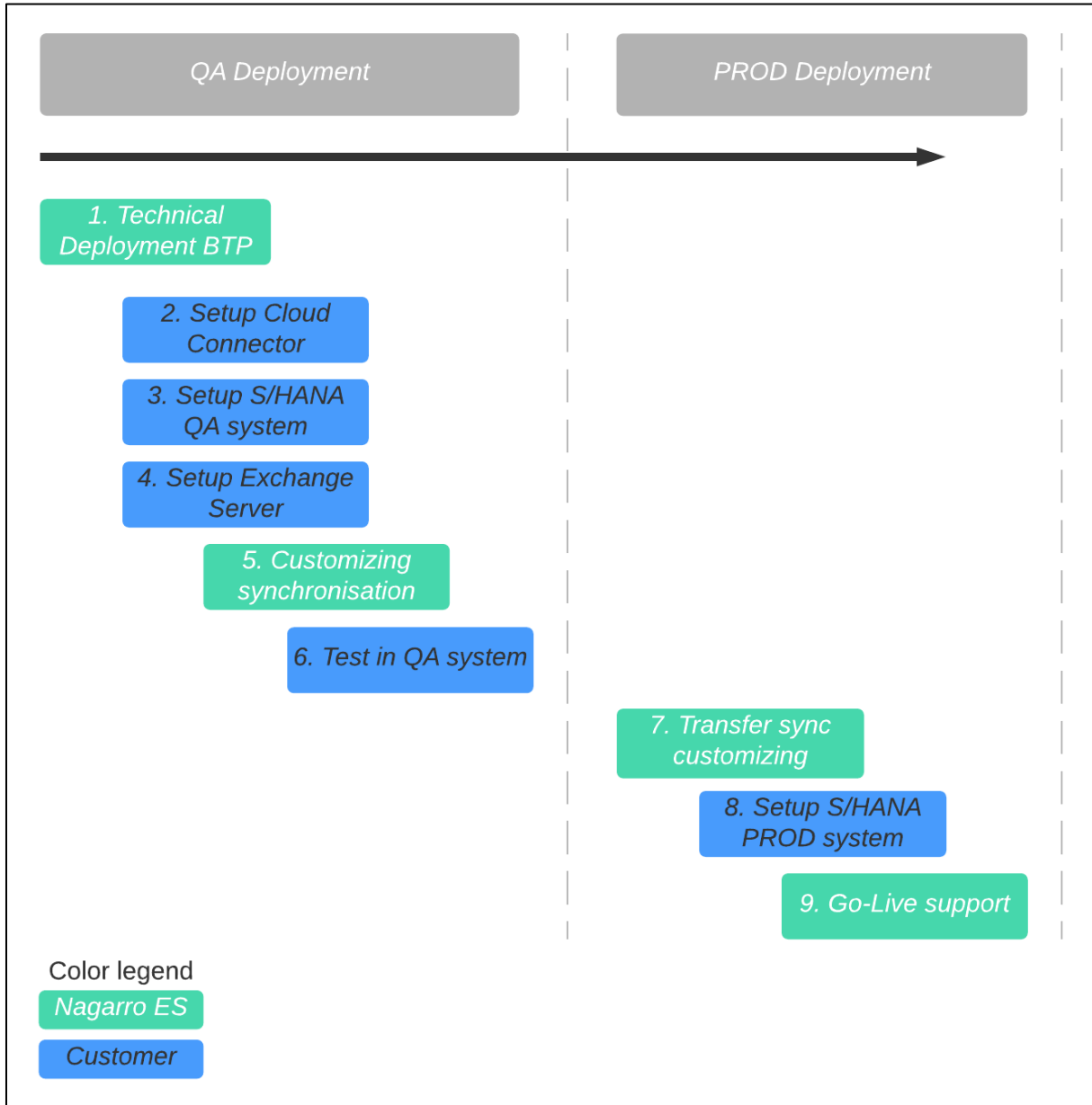


Figure 2: Deployment sequence

What needs to be done in each step is further explained here. In the following chapters you will find a detailed description for each step.

- maiConnect application is hosted on SAP BTP. The technical deployment required there for the QA and PROD environment is done by Nagarro ES.
 This step results in the subaccount IDs for the Cloud Connector.
- The setup of the SAP Cloud Connector for the QA and PROD environment is performed in the customer's system landscape. Since this requires network access, this setup must be done by the customer. If Nagarro ES is granted network access via VPN or similar, this step can also be done by Nagarro ES. This setup is described in chapter 3.

To establish communication between the systems, Nagarro ES has to be provided with different information. Please refer to chapter 3.6.

3. Various setups need to be made in the SAP S/4HANA system. Again, this setup must be done by the customer and can only be done by Nagarro ES if network access is provided.

In addition to the technical setup, the customer's business department must define which transaction types can be used for synchronization. See chapter 4.3.

For the setup of the RFC connection Nagarro ES provides the URL to the maiConnect system. See chapter 4.5.

4. The setup of the Exchange Server has to be done by the customer. This is described in chapter 5. Depending on what kind of Exchange Server is used by the customer, either the setup for an Exchange onPrem (chapter 5.2.1) or Office 365 (chapter 5.2.2) has to be done.

In principle, however, maiConnect also supports multiple Exchange environments. This is relevant, for example, if maiConnect is to be used in different countries that have their own Exchange server.

5. If the steps up to here have been done, then the synchronization can be set up. This is done at a meeting with Nagarro ES and colleagues from the customer's business department. During this meeting the synchronization can be tested. The prerequisite for this is to provide a S/4HANA sample user who has a valid email inbox.

Please review the synchronisation checklist below prior to this meeting.

In addition, one or more persons responsible for the administration of maiConnect must be named by the customer. The AdminCockpit settings will then be trained at another meeting.

6. At this step the customer has the possibility to test the synchronization. Any changes to the synchronization settings can be made.
7. Before go-live, Nagarro ES transfers the administration settings to the PROD system. This ensures that the settings are identical in the QA and PROD systems at this time.
8. In this step, the settings in the S/4 system are transferred from the customer to the productive S/4HANA system.
9. During go-live, the business users are added to the maiConnect AdminCockpit. Problems can be reported via maiConnect support at support@cxaddons.com.

2.1 Synchronization checklist

Appointments	
Which appointment transaction types should be synchronized from S/4HANA to Outlook?	
Should appointments be synchronized from Outlook to S/4HANA?	<input type="checkbox"/>
Should all Outlook appointments be synchronized? Or	<input type="checkbox"/> or
Should the synchronization be triggered for every appointment by setting a category or sync tag?	<input type="checkbox"/>
Synchronization of private appointments?	<input type="checkbox"/>
Synchronization of serial appointments from Outlook to S/4HANA?	<input type="checkbox"/>
Should appointment attachments be synchronized?	<input type="checkbox"/>
Which S/4HANA contact person and participant partner functions are relevant for synchronization? Default for contact persons: 00000015, default for participants: 00000032	
Tasks	
Should tasks be synchronized in general?	<input type="checkbox"/>
Which task transaction types should be synchronized from S/4HANA to Outlook?	
Should tasks be synchronized from Outlook to S/4HANA?	<input type="checkbox"/>
Should all Outlook tasks be synchronized? Or	<input type="checkbox"/> or
Should the synchronization be triggered by category or by sync tag?	<input type="checkbox"/>
Contacts	
Should contacts be synchronized from S/4HANA to Outlook?	<input type="checkbox"/>
Which S/4HANA relationship type is used for the relationships between customer and contact person? Default BUR001	
Should the synchronization be triggered by setting a relationship to the contact person? Which relationship type should be used for this? Default BUR011	<input type="checkbox"/>
Should the synchronization be triggered by setting a relationship to the customer? Which relationship type should be used for this? Default BUR011	<input type="checkbox"/>

3 Cloud Connector Setup

General information regarding the Cloud Connector (Prerequisites, Installation, ...) can be found here: <https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/e6c7616abb5710148cfc3e75d96d596.html>

3.1 Download & Installation

The Cloud Connector must be installed in the same system environment in which the S4 system is running. To do this, download the appropriate installation file from <https://tools.hana.ondemand.com/#cloud>, start the installation and follow the instructions of the installation wizard.

3.2 First steps after installation

Once the installation has been successfully completed, you can set up the Cloud Connector via URL <https://localhost:8443/> (replace the port 8443 accordingly if you specified a different port during the installation). The credentials for the first login can be found below:

User: administrator

Password: manage

Right after the first login you will have to change the initial password. If not specified otherwise, please select "Master" as the installation type:



Figure 3: Cloud Connector - Login

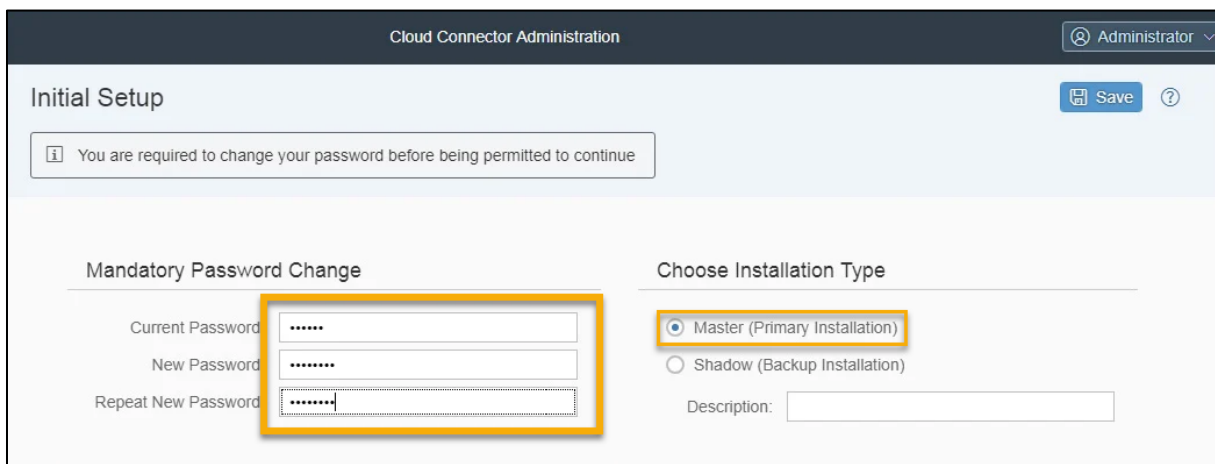


Figure 4: Cloud Connector – Changing the initial password & choosing the installation type

3.3 Adding a subaccount

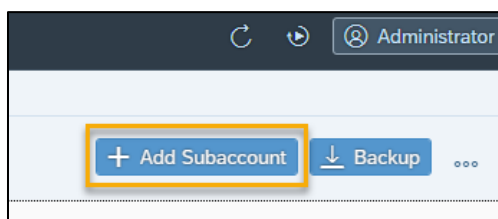
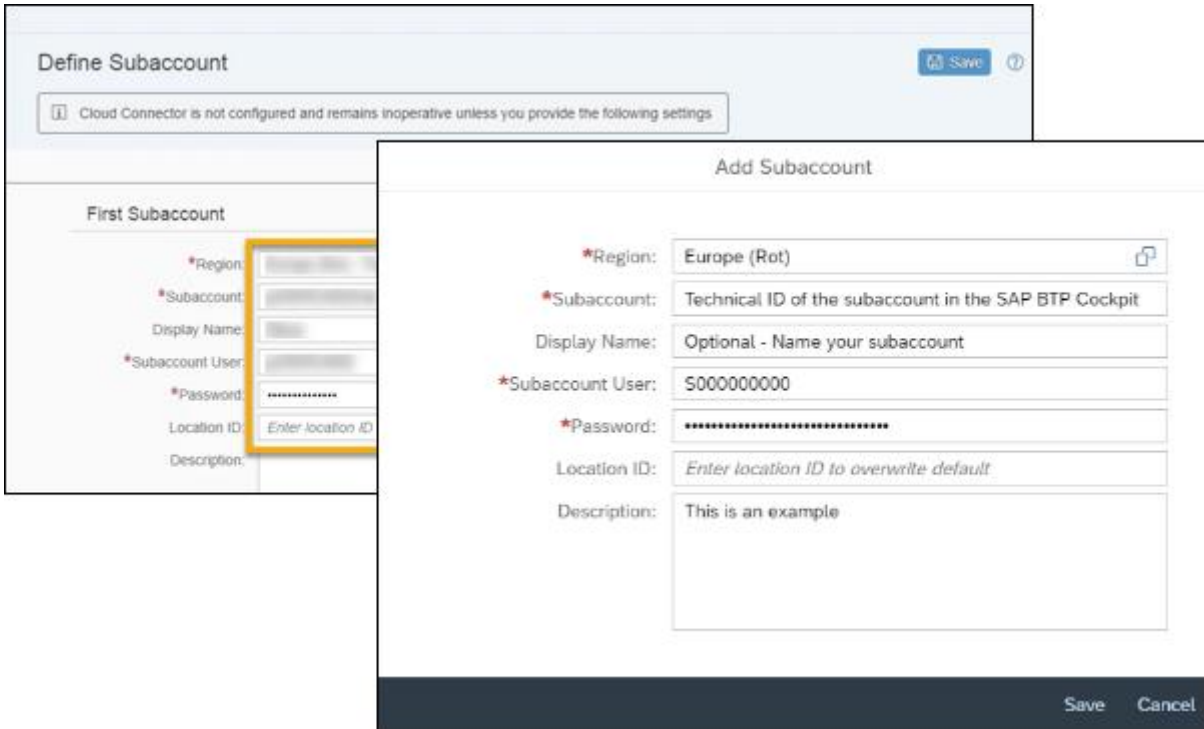


Figure 5: Cloud Connector – Adding subaccount

If you have just installed the Cloud Connector and are logging in for the first time, you should be automatically prompted to specify a subaccount in the next step. If not, you can add a subaccount using the "+ Add Subaccount" button in the upper right corner.

The individual fields are described in more detail below. Please note that the fields marked with a red asterisk (*) are mandatory fields:



The image shows two overlapping screenshots of the Cloud Connector interface. The top screenshot, titled 'Define Subaccount', shows a list of subaccounts under 'First Subaccount' with fields for Region, Subaccount, Display Name, Subaccount User, Password, Location ID, and Description. A yellow box highlights the 'Subaccount' field. The bottom screenshot, titled 'Add Subaccount', shows a form with the following fields:

- *Region:** Europe (Rot)
- *Subaccount:** Technical ID of the subaccount in the SAP BTP Cockpit
- Display Name:** Optional - Name your subaccount
- *Subaccount User:** S000000000
- *Password:** [Redacted]
- Location ID:** Enter location ID to overwrite default
- Description:** This is an example

 The form has 'Save' and 'Cancel' buttons at the bottom right.

Figure 6: Cloud Connector – Adding a subaccount

Region: Unless otherwise specified by Nagarro ES, please select the region *Europe (Rot)* here.

Subaccount: Enter the technical ID of the subaccount from the SAP BTP Cockpit. You will receive this from Nagarro ES.

Display Name: Optional field. If required, enter an internal name for the connected subaccount here.

Subaccount User: User ID of your P or S user.

Please note that the SAP does not support technical communication users in the Cloud Connector, instead a normal P-/S-User must be used.

Password: Password of the user entered above.

Location ID: Not relevant

Description: Optional. Enter a short description if required.

