Deployment Guide

Release 2303 – März 2023

maiConnect
for SAP S4/HANA®

cxAddOns

cxAddOns

Global AddOn specialist for Enterprise Software.

Inhaltsverzeichnis

1 Systemlandschaft

maiConnect@S4 wird auf der SAP Business Technology Plattform (SAP BTP) gehostet. Für den Datenaustausch zwischen SAP S/4HANA onPrem und Microsoft Exchange (inkl. Office 365) verwendet es die Standard-Schnittstellen der SAP und Microsoft.

Die Kommunikation von SAP S/4HANA in Richtung SAP BTP geschieht über eine RFC-Verbindung. Wird ein Objekt in SAP S/4HANA angelegt/verändert/gelöscht, wird ein Event getriggert und eine hinterlegte maiConnect@Cloud URL aufgerufen.

Aus Richtung SAP BTP kommuniziert maiConnect über einen Cloud Connector mit Standard-OData-Services. Weitere, von maiConnect benötigte OData-Services, werden über einen Transport ins S/4HANA System eingespielt.

Der Anwender kommuniziert über den Microsoft Outlook Client ebenfalls mit dem Microsoft Exchange Server und erhält so sämtliche Termine, Aufgaben und Kontakte.

Durch die direkte Kommunikation von maiConnect@S4 mit dem Microsoft Exchange Server ist es auch möglich, dass Termine, Aufgaben und Kontakte direkt auf sämtlichen Exchange kompatiblen Endgeräten wie z.B. iPhone oder Tablet zur Verfügung gestellt werden.

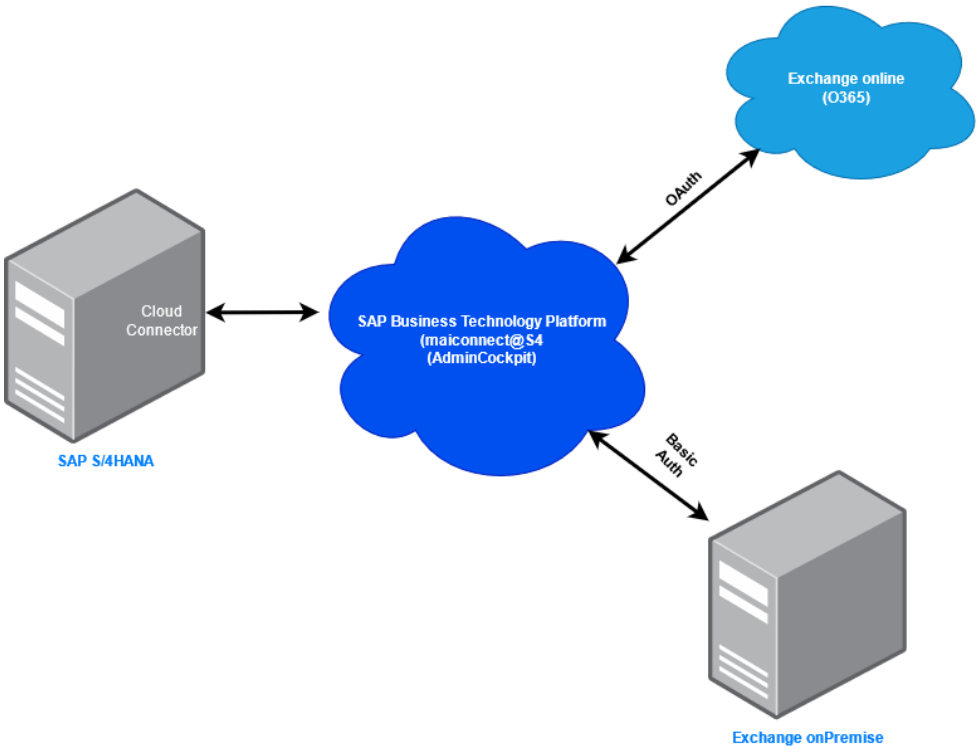

Abbildung 1: Systemlandschaft

2 Deployment Schritte

In diesem Kapitel werden die grundsätzlichen Schritte für ein maiConnect@S4 Deployment beschrieben. Hier ein Überblick über die einzelnen Schritte und deren Abfolge.