When you save your settings, the subaccount will be added and if everything went correctly, the following overview page will be displayed:

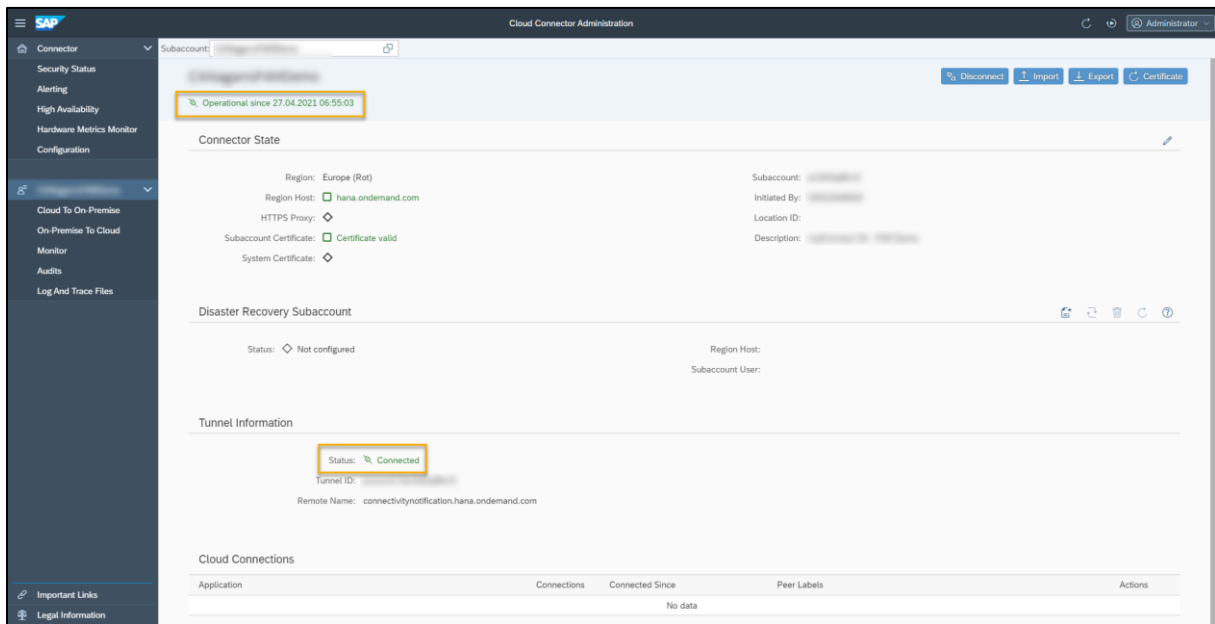


Figure 7: Cloud Connector – Subaccount successfully added

Please refer to this SAP note in case of http error 417:

<https://me.sap.com/notes/0002461997>

3.4 System Mapping

Now select the menu item “Cloud To On-Premise” for the subaccount you just added and add a system mapping via the “+” button.

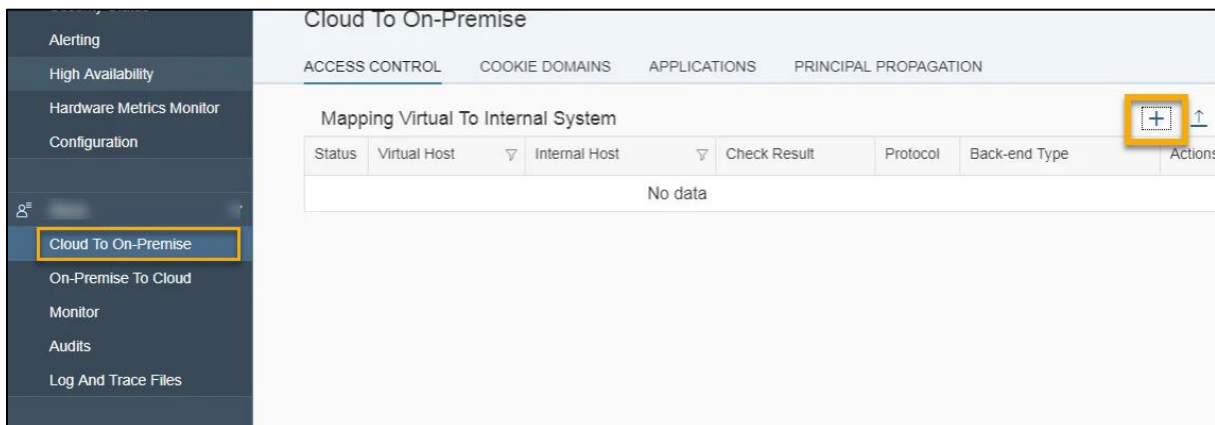


Figure 8: Cloud Connector – Cloud To On-Premise mapping

Now click through the dialog sequence and select the following values for the respective parameters:

- Back-end Type** : ABAP System
- Protocol** : HTTPS
- Internal Host, Internal Port** : URL / host name and HTTPS port of the S4 system
- Virtual Host, Virtual Port** : Virtual URL / host name und HTTPS port (freely selectable)
- Host in Request Header** : Use Virtual Host
- Principal Type** : None
- Description** : (Optional) Enter a description if required.

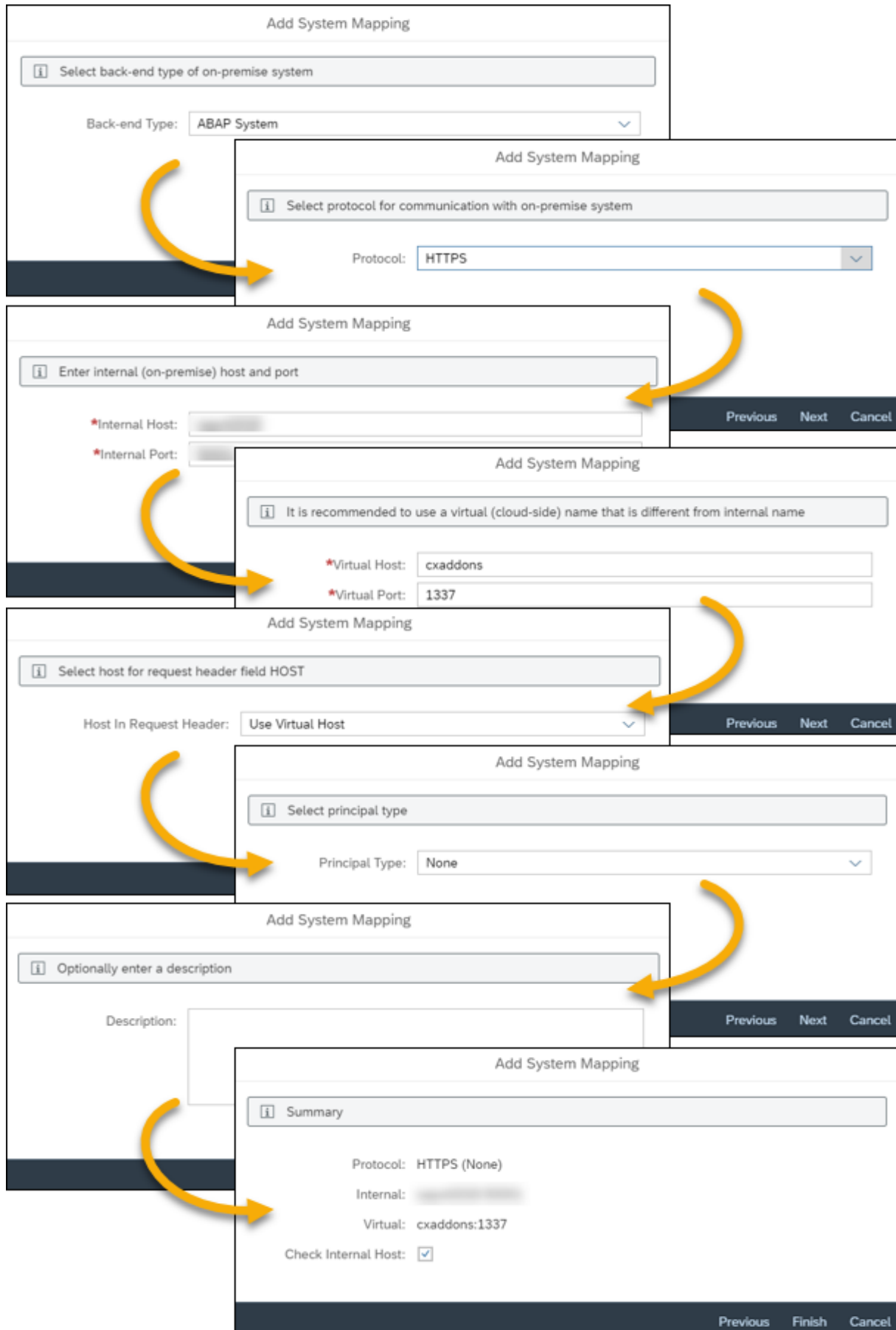


Figure 9: Cloud Connector – Settings for the system mapping

Confirm the previously made entries at the end and select "Check Internal Host" to test the connection directly when saving the mapping. Alternatively, you can also use the button marked on the right in the figure below:

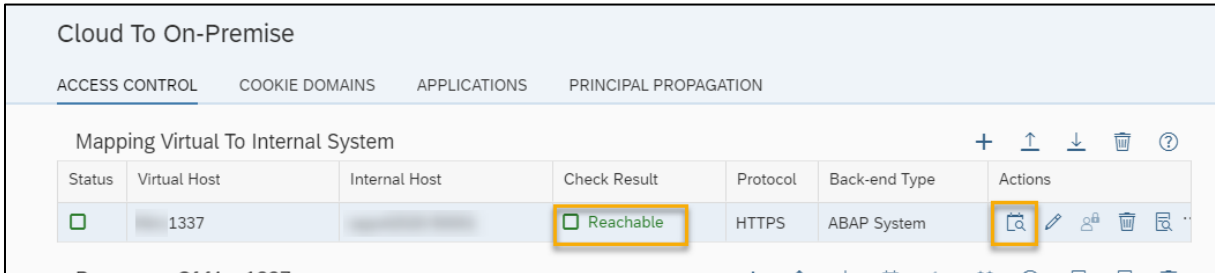


Figure 10: Cloud Connector – System mapping created successfully

3.5 Determination of resources

Next, the resources to which access is granted via the Cloud Connector must be specified.

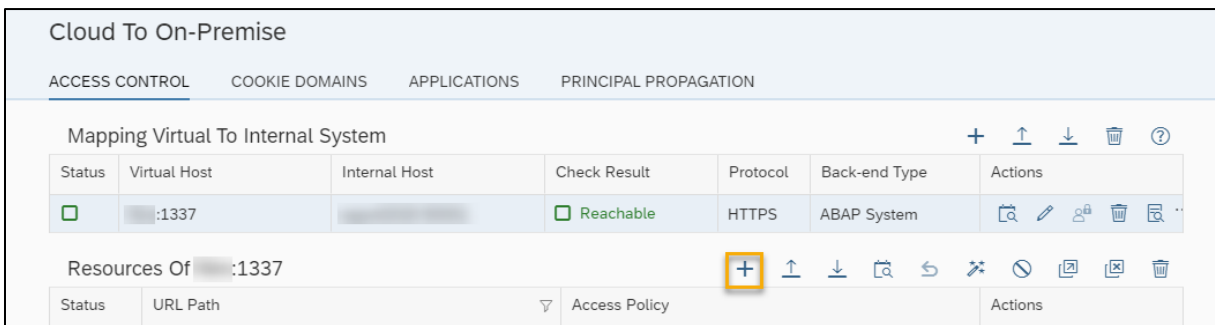


Figure 11: Cloud Connector - Resources

For maiConnect S4 access to the resource /sap/opu/odata is required. Add the following entry via the "+" button:

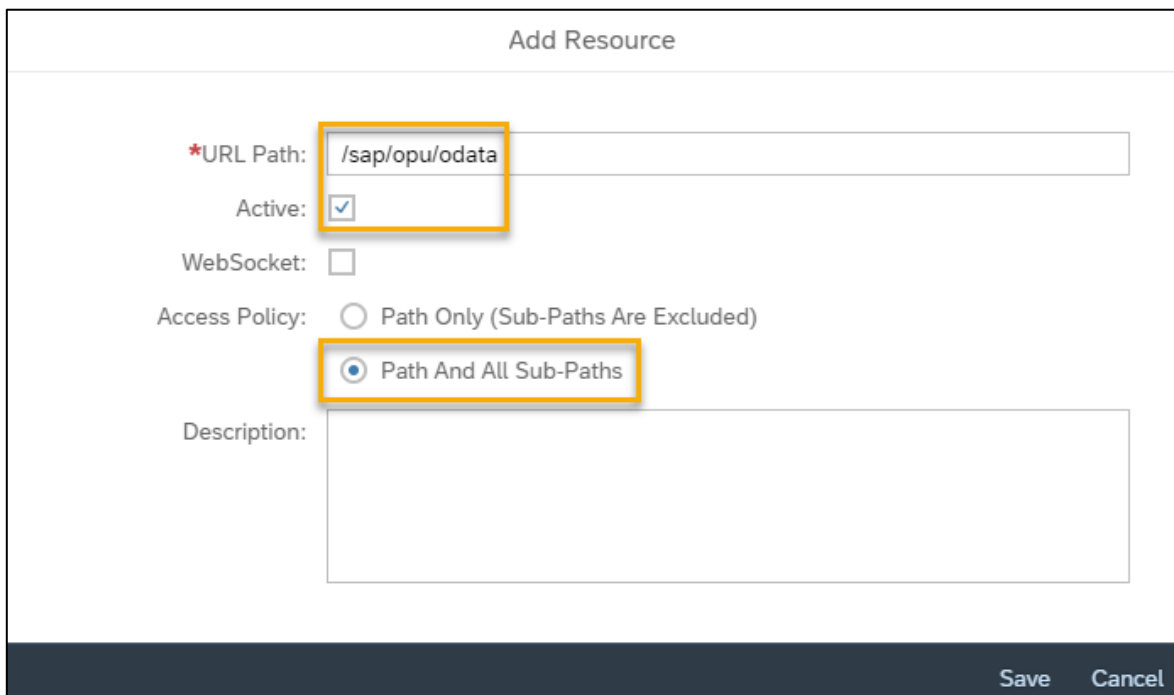


Figure 12: Cloud Connector – Add Resource

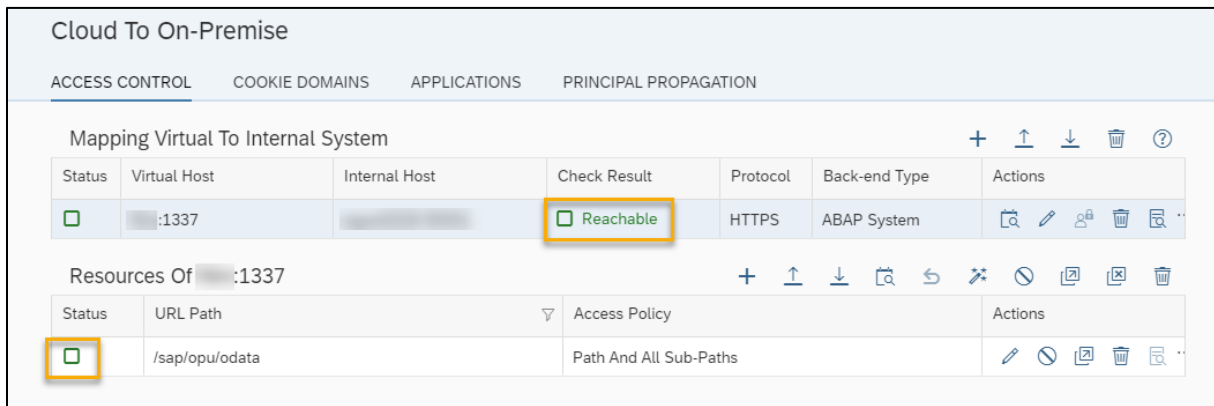



Figure 13: Cloud Connector – Resource maintained

After you have added the resource, the Cloud Connector setup is complete. The figure above shows how it should look like.

3.6 Providing communication information

 To be able to establish the connection, a destination must be created in the SAP BTP Cockpit. For this purpose, your Deployment Consultant of Nagarro ES needs the following data from you:

- Virtual Host, Virtual Port**
- SAP Client**
- SAP Communication User, Password**

See chapter 4.1 for further information about the communication user.

You are welcome to send us this data via email or text message - alternatively, we can organize a web session where you enter the data yourself via screen sharing. Just contact us at support@cxaddons.com to discuss how to proceed.

4 SAP System Settings

To continue with the setup and to perform the following changes / settings, you will receive a transport from Nagarro ES, which you must import.

4.1 Communication User

The maiConnect changes in the SAP system are carried out centrally by a system user (referred to as “communication user”). This user requires the appropriate authorizations to be able to display and change activities and business partners.

This user needs to have the type “System”. It is not necessary for this user to have the type “Dialog” user.

The provided transports contain a customizing transport that is used to create a separate role in the SAP system. This role contains all necessary permissions for the communication user.

The name of the role is:

- /NAG/SAP_MAICONNECT

4.2 Activating the required OData Services

The following OData Services need to be activated in the SAP system for maiConnect to work:

- /NAG/CRM_BUPA_ODATA_SRV
- /NAG/MAICONNECT_CONTPERS_CDS
- /NAG/MAICONNECT_EMPLOYEE_CDS
- /NAG/CRM_APPOINTMENT_SRV_01
- /NAG/MAI_CRM_TASK_SRV
- /NAG/PARTNER_ADDRESS_SEARCH_SRV

Execute transaction **/N/IWFND/MAINT_SERVICE**. If this transaction is not available, execute transaction **SE38** instead and run report **/IWFND/R_MGW_REGISTRATION**. Select the option „Add service“:

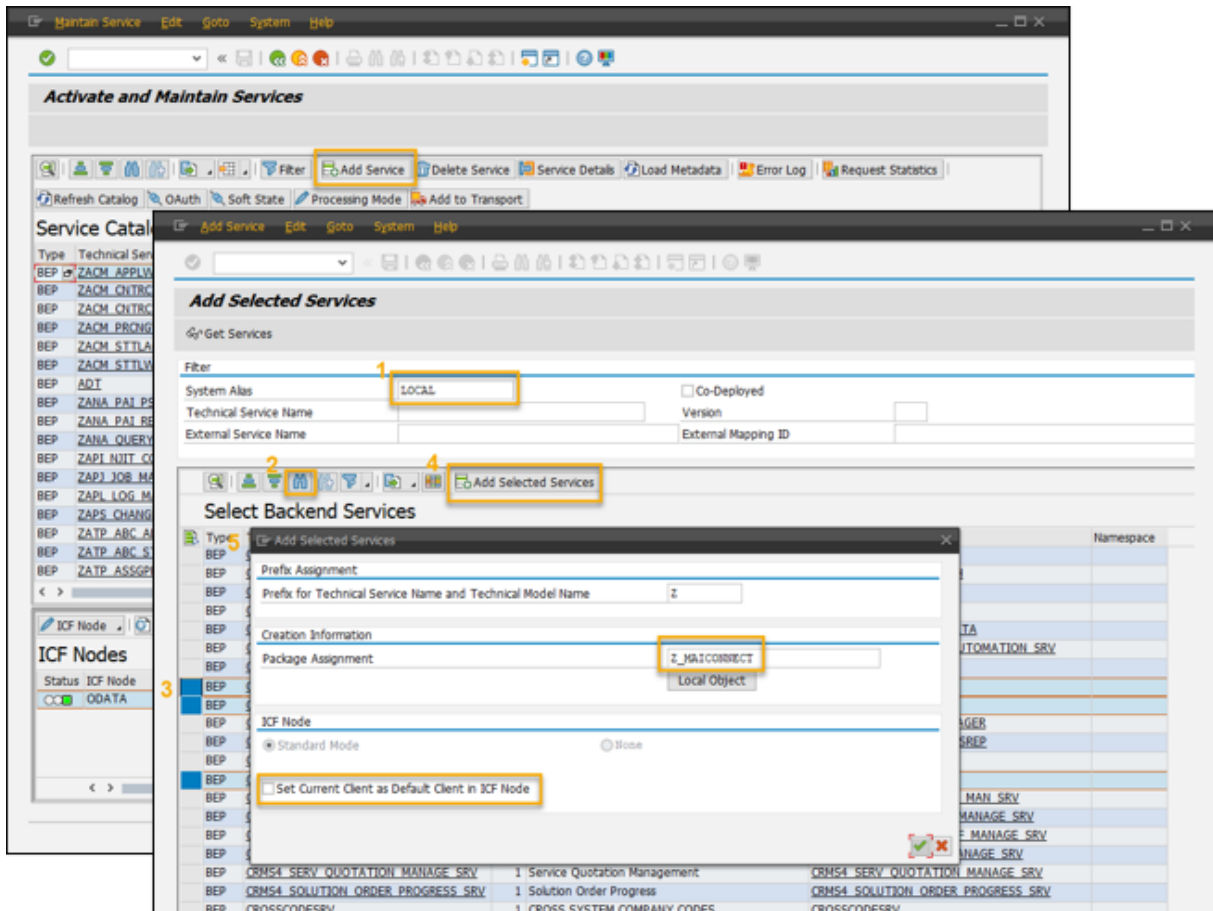


Figure 14: SAP – Adding OData Services

- (1) Enter „LOCAL“ as System Alias and confirm with <ENTER>
- (2) With the search you can quickly find the services you need
- (3) Mark the services
- (4) Add the services
- (5) Choose ‚Z‘ as prefix, assign the services to a package and confirm your entries

In the next step you need to save those changes to a transport.

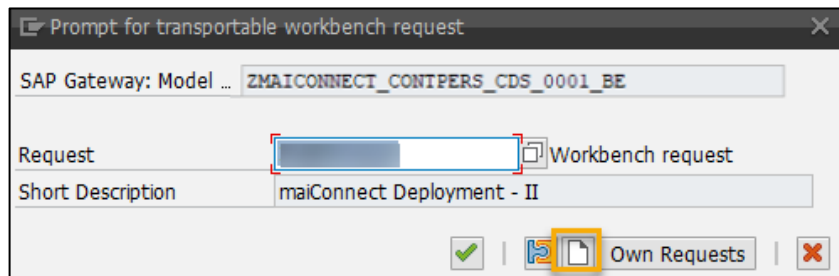
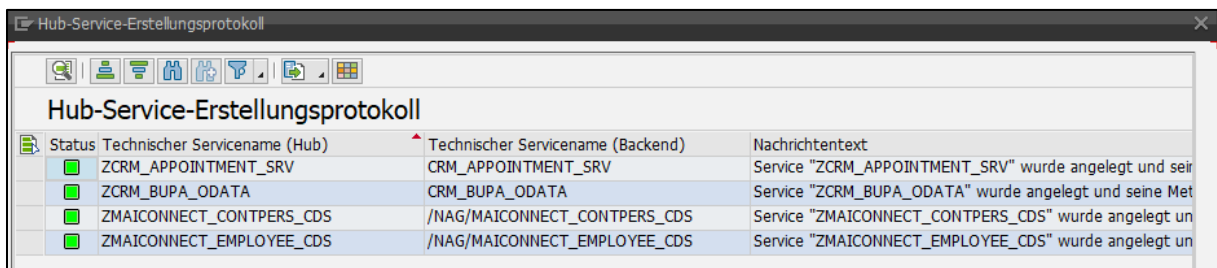


Figure 15: SAP – Adding the services to a transport



Status	Technischer Servicename (Hub)	Technischer Servicename (Backend)	Nachrichtentext
<input checked="" type="checkbox"/>	ZCRM_APPOINTMENT_SRV	CRM_APPOINTMENT_SRV	Service "ZCRM_APPOINTMENT_SRV" wurde angelegt und sein
<input checked="" type="checkbox"/>	ZCRM_BUPA_ODATA	CRM_BUPA_ODATA	Service "ZCRM_BUPA_ODATA" wurde angelegt und seine Met
<input checked="" type="checkbox"/>	ZMAICONNECT_CONTPERS_CDS	/NAG/MAICONNECT_CONTPERS_CDS	Service "ZMAICONNECT_CONTPERS_CDS" wurde angelegt un
<input checked="" type="checkbox"/>	ZMAICONNECT_EMPLOYEE_CDS	/NAG/MAICONNECT_EMPLOYEE_CDS	Service "ZMAICONNECT_EMPLOYEE_CDS" wurde angelegt un

Figure 16: SAP – Overview of activated services (here in German)

After this you need to assign those 6 OData services the system alias “LOCAL” via **SPRO**:

SAP NetWeaver > SAP Gateway > OData Channel > Administration > General Settings > Assign SAP-System Aliases to OData Service

(https://help.sap.com/saphelp_em92/helpdata/en/9d/f4ff5082d2793ee10000000a423f68/content.htm)

4.3 Define activity types

All activity types for which appointments or tasks are to be synchronized in the direction of Exchange must be maintained in the respective table through transaction SM30. The text type is particularly important here. This is the text that is then displayed in the note field of the respective Outlook appointment.

Execute transaction **SM30** and display the respective table. You can then create a new entry here for each relevant activity type.

Appointments: CRMV_APPT_OD

Tasks: CRMV_TASK_OD

Please make sure to add only process types of bus type 2000126 for appointments - and only process types of bus type 2000125 for tasks.

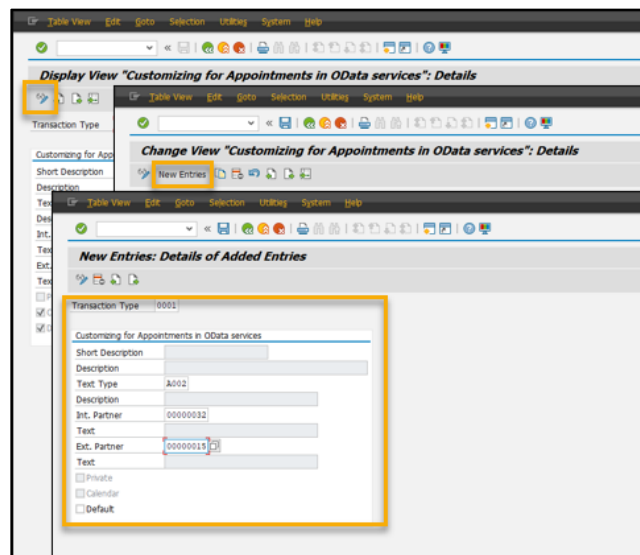


Figure 17: SAP – Define activity types

4.4 Activate & assign events

Execute transaction SM30 and open the table CRMV_FUNC_ASSIGN for maintenance. Please create an entry exactly as shown in the picture below:

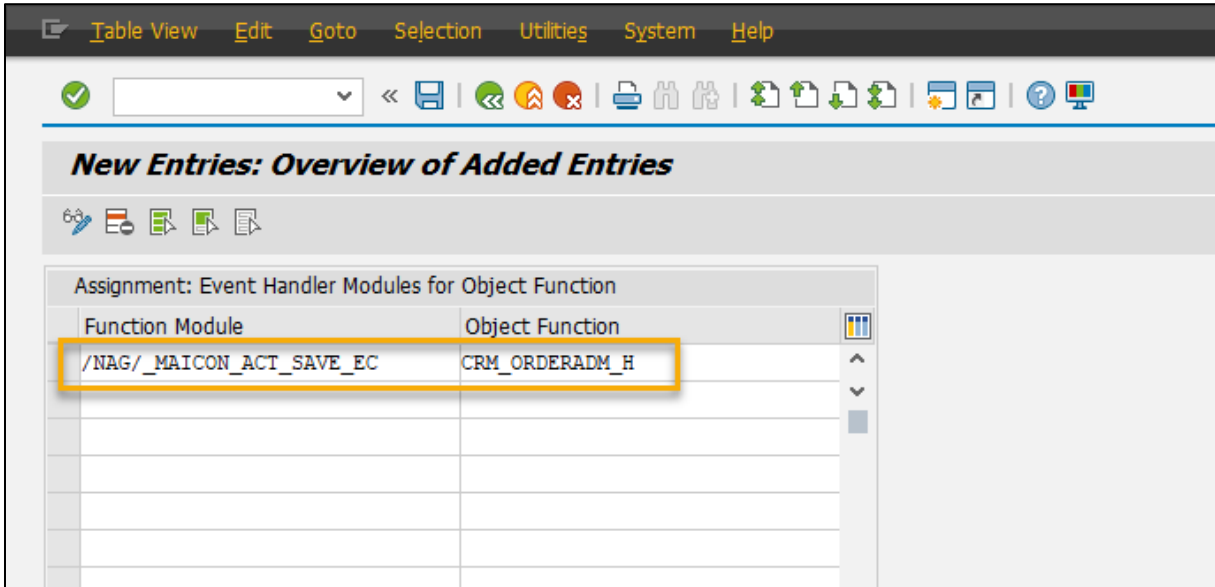


Figure 18: SAP – Event Handler Module Assignment

Confirm the entry with <Enter> and add the changes to a transport request. Then execute transaction CRMV_EVENT, click the "Callback for Cat./Obj./Event" button, switch to edit mode and add a new entry.

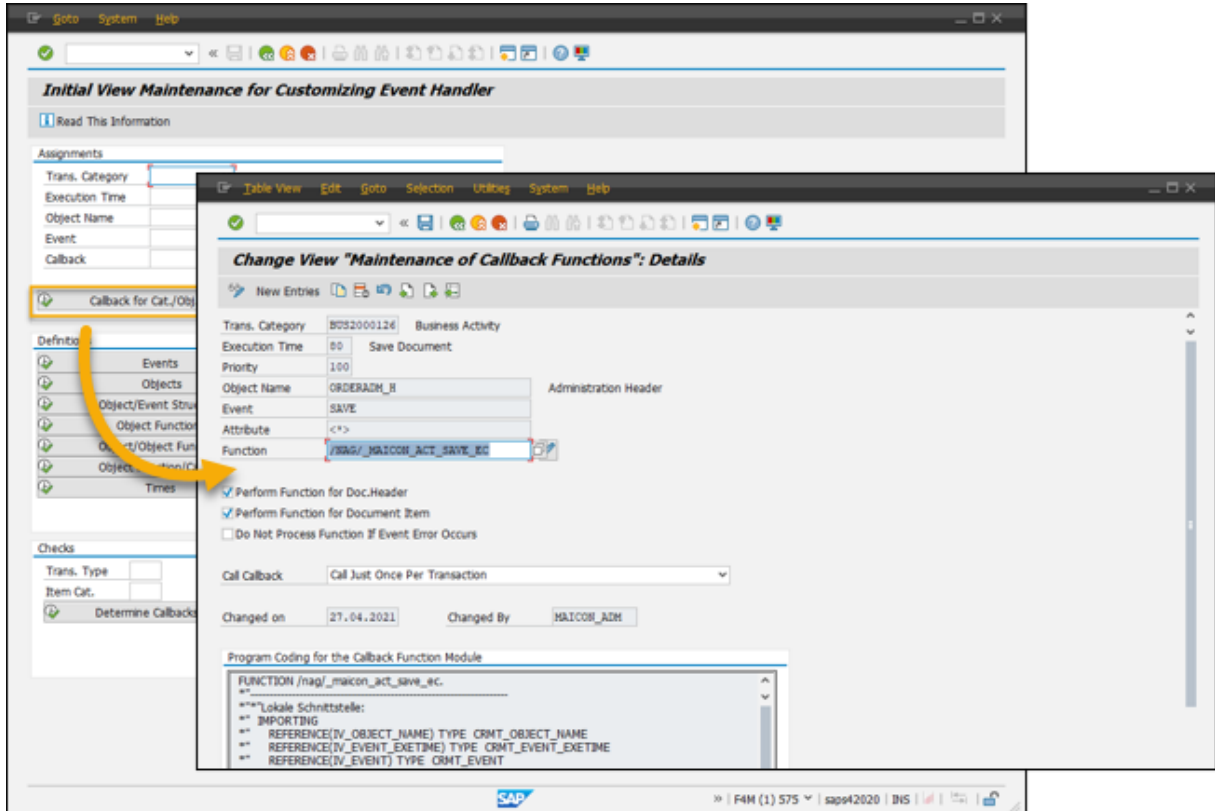


Figure 19: SAP – Adding an event

4.5 Setting up the RFC connection

Execute transaction **SM59** and create a new HTTP Connection to External Server. This is the maiConnect connection to the SAP BTP.

Open the created connection, switch to the "Technical Settings" tab and enter the host you received from Nagarro ES (ending in ...hana.ondemand.com). As port please enter **443** – the path prefix can be left blank.

If you are using a proxy, please enter the corresponding data here as well.