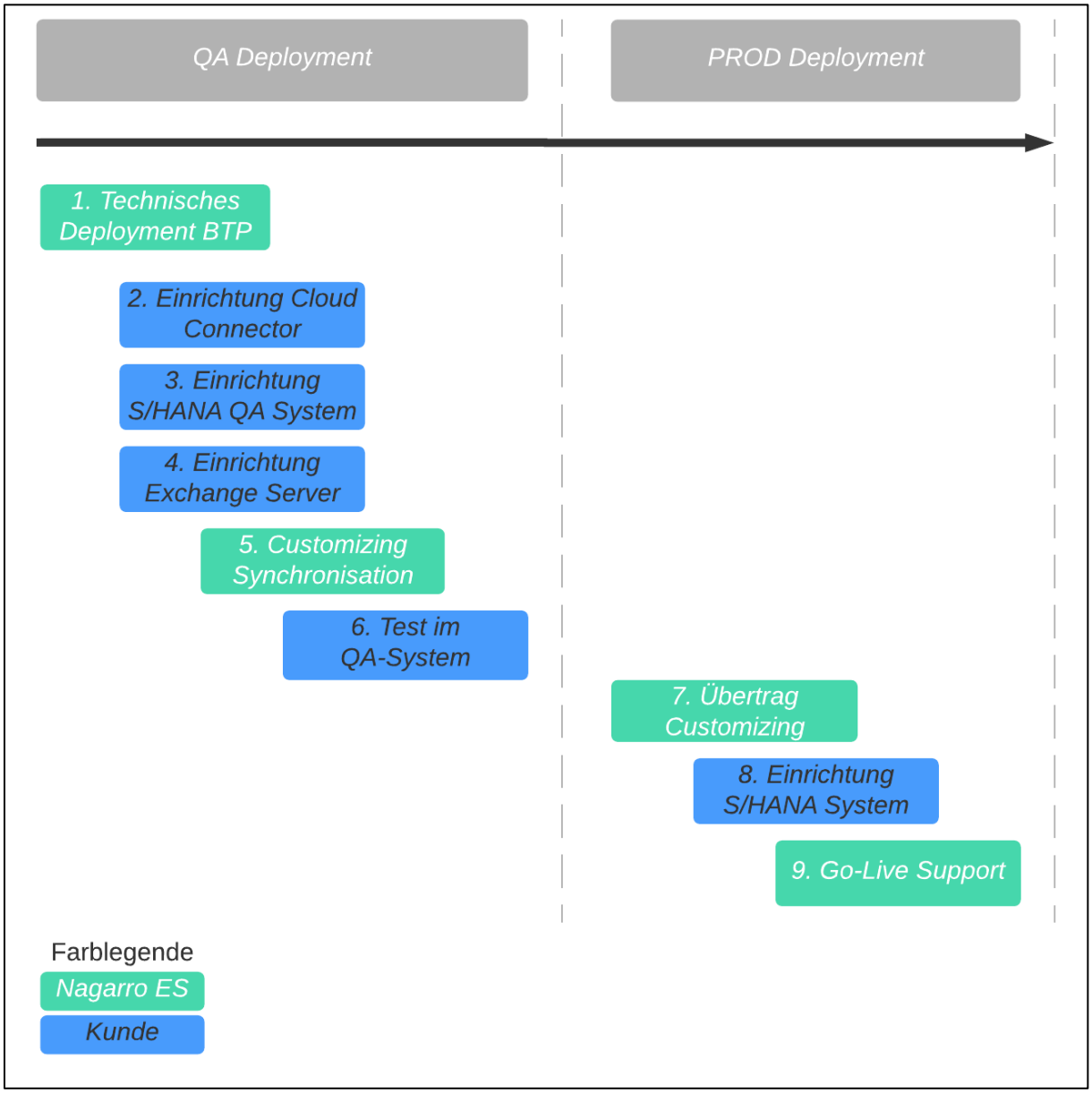

Abbildung 2: Deployment Abfolge

Was bei den jeweiligen Schritten getan werden muss, ist hier weiter erklärt. In den folgenden Kapiteln finden Sie eine detaillierte Beschreibung zu jedem Schritt.

1. Die maiConnect Applikation wird auf der SAP BTP gehostet. Das dort notwendige technische Deployment für die QA und PROD-Umgebung wird von Nagarro ES durchgeführt.

   Aus diesem Schritt ergeben sich die Subaccount IDs für den Cloud Connector.