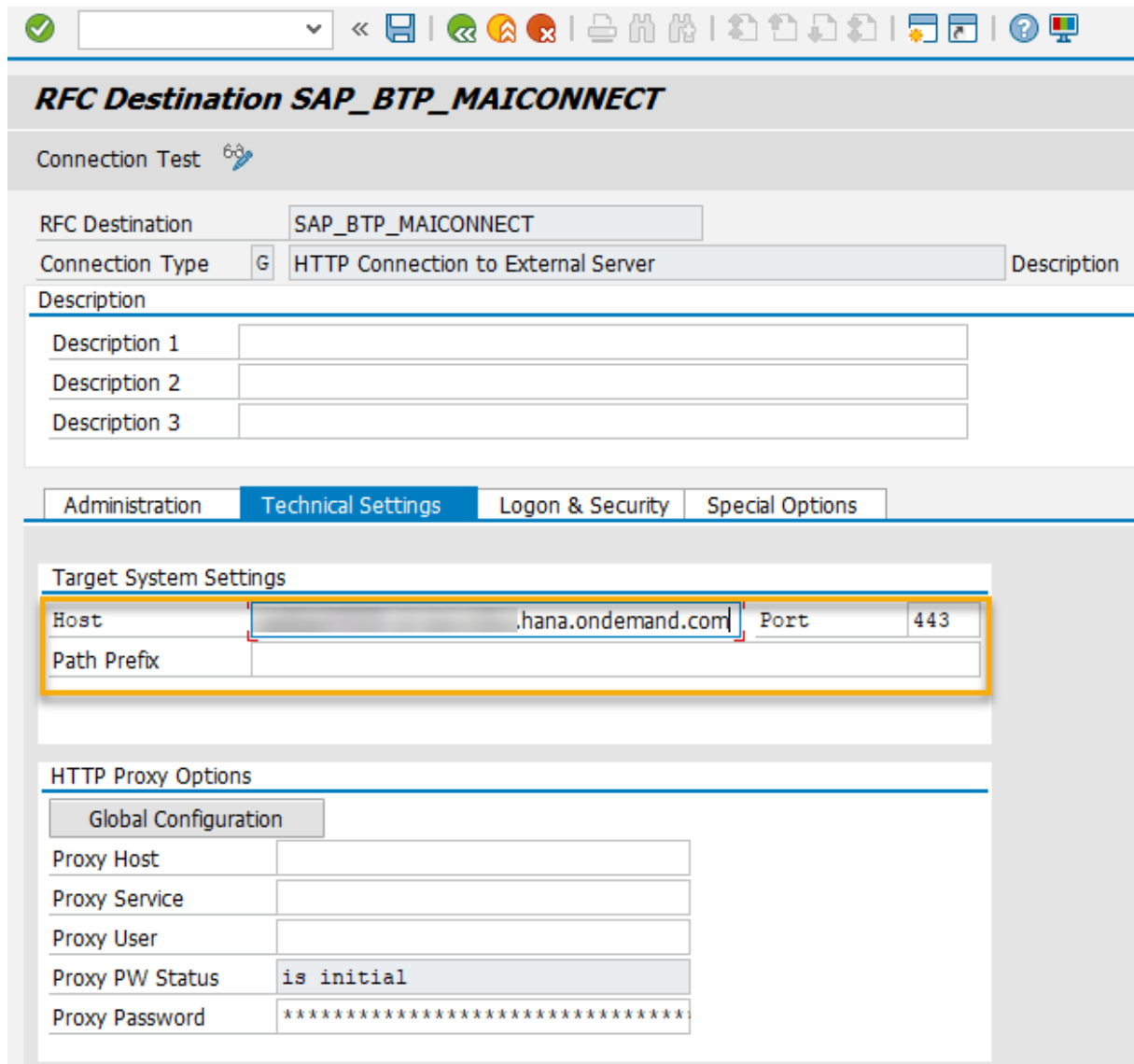
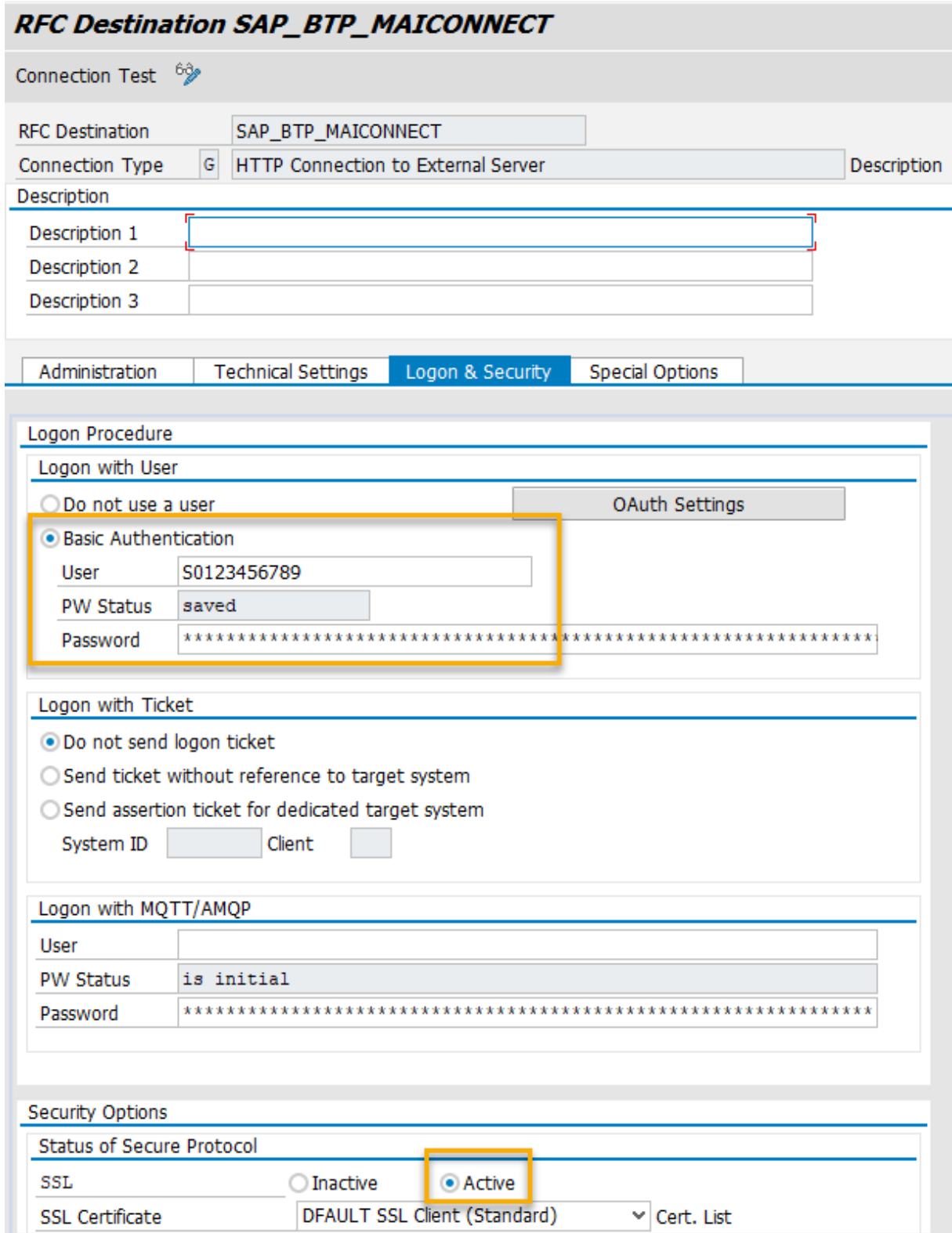



Figure 20: SAP – RFC Connection – Technical Settings

Now switch to the tab “Logon & Security”, enter the P- or S-User for basic authentication (use the same user as for the setup of the Cloud Connector (chapter 3.3) and activate SSL:



RFC Destination SAP_BTP_MAICONNECT

Connection Test 

RFC Destination: SAP_BTP_MAICONNECT

Connection Type: G HTTP Connection to External Server Description

Description

Description 1	
Description 2	
Description 3	

Administration | Technical Settings | **Logon & Security** | Special Options

Logon Procedure

Logon with User

Do not use a user OAuth Settings

Basic Authentication

User: S0123456789

PW Status: saved

Password: *****

Logon with Ticket

Do not send logon ticket

Send ticket without reference to target system

Send assertion ticket for dedicated target system

System ID: Client:

Logon with MQTT/AMQP

User:

PW Status: is initial

Password: *****

Security Options

Status of Secure Protocol

SSL: Inactive **Active**

SSL Certificate: DEFAULT SSL Client (Standard) Cert. List

Figure 21: SAP – RFC connection – Logon & Security

After this, you can start a connection test.

Execute transaction **SM30** once more and open the table `/NAG/MAICONDESTI`. Please create an entry with the name of the previously created RFC connection and save it:

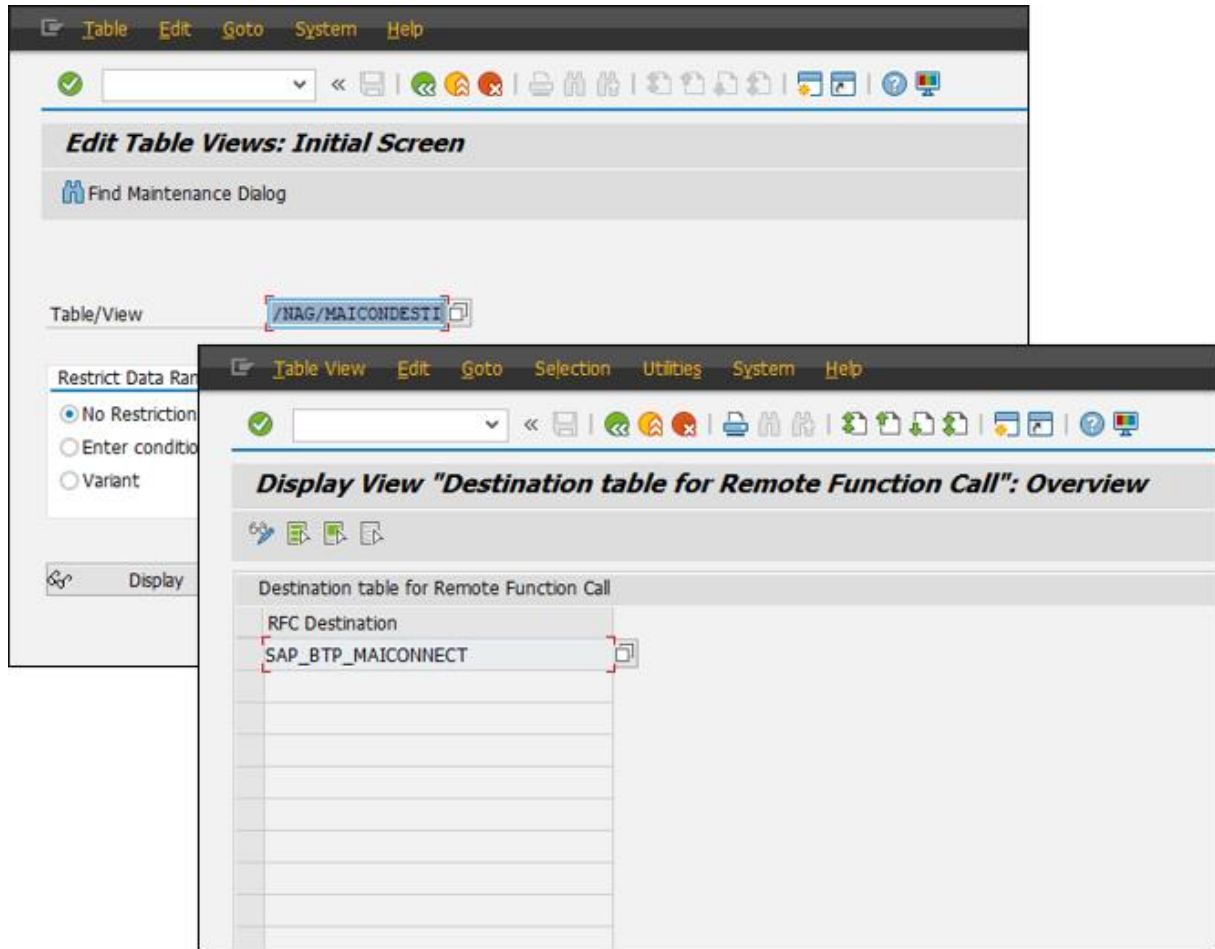



Figure 22: SAP – Maintaining the RFC connection



Please note that the entries in this table won't be transported. Therefore the respective entry needs to be maintained manually in each system maiConnect is running in.

4.6 Customizing for the Synchronization of Contacts

 The customizing settings described in this chapter are only required if the synchronization of contacts is to be used as a feature. If the contact synchronization is not used, you can continue with the settings in the next chapter.

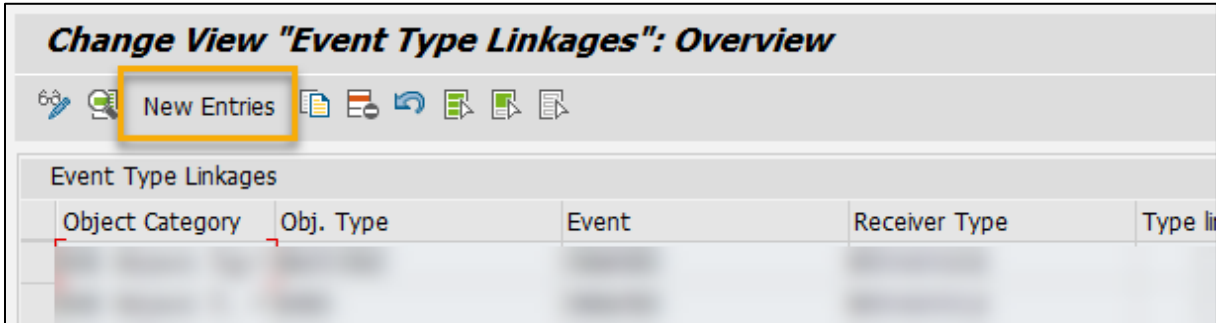


Figure 23: Transaction SWE2 – Adding new customizing entries

Execute transaction SWE2 and create three individual entries here via the "New Entries" button. The following illustrations show which details you have to specify in each case.

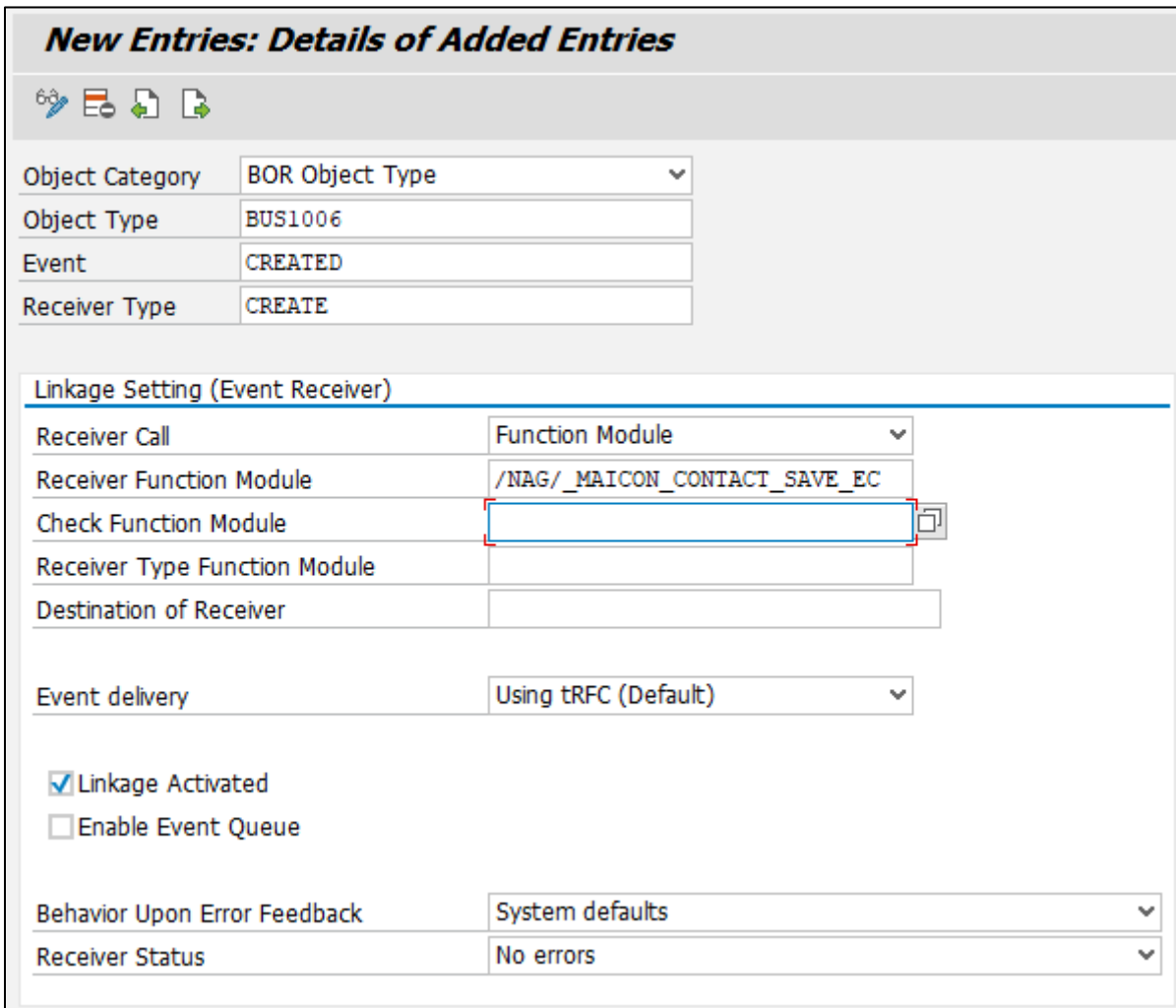






Figure 24: SWE2 Entry - Creation

New Entries: Details of Added Entries

Object Category	BOR Object Type
Object Type	BUS1006
Event	CHANGED
Receiver Type	CHANGED

Linkage Setting (Event Receiver)

Receiver Call	Function Module
Receiver Function Module	/NAG/_MAICON_CONTACT_SAVE_EC
Check Function Module	<input style="border: 2px solid red;" type="text"/>
Receiver Type Function Module	
Destination of Receiver	

Event delivery Using tRFC (Default) ▼

Linkage Activated

Enable Event Queue

Behavior Upon Error Feedback	System defaults
Receiver Status	No errors

Figure 25: SWE2 Entry – Changes / Updates

New Entries: Details of Added Entries

Object Category: BOR Object Type
 Object Type: BUS1006
 Event: DELETED
 Receiver Type: DELETED

Linkage Setting (Event Receiver)

Receiver Call: Function Module
 Receiver Function Module: /NAG/_MAICON_CONTACT_SAVE_EC
 Check Function Module:
 Receiver Type Function Module:
 Destination of Receiver:

Event delivery: Using tRFC (Default)

Linkage Activated
 Enable Event Queue

Behavior Upon Error Feedback: System defaults
 Receiver Status: No errors

Figure 26: SWE2 Entry - Deletion

After creating those three customizing entries please save your changes.