2. Die Einrichtung des SAP Cloud Connectors für die QA- und PROD-Umgebung wird in der Systemlandschaft des Kunden durchgeführt. Da hierfür ein Netzwerkzugriff notwendig ist, muss diese Einrichtung vom Kunden gemacht werden. Sofern Nagarro ES ein Netzwerkzugriff per VPN o.ä. gewährt wird, kann dieser Schritt auch von Nagarro ES gemacht werden. Diese Einrichtung ist in Kapitel 3 beschrieben.

Damit die Kommunikation zwischen den Systemen hergestellt werden kann, müssen der Nagarro ES verschiedene Informationen bereitgestellt werden. Siehe dazu Kapitel 3.6.

3. Im SAP S/4HANA System müssen verschiedene Einrichtungen gemacht werden. Auch hier gilt: Diese Einrichtung muss vom Kunden gemacht werden und kann nur bei Bereitstellung eines Netzwerkzugriffs von Nagarro ES durchgeführt werden.

   Neben der technischen Einrichtung muss hier vor allem vom Fachbereich des Kunden definiert werden, welche Vorgangsarten für die Synchronisation in Frage kommen. Siehe Kapitel 4.3.

   Für die Einrichtung der RFC-Verbindung liefert Nagarro ES die URL zum maiConnect System. Siehe Kapitel 4.5.

4. Die Einrichtung des Exchange Servers muss vom Kunden durchgeführt werden. Dies ist in Kapitel 5 beschrieben. Abhängig davon, was für ein Exchange Server beim Kunden im Einsatz ist, muss entweder die Einrichtung für ein Exchange onPrem (Kapitel 5.2.1) oder Office 365 (Kapitel 5.2.2) durchgeführt werden.

   Grundsätzlich unterstützt maiConnect aber auch mehrere Exchange Umgebungen. Dies ist z.B. dann relevant, wenn maiConnect in unterschiedlichen Ländern eingesetzt werden soll, die einen eigenen Exchange Server haben.

5. Wenn die Schritte bis hierher durchgeführt wurden, dann kann die Synchronisation eingerichtet werden. Dies wird bei einem Meeting mit Nagarro ES und Kollegen des Kunden-Fachbereichs gemacht. Bei diesem Meeting kann die Synchronisation getestet werden. Voraussetzung dafür ist das Bereitstellen eines S/4HANA Beispiel-Users, der ein gültiges E-Mail-Postfach hat.

   Bitte prüfen Sie vor diesem Meeting die untenstehende Synchronisations-Checkliste.

   Zusätzlich muss vom Kunden ein oder mehrere Verantwortliche für die Administration von maiConnect benannt werden. Bei einem weiteren Meeting werden dann die AdminCockpit Einstellungen geschult.

6. Bei diesem Schritt hat der Kunde die Möglichkeit die Synchronisation zu testen. Eventuelle Änderungen an den Synchronisationseinstellungen können durchgeführt werden.

7. Vor dem Go-Live überträgt Nagarro ES die Administrations-Einstellungen in das PROD-System. Damit wird sichergestellt, dass die Einstellungen zu diesem Zeitpunkt im QA- und PROD-System identisch sind.

8. In diesem Schritt werden die Einstellungen im S/4System vom Kunden in das produktive S/4HANA System übertragen.

9. Beim Go-Live werden die Business-User zum maiConnect AdminCockpit hinzugefügt. Über den maiConnect-Support unter support@cxaddons.com können Probleme gemeldet werden.