Enable BAdI Implementation

If something is changed in the relationships relevant for synchronisation, no SAP standard event is called. To cover this case, a BAdI implementation must now be created / activated.

In transaction SE18, please display the BAdI *BUPA_RELATSHP_UPDATE*:

Enhancement Spot Edit Goto Utilities Enhancement Implementa

BAdI Builder: Initial Screen for Definitions

Enhancement Spot:
 BAdI Name:

Display Change Create

Figure 27: SE18

In the menu, please select “Implementation – Create”:

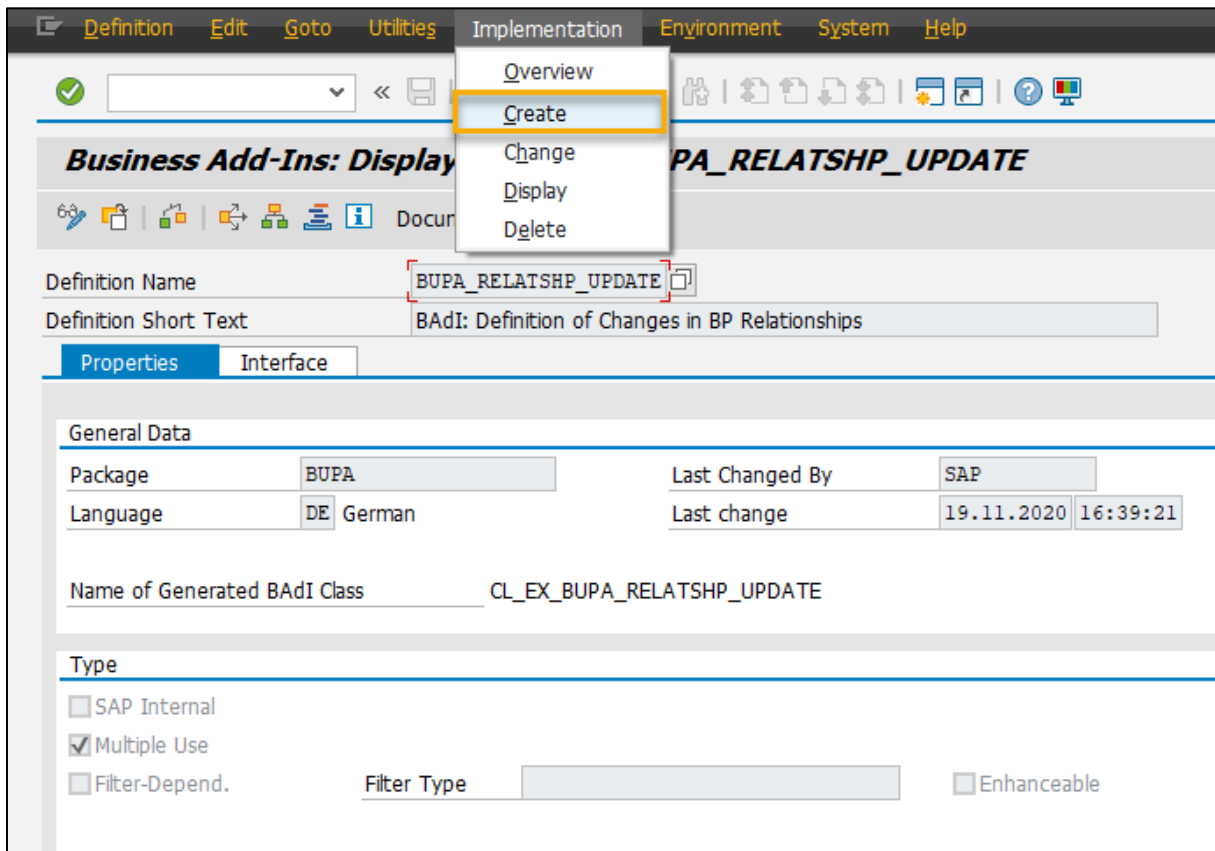


Figure 28: Create BAdI Implementation

Enter a name for the implementation:

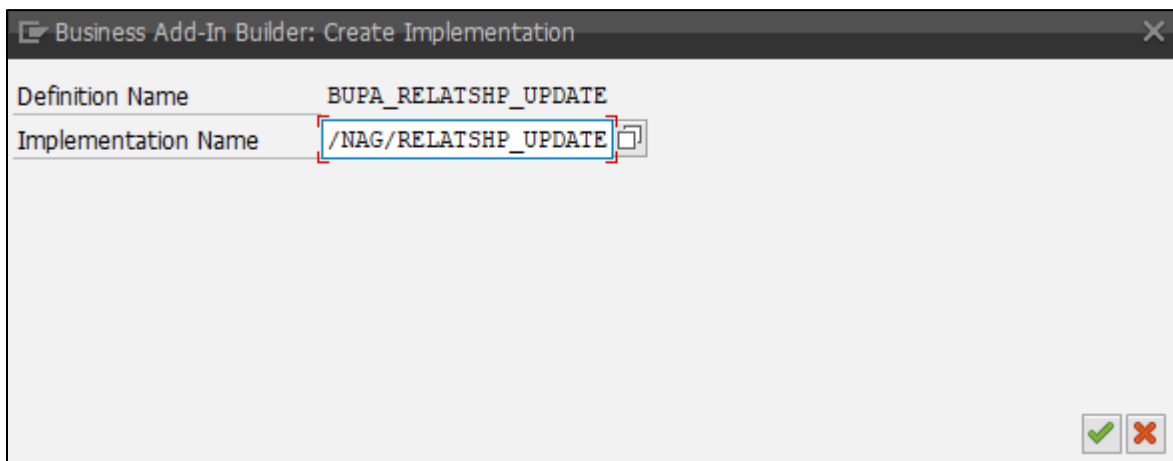


Figure 29: Naming the implementation

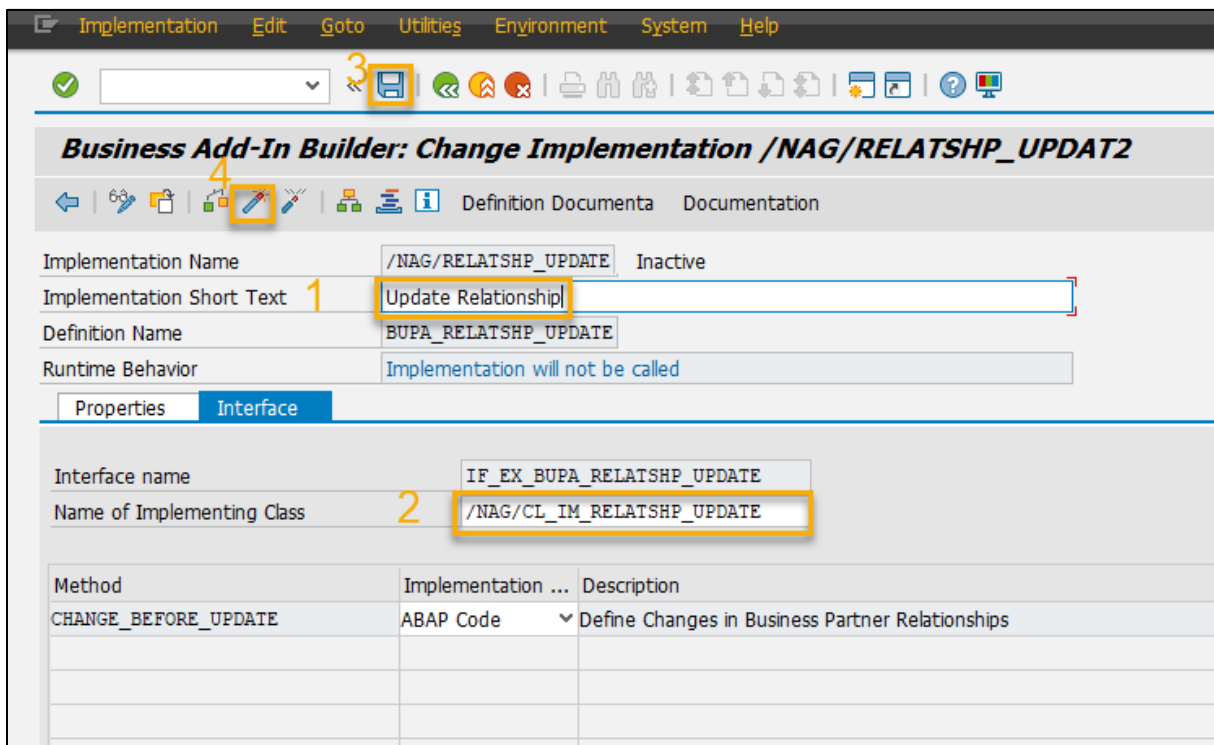


Figure 30: Setting up and activating the implementation

Enter a short text (1) and make sure that `/NAG/CL_IM_RELATSHP_UPDATE` is set as name of the implementing class (2). Save the settings (3) – this might require a transport to be selected / chosen.

Afterwards, activate the implementation (4).

5 Exchange Server Settings

The following settings must be made on the Microsoft Exchange Server by the appropriate administrator.

5.1 Enable EWS and local authentication

5.1.1 Local Exchange Server

On the Exchange Server, EWS must be enabled, as well as Anonymous Authentication and Basic Authentication for EWS.

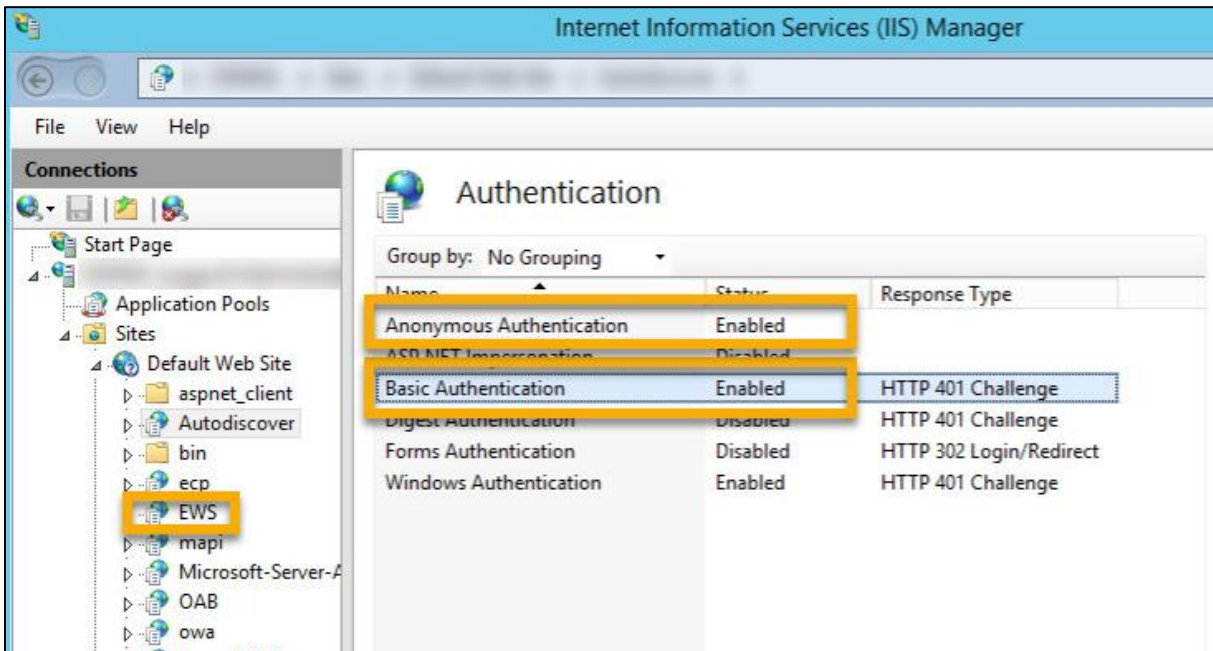


Figure 31: Exchange Server – IIS Configuration (Example)

The setup of the permissions for a Exchange OnPrem server are described in chapter 5.2.1

5.1.2 Office 365

In a cloud scenario OAuth must be activated on Exchange Online. By default, this is the case.

The setup of OAuth is described in detail in chapter 5.2.2.

5.2 Setting up mailbox access

To ensure access, either a dedicated service user (in the sense of a communication user) or OAuth can be used.

Please note that access via a service user is only possible with Exchange onPrem. For Office 365, Microsoft only supports access via OAuth.

5.2.1 Dedicated service user

To carry out changes in the groupware, maiConnect uses a dedicated Exchange user. For this purpose, this user must have the required access rights for the users' mailboxes.

The rights can be assigned in various ways, which differ greatly in terms of the effort required and the subsequent maintenance required. The methods listed here are examples and can be adapted, extended and combined for the respective needs. Depending on the Exchange version and system environment, certain methods may not be available.

5.2.1.1 Mailbox database level rights

A central Exchange user is required who has read and write permission to all Outlook mailboxes. This permission can be granted using the following command:

```
Get-MailboxDatabase -identity "MailboxDatabase01" | Add-ADPermission -user
"EXCH_ADMIN" -AccessRights GenericAll
```

This command only provides access to the MailboxDatabase01 object - not to the Active Directory objects. If there are multiple mailbox databases, the command must be executed for each database individually. However, this command only grants access to all currently existing mailboxes; if a new mailbox is added, the command must be executed again. This can be scheduled as a script if necessary.

5.2.1.2 Assigning rights via RBAC

If the RBAC roles are created, two commands must be executed in the Exchange Management Shell (adapted to the environment):

```
New-ManagementScope -Name "MAICONNECT_SCOPE" -RecipientRoot
"contoso.de/Employee" -RecipientRestrictionFilter {RecipientType -eq
"UserMailbox"}
```

At this point, a restriction to a partial group of users of the Exchange system is created. The access rights can then be assigned with the help of this restriction:

```
New-ManagementRoleAssignment -Name " MAICONNECT_ROLE" -Role
"ApplicationImpersonation" -User:"MAICONNECT_USER" -
CustomRecipientWriteScope:"MAICONNECT_SCOPE"
```

The assignment of the ApplicationImpersonation role can also be done without CustomRecipientWriteScope and then refers to all users. Alternatively, the CustomRecipientWriteScope can be adjusted according to the needs (e.g. restricted to a user group) to restrict the access rights of the service user.

5.2.1.3 Setting up individual access to mailboxes

If the Exchange Admin User's access to the mailboxes is to be managed individually for each mailbox, it must be granted the required access rights to the individual folders (Calendar, Tasks & Contacts).

This can be done automatically via script, as briefly described below - or directly from the users' mailboxes.