2.1 Synchronisations-Checkliste

Termine	
Welche Termin-Vorgangsarten sollen von S/4HANA nach Outlook synchronisiert werden?	
Sollen Termine von Outlook nach S/4HANA synchronisiert werden?	☐
Sollen alle Outlook-Termine synchronisiert werden? Oder Soll die Synchronisierung pro Termin per Zuweisung einer Kategorie oder per Sync-Tag getriggert werden?	☐ Oder ☐
Synchronisation von privaten Terminen?	☐
Synchronisation von Serienterminen von Outlook nach S/4HANA?	☐
Sollen Termin-Anhänge synchronisiert werden?	☐
Welche S/4HANA Ansprechpartner- und Teilnehmer-Partnerfunktionen sind für die Synchronisation relevant? Default für Ansprechpartner: 00000015, Default für Teilnehmer: 00000032	
Aufgaben	
Sollen Aufgaben grundsätzlich synchronisiert werden?	☐
Welche Aufgaben-Vorgangsarten sollen von S/4HANA nach Outlook synchronisiert werden?	
Sollen Aufgaben von Outlook nach S/4HANA synchronisiert werden?	☐
Sollen alle Outlook-Aufgaben synchronisiert werden? Oder Soll die Synchronisierung per Kategorie oder per Sync-Tag getriggert werden?	☐ Oder ☐
Kontakte	
Sollen Kontakte von S/4HANA nach Outlook synchronisiert werden?	☐
Welcher S/4HANA Beziehungstyp wird für die Beziehungen zwischen Kunde und Ansprechpartner verwendet? Default BUR001	
Soll die Synchronisation über das Setzen einer Beziehung zum Ansprechpartner getriggert werden? Wenn ja, welcher Beziehungstyp soll dafür verwendet werden? Default BUR011	☐
Soll die Synchronisation über das Setzen einer Beziehung zum Kunden getriggert werden? Wenn ja, welcher Beziehungstyp soll dafür verwendet werden? Default BUR011	☐

3 Cloud Connector Setup

Allgemeine Informationen zum Cloud Connector (Voraussetzungen, Installation, …) finden sich unter: https://help.sap.com/viewer/cca91383641e40ffbe03bdc78f00f681/Cloud/en-US/e6c7616abb5710148cfcf3e75d96d596.html

3.1 Download & Installation

Der Cloud Connector muss in der Systemumgebung installiert werden, in der auch das S4 System läuft. Laden Sie dazu die passende Installationsdatei von https://tools.hana.ondemand.com/#cloud herunter, starten Sie die Installation und folgen Sie den Anweisungen des Installationsprogramms.

3.2 Erste Schritte nach der Installation

Sobald die Installation erfolgreich abgeschlossen wurde, können Sie die weiteren Einstellungen unter der URL https://localhost:8443/ treffen (ersetzen Sie den Port 8443 entsprechend, falls Sie während der Installation des Programms einen anderen Port angegeben haben). Die Zugangsdaten für den ersten Login lauten:

Benutzer: Administrator

Passwort: manage

Direkt nach dem ersten Login müssen Sie das Initialkennwort ändern. Falls nicht anders vorgegeben wählen Sie bitte „Master“ als Installationstyp:

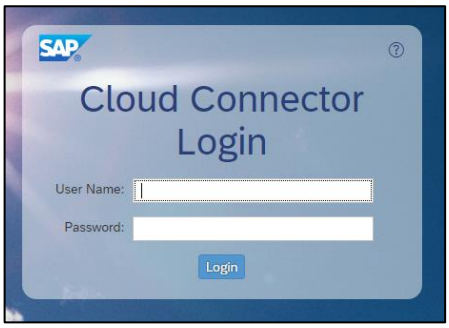

Abbildung 3: Cloud Connector - Login

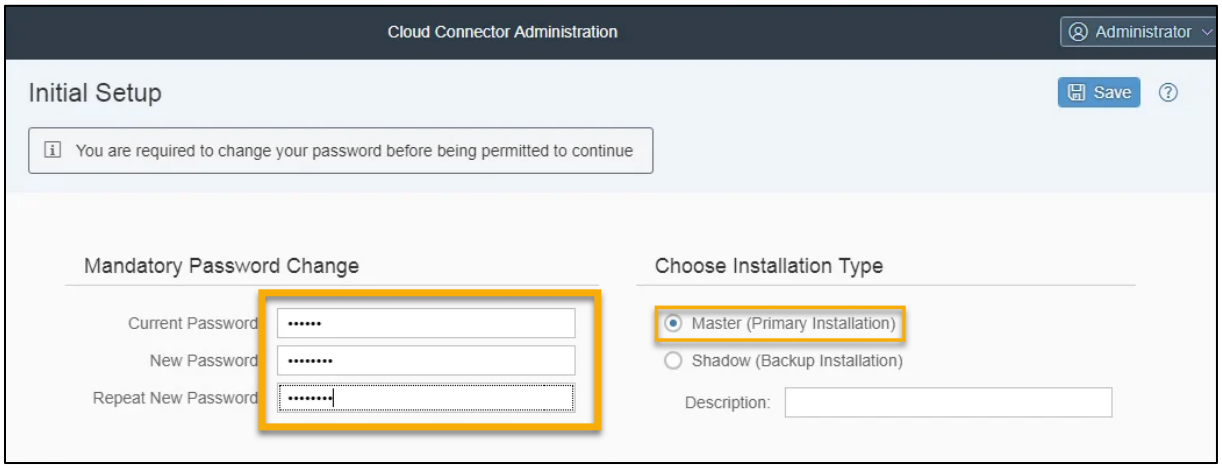

Abbildung 4: Cloud Connector - Ändern des Initialkennworts & Wahl des Installationstyps

3.3 Hinzufügen eines Subaccounts

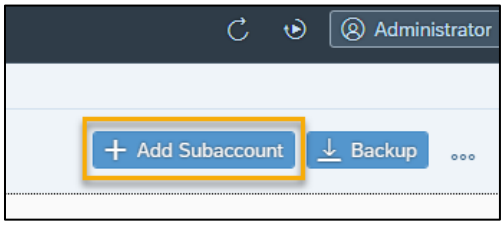

Abbildung 5: Cloud Connector - Hinzufügen

Wenn Sie den Cloud Connector gerade erst installiert haben und sich zum ersten Mal einloggen, sollten Sie im nächsten Schritt automatisch aufgefordert werden, einen Subaccount zu bestimmen. Falls das nicht so ist, können Sie über die Schaltfläche “+ Add Subaccount” rechts oben einen Subaccount hinzufügen.

Im Folgenden werden die einzelnen Felder näher beschrieben. Bitte beachten Sie, dass die Felder, die mit einem roten Asterisk (*) markiert sind, Pflichtfelder sind:

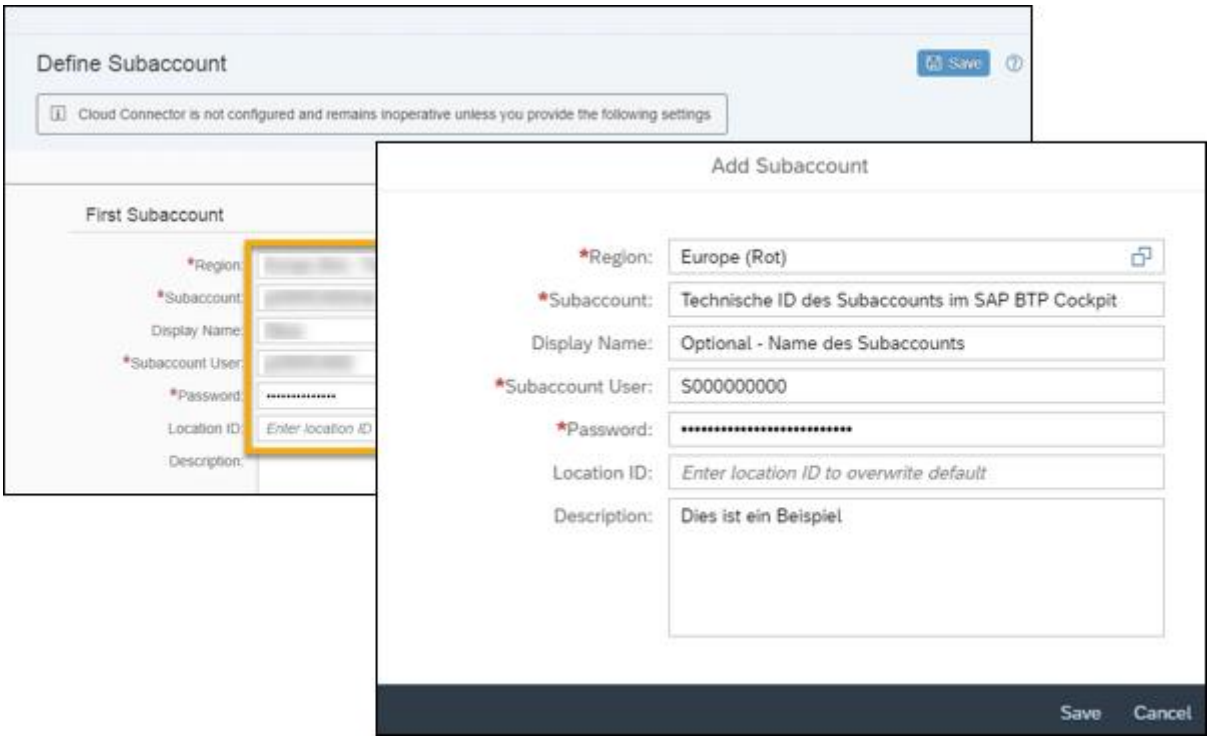

Abbildung 6: Cloud Connector – Hinzufügen eines Subaccounts

Region: Sofern von Nagarro ES nicht anders vorgegeben, wählen Sie hier die Region *Europe (Rot).*

Subaccount: Hier tragen Sie die technische ID des Subaccounts aus dem SAP BTP Cockpit ein. Diese erhalten Sie von Nagarro ES.