Script

Using the following script access to the calendar of all users can be established:

```
$rooms = Get-Mailbox -RecipientTypeDetails UserMailbox  
$rooms | %{Add-MailboxFolderPermission $_:"\Calendar" -User folderrights -  
AccessRights Owner}
```

Alternatively, for one mailbox:

```
Add-MailboxFolderPermission -Identity max.mustermann@cxaddons.com:\calendar -  
<User>-AccessRights Owner
```

Full access:

```
Add-MailboxPermission -Identity max.mustermann@cxaddons.com -User  
Maiconnect_User -AccessRights FullAccess -InheritanceType All
```

5.2.2 Authorization via OAuth (Office 365)

If Office365 is used the authorization can be handled via OAuth. Therefore, maiConnect needs to be registered in the respective Azure AD - through the classic Azure Portal <https://portal.azure.com/>.

5.2.2.1 Registration in Azure Portal

Log in with a user who has administrator rights and navigate to "Azure Active Directory" -> "App registrations". Click "+ New registration".

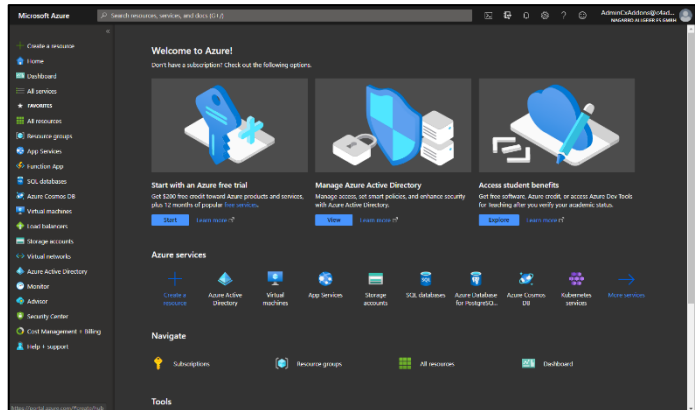


Figure 32: Azure Portal – Home Page

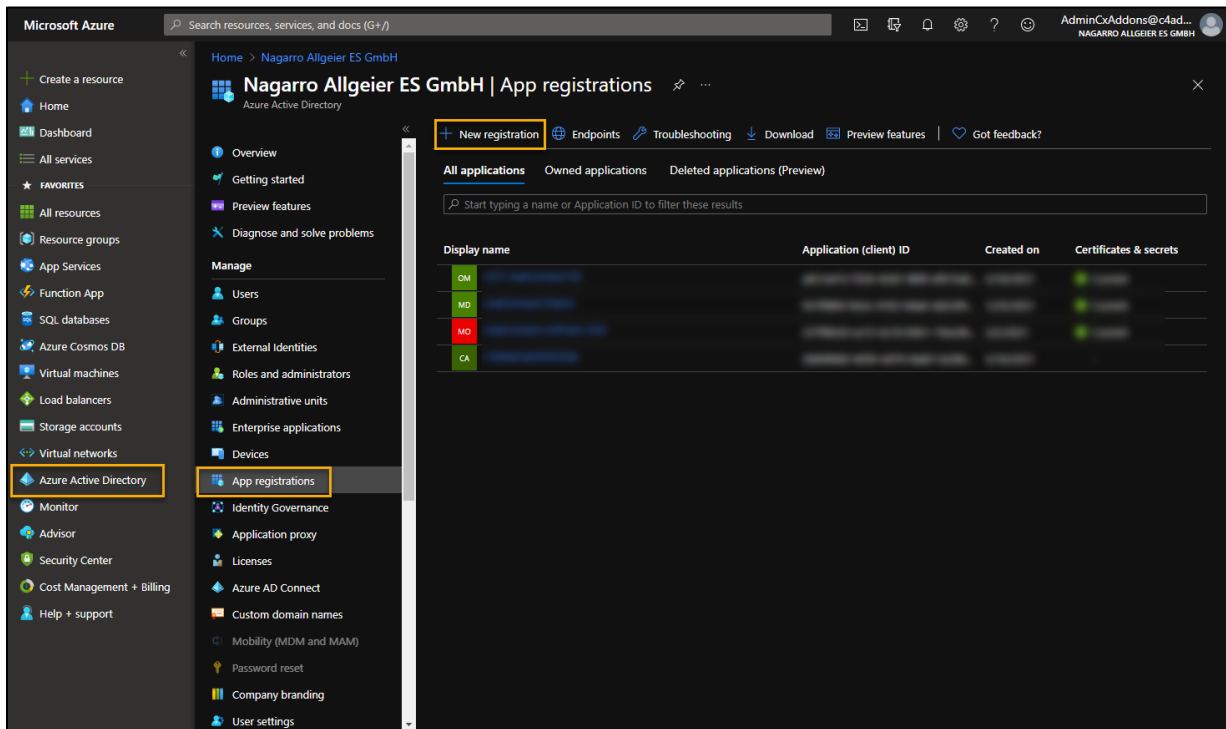


Figure 33: Azure Portal – App registrations

Provide a name for your application (e.g. “maiConnect”), select the account type as outlined in the screenshot below and leave the redirect URL empty. Click “Register”.

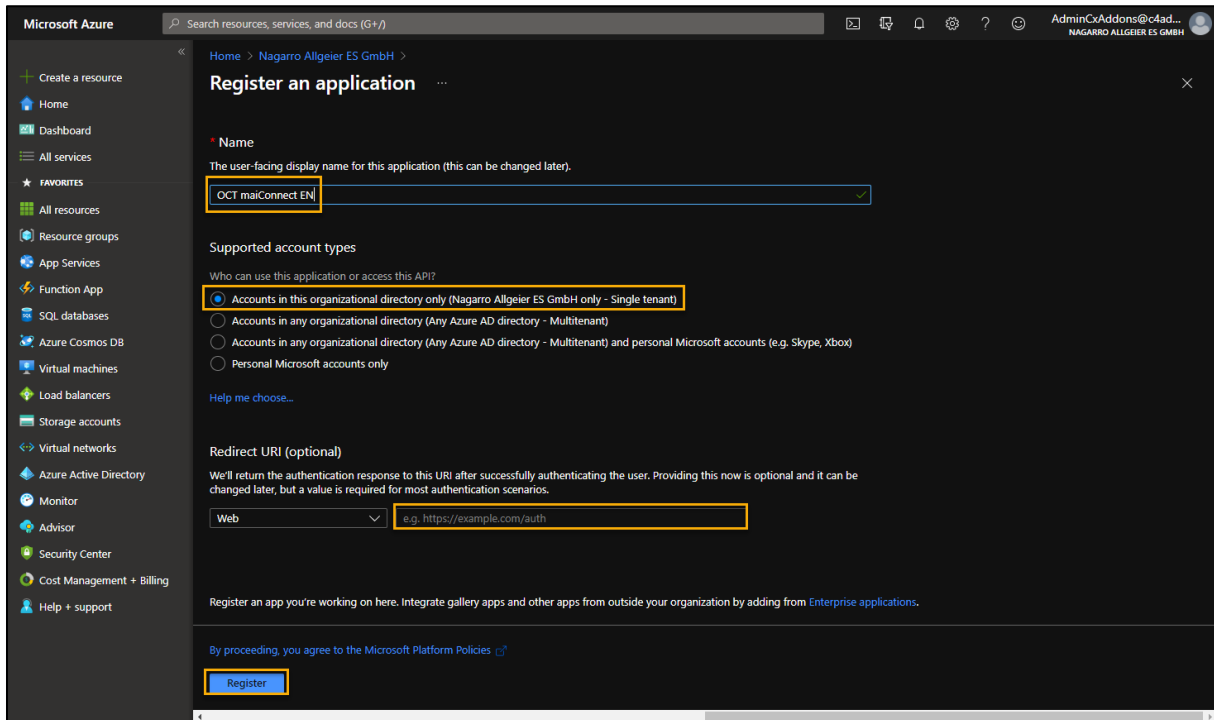


Figure 34: Azure Portal – Registering a new application

Open your newly registered app by clicking the name:

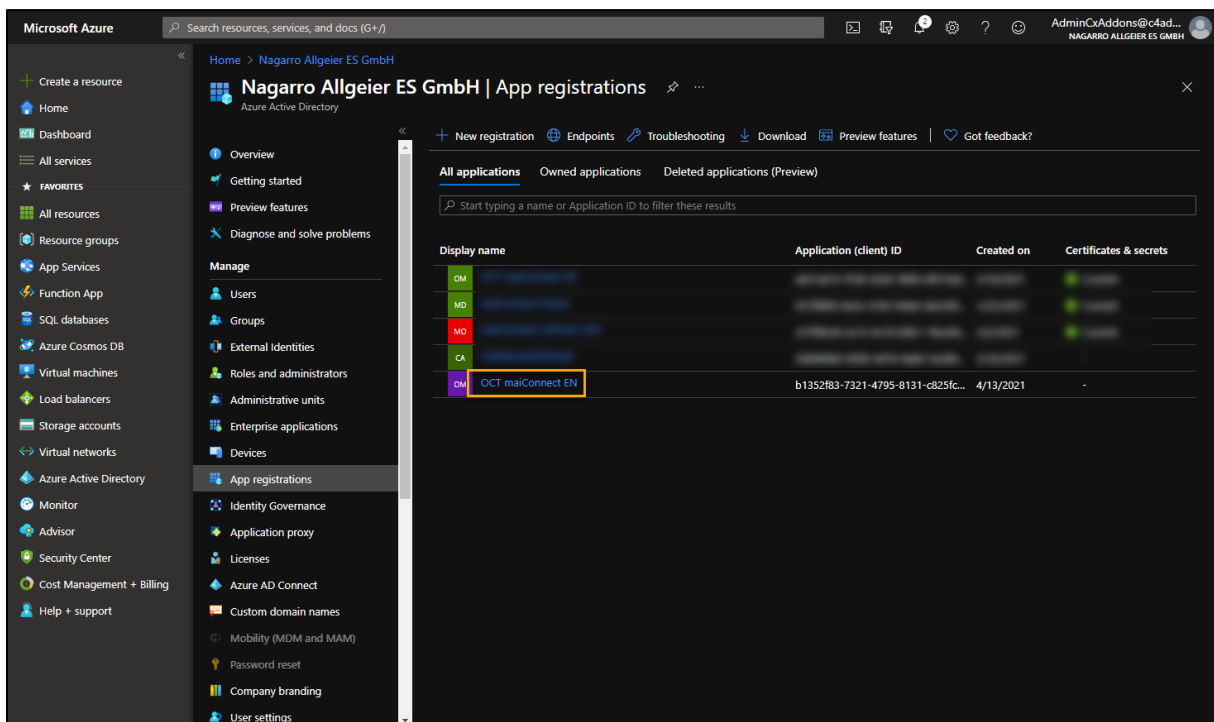


Figure 35: Azure Portal - Opening the newly registered application

Head over to “API permissions”:

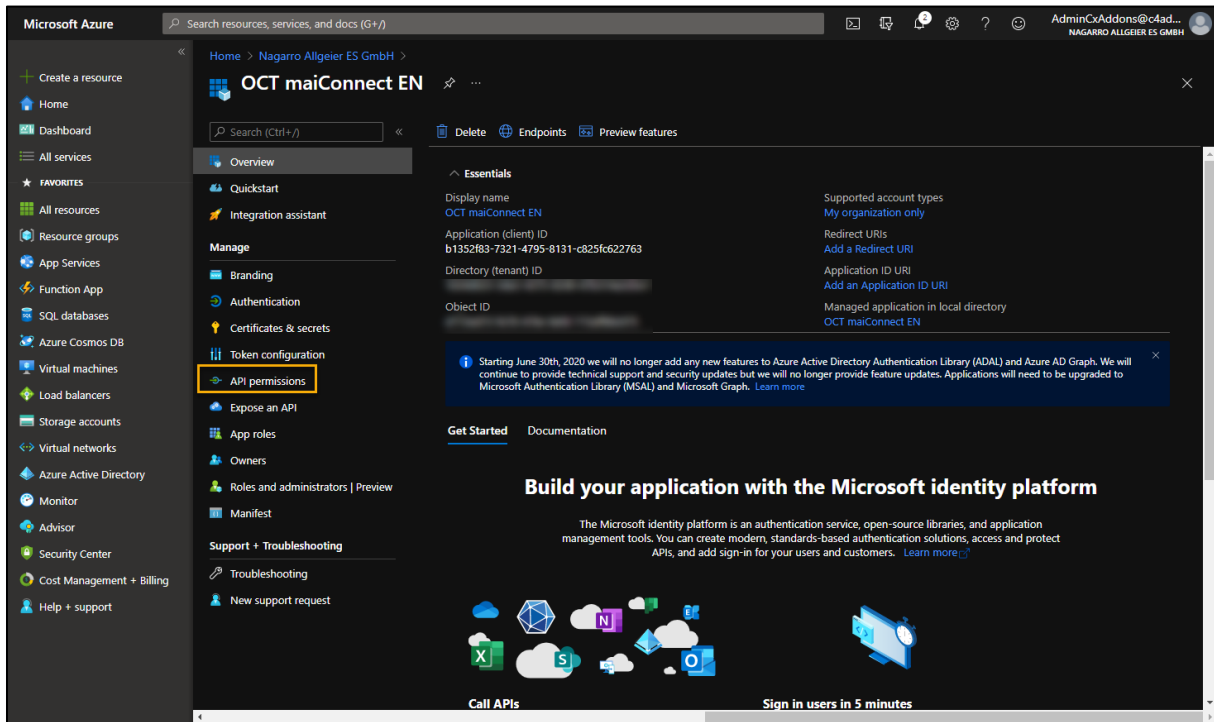


Figure 36: Azure Portal - Overview of the newly registered application

Add new permissions by clicking “+ Add a permission”:

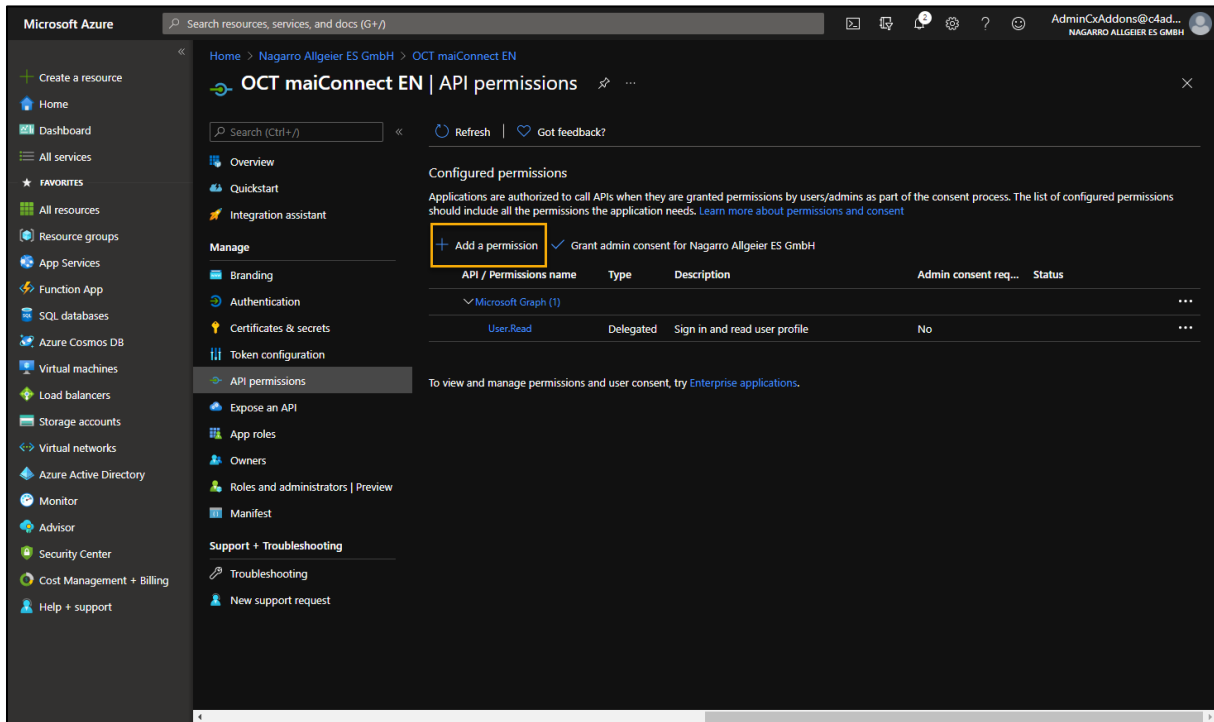


Figure 37: Azure Portal - Add permissions

Select “APIs my organization uses”, search for “office” and select “Office 365 Exchange Online”:

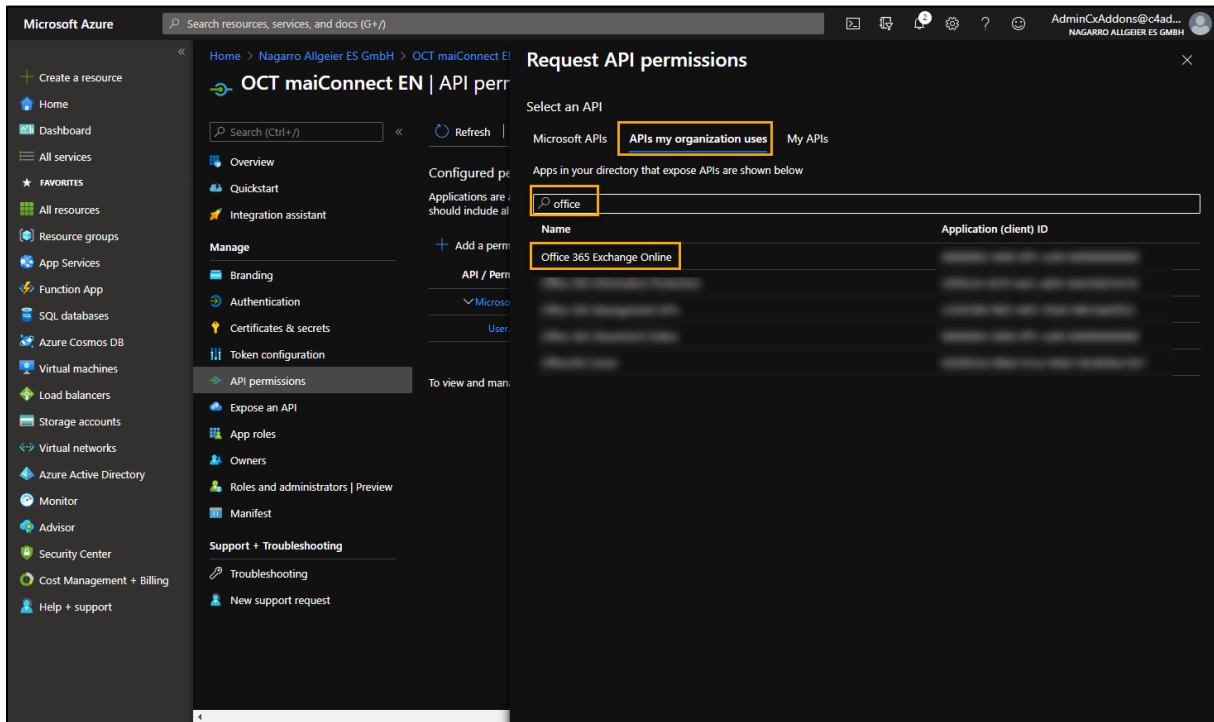


Figure 38: Azure Portal - APIs my organization uses

Choose “Application permissions” and select “full_access_as_app”. Add them by clicking the button below:

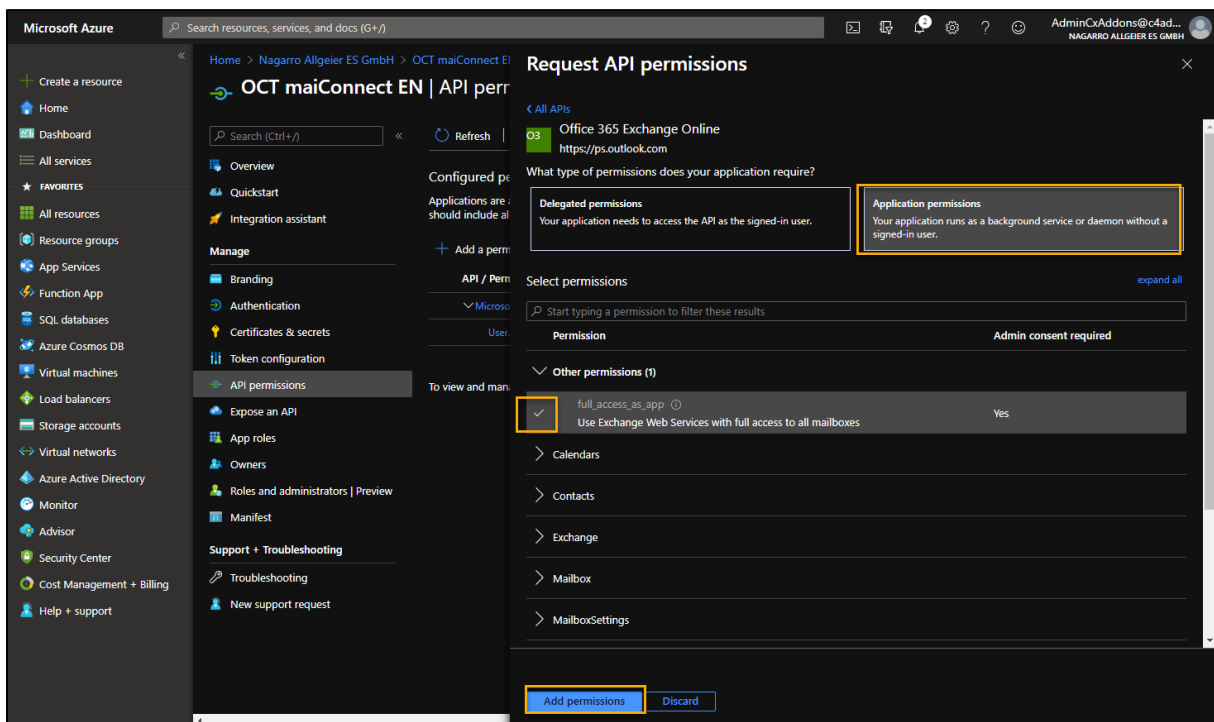


Figure 39: Azure Portal - Application permissions

Now you must grant admin consent for your organization:

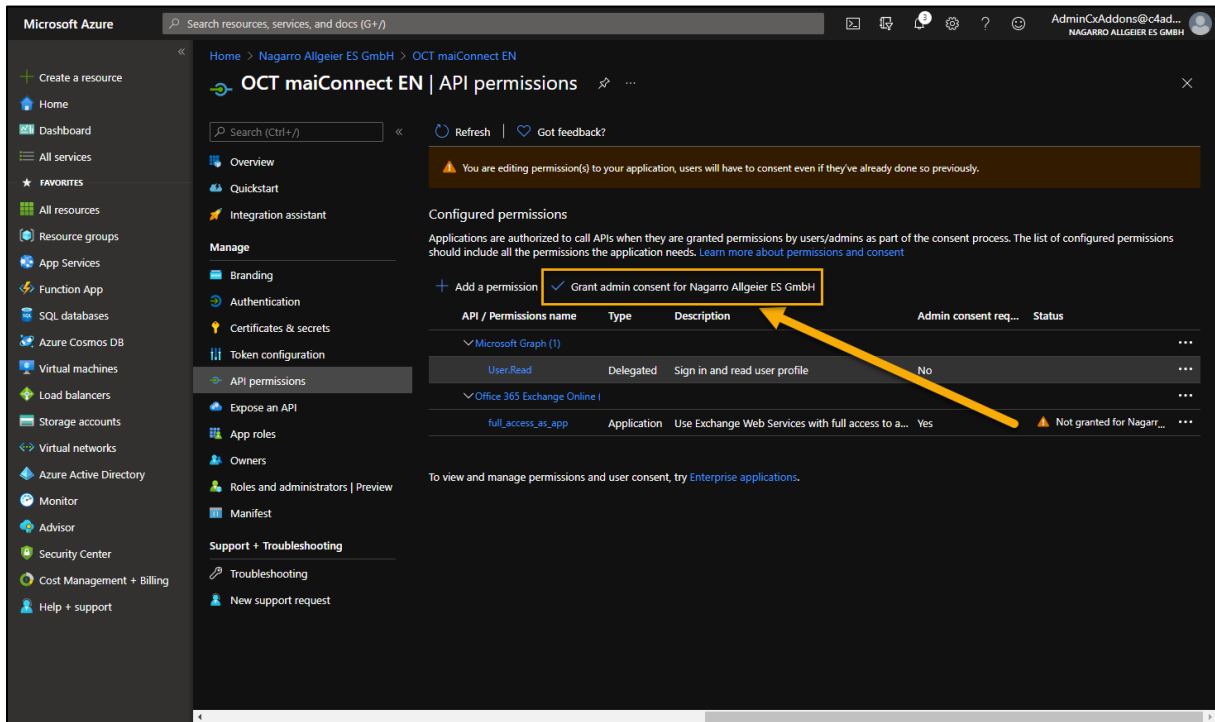


Figure 40: Azure Portal - Grant admin consent

Confirm the popup:

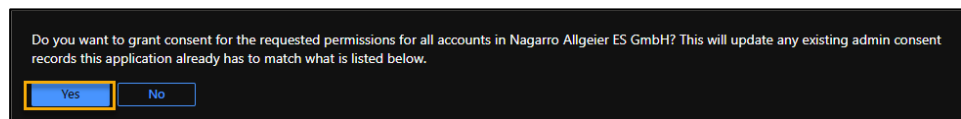


Figure 41: Azure Portal - Confirm granting consent

It should look like this now:

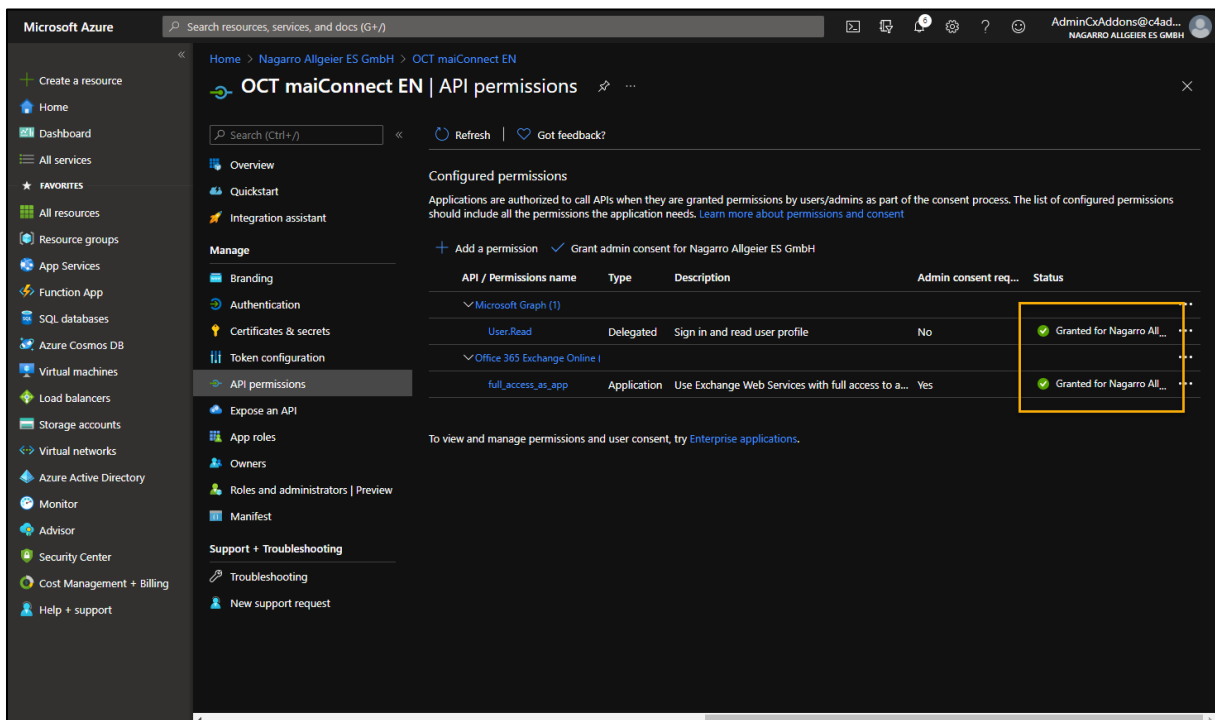


Figure 42: Azure Portal - Permissions successfully added

You can either directly edit the text right in the Azure Portal or you can download the manifest as JSON file, open it with an editor, exchange the relevant part, save it and re-upload the file as shown below.

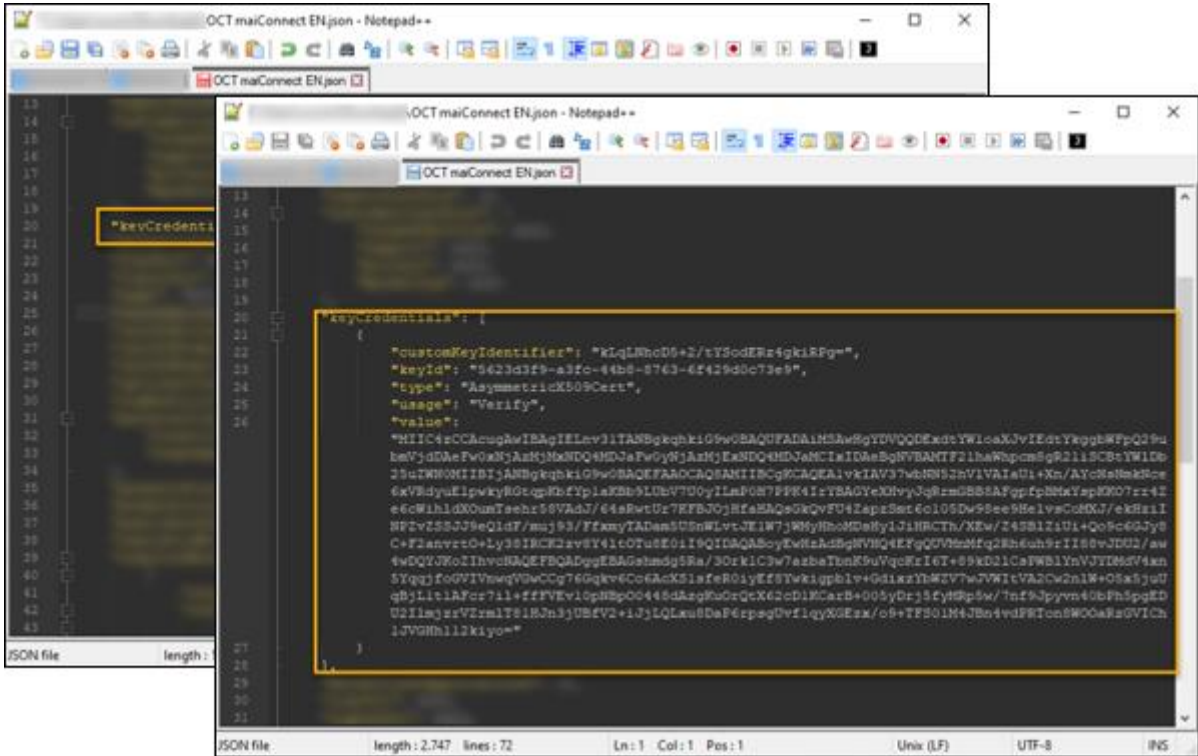


Figure 44: Editing the manifest via editor

Make sure to SAVE the edited manifest:

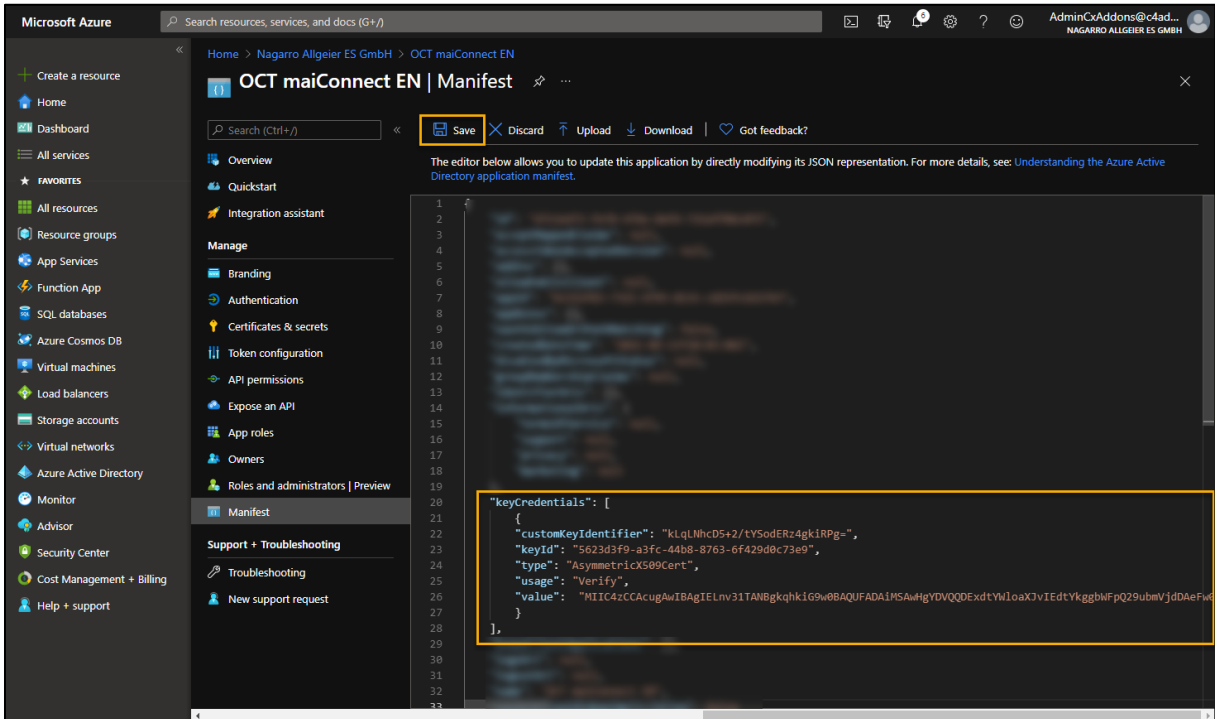


Figure 45: Azure Portal - Saving the manifest

Now go back to the overview of your application and note down the “Application (client) ID”. After this, click on “Endpoints”:

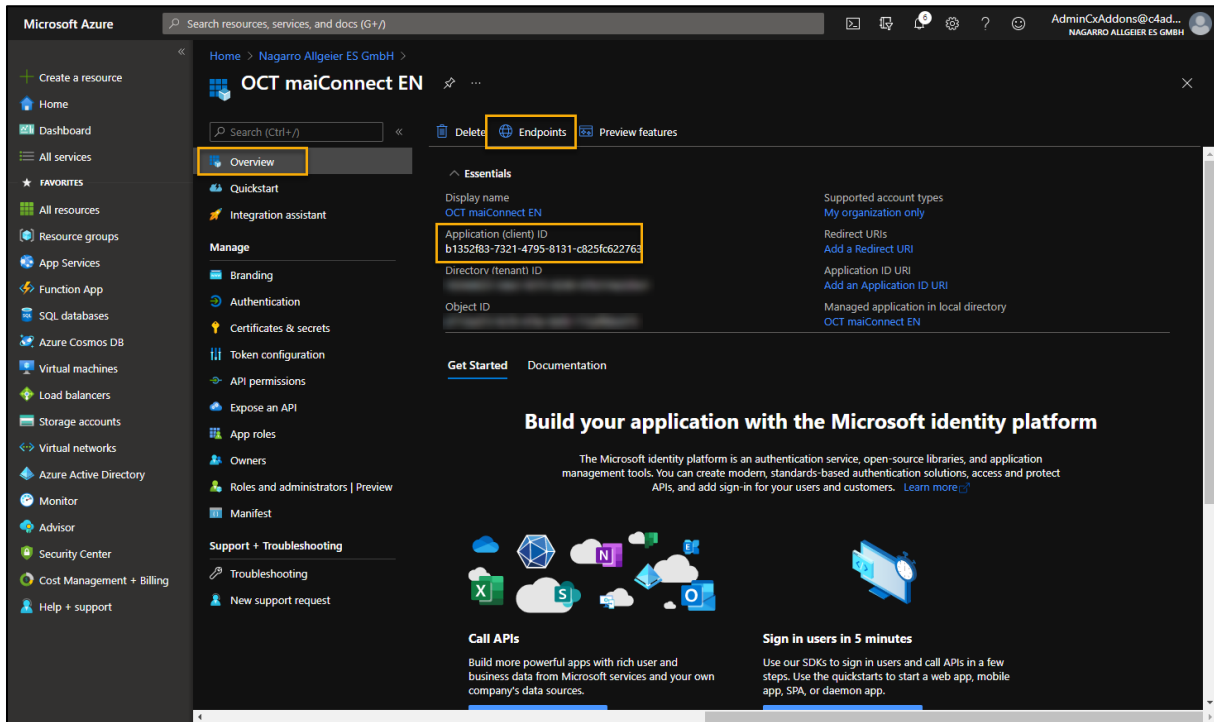


Figure 46: Azure Portal - Application-ID

From the list of endpoints, select the one outlined in the picture below and provide this, along with the application ID to the business administrator responsible for maiConnect.

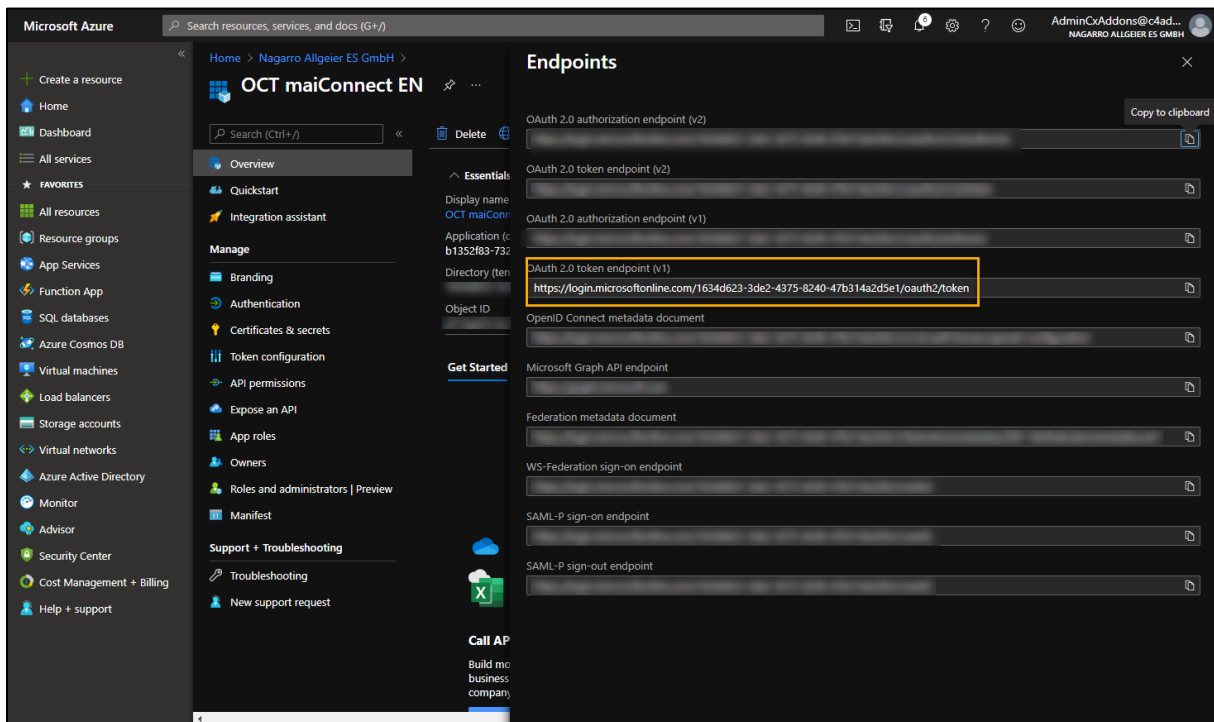


Figure 47: Azure Portal – Endpoints

5.2.3 Note about the Azure API permissions

According to the above description in Microsoft Azure, maiConnect requires the application permission "full_access_as_app" for the EWS interface. This means, that the maiConnect application theoretically has access to all mailboxes.

The maiConnect AdminCockpit is used to define for which users the synchronization should take place. Only for the configured users an access to the mailbox takes place. Other mailboxes are not known to maiConnect at all. Therefore, it is hereby assured that no other mailboxes are accessed than the configured maiConnect users.

In addition, Microsoft Azure offers the possibility to control access to individual mailboxes via an ApplicationAccessPolicy. See the following page for more information:

<https://docs.microsoft.com/en-us/powershell/module/exchange/new-applicationaccesspolicy?view=exchange-ps>

To create a new ApplicationAccessPolicy the following command must be executed in Exchange Online PowerShell:

```
New-ApplicationAccessPolicy -AccessRight <ApplicationAccessPolicyRight> -
AppId <String[]> -PolicyScopeGroupId <RecipientIdParameter>
```

- AccessRight: DenyAccess / RestrictAccess.
- AppID: ID of the Azure AD application
- PolicyScopeGroupId: UPN of the user or name of the group

The simplest way to use policy is to create a RestrictAccess policy for an application with access to the necessary mailboxes. Access to mailboxes not stored in the policy is prevented.

5.3 Exchange Throttling Policy

A throttling policy can be used to limit the number of connections per exchange account. The EWSMaxConcurrency parameter is of particular importance here.

The following errors describe how a throttling policy can be implemented for maiConnect.



Please note that Office365 does not allow these settings by default and for Exchange 2013 certain parameters no longer exist!

Create a policy name

```
New-ThrottlingPolicy MaiConnect
```

Remove limitations for the service user

```
Set-ThrottlingPolicy MaiConnect -RCAMaxConcurrency $null -RCAPercentTimeInAD
 $null - RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null -
 EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -
 EWSPercentTimeInMailboxRPC $null -

EWSMaxSubscriptions $null -EWSFastSearchTimeoutInSeconds $null -
 EWSFindCountLimit $null
```

Exchange 2013

```
Set-ThrottlingPolicy MaiConnect -RCAMaxConcurrency Unlimited -EWSMaxConcurrency
Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited -
 EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
```

Assign service user to policy

```
Set-Mailbox "<maiConnectAdmin>" -ThrottlingPolicy MaiConnect
```

5.4 Connection between Exchange and SAP BTP

To access the Exchange Server, maiConnect uses the EWS interface (Exchange Web Service) from Microsoft. That means queries or changes are performed by Web Services from the SAP BTP on the Exchange Server. Depending on the network topography and security policies of the maiConnect customers, these web service calls can go through a proxy or a firewall that forwards the request to the corresponding Exchange Server.

For the synchronization from Exchange to SAP BTP, subscriptions are created for each mailbox. Thus, maiConnect is notified about changes (creation, updates, or deletions) in a subscribed mailbox via push notifications. These notifications are processed, and a response is sent back to the Exchange Server. If maiConnect does not respond, e.g., due to a downtime, the Exchange Server will resend the request. If there is no response to the message after several attempts, the subscription is automatically deleted from the Exchange Server. Subscriptions are created automatically when users are added via the maiConnect admin cockpit. In case the subscriptions on the Exchange Server for certain mailboxes have been deleted, a background job is running in maiConnect to renew the subscriptions. In this case, a watermark is used to replicate all missed changes.

When creating the subscription, a callback URL is specified to which the notifications of the Exchange Server should be sent. This custom URL is required for the setup on the S/4HANA system side and is provided to the customer by Nagarro ES before the setup of maiConnect.

See this graphic from Microsoft about the push notifications:

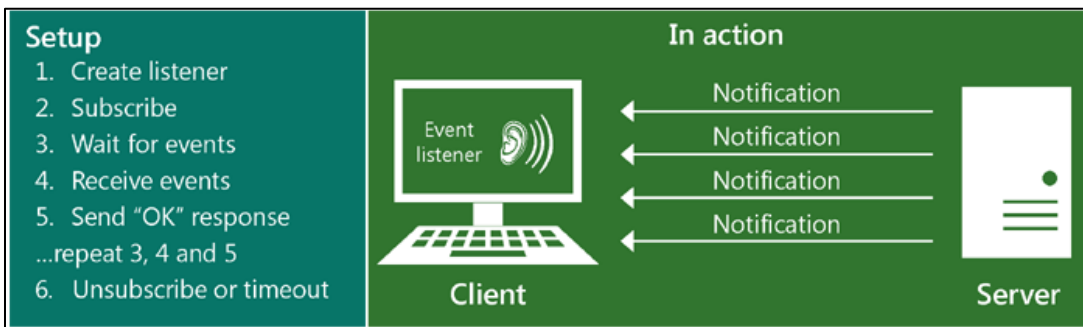




Figure 48: Push Notifications



Further information about the push notifications can be found here:

<https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/notification-subscriptions-mailbox-events-and-ews-in-exchange>

The customer must ensure that the connection from Exchange to the SAP BTP via EWS is secure. The customer must also check that the callback URL of the subscriptions is accessible from the Exchange server.

-  The network environment is customer specific and therefore the setup of the above-mentioned points is up to the customer. Please make sure that the communication between SAP BTP and Exchange Server is not blocked by a reverse proxy or the firewall!
-  Communication between SAP BTP and Exchange is encrypted. The SAP BTP holds a certificate from the Baltimore Cybertrust Root. Generally, this is already available on an Exchange server.

With the push notifications, a connection is established from Exchange to the SAP BTP. If this does not happen, please check whether Baltimore Cybertrust is set as trusted on the Exchange and whether the certificate is up to date.

-  If the connection to the Exchange Server is secured via SSL with a certificate, then the certificate must have been issued by certain trusted certificate authorities. A list of certification authorities accepted by SAP can be found here:
<https://wiki.scn.sap.com/wiki/display/CLOUD/Trusted+Certificate+Authorities>
-  If the customer uses a proxy server and the connection from Exchange towards the SAP BTP cannot be established successfully, then an outgoing allowance rule must be activated in the proxy to enable the communication

6 List of Figures

Figure 1: System landscape	3
Figure 2: Deployment sequence	4
Figure 3: Cloud Connector - Login	7
Figure 4: Cloud Connector – Changing the initial password & choosing the installation type	7
Figure 5: Cloud Connector – Adding subaccount.....	7
Figure 6: Cloud Connector – Adding a subaccount	8
Figure 7: Cloud Connector – Subaccount successfully added.....	9
Figure 8: Cloud Connector – Cloud To On-Premise mapping	9
Figure 9: Cloud Connector – Settings for the system mapping.....	10
Figure 10: Cloud Connector – System mapping created successfully.....	11
Figure 11: Cloud Connector - Resources	11
Figure 12: Cloud Connector – Add Resource	11
Figure 13: Cloud Connector – Resource maintained	12
Figure 14: SAP – Adding OData Services.....	14
Figure 15: SAP – Adding the services to a transport	14
Figure 16: SAP – Overview of activated services (here in German)	15
Figure 17: SAP – Define activity types	15
Figure 18: SAP – Event Handler Module Assignment	16
Figure 19: SAP – Adding an event	16
Figure 20: SAP – RFC Connection – Technical Settings	17
Figure 21: SAP – RFC connection – Logon & Security.....	18
Figure 22: SAP – Maintaining the RFC connection.....	19
Figure 23: Transaction SWE2 – Adding new customizing entries	20
Figure 24: SWE2 Entry - Creation	20
Figure 25: SWE2 Entry – Changes / Updates.....	21
Figure 26: SWE2 Entry - Deletion	22
Figure 27: Exchange Server – IIS Configuration (Example)	25
Figure 28: Azure Portal – Home Page	28
Figure 29: Azure Portal – App registrations	28
Figure 30: Azure Portal – Registering a new application	29
Figure 31: Azure Portal - Opening the newly registered application	29
Figure 32: Azure Portal - Overview of the newly registered application.....	30
Figure 33: Azure Portal - Add permissions.....	30
Figure 34: Azure Portal - APIs my organization uses	31
Figure 35: Azure Portal - Application permissions	31
Figure 36: Azure Portal - Grant admin consent.....	32
Figure 37: Azure Portal - Confirm granting consent.....	32
Figure 38: Azure Portal - Permissions successfully added.....	32
Figure 39: Azure Portal - Manifest.....	33
Figure 40: Editing the manifest via editor	34
Figure 41: Azure Portal - Saving the manifest.....	34
Figure 42: Azure Portal - Application-ID	35
Figure 43: Azure Portal – Endpoints	35
Figure 44: Push Notifications.....	38