Display Name: Optionales Feld. Vergeben Sie hier bei Bedarf einen internen Namen für den verbundenen Subaccount.

Subaccount User: Benutzer ID Ihres P- oder S-Users.

Bitte beachten Sie, dass die SAP im Cloud Connector keine technischen Kommunikationsbenutzer unterstützt, sondern ein normaler P-/S-User verwendet werden muss.

Password: Passwort des darüber eingetragenen Benutzers.

Location ID: Nicht relevant

Description: Optional. Tragen Sie bei Bedarf eine Kurzbeschreibung ein.

Mit dem Speichern wird der Subaccount hinzugefügt und wenn alles korrekt ablief, wird die folgende Übersichtsseite angezeigt:

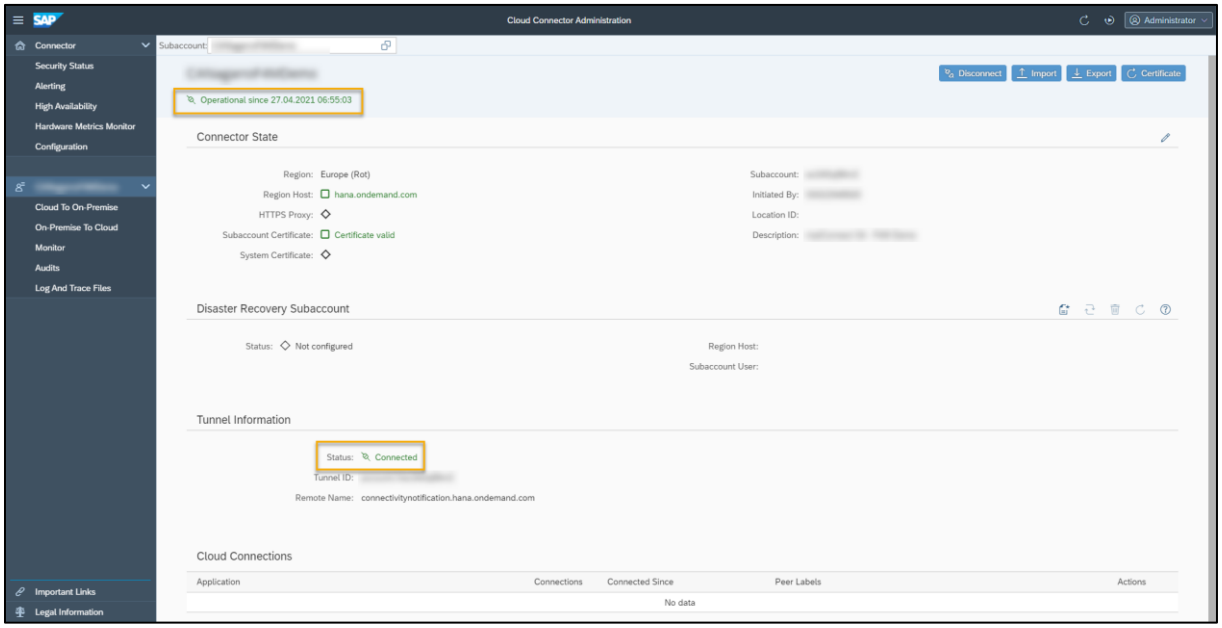

Abbildung 7: Cloud Connector – Subaccount erfolgreich hinzugefügt

Bitte beachten Sie diese SAP-Note, falls es zu dem http Fehler 417 kommt:

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

3.4 System Mapping

Nun wählen Sie für den gerade hinzugefügten Subaccount den Menüpunkt „Cloud To On-Premise“ aus und fügen über die „+“ Schaltfläche ein System Mapping hinzu.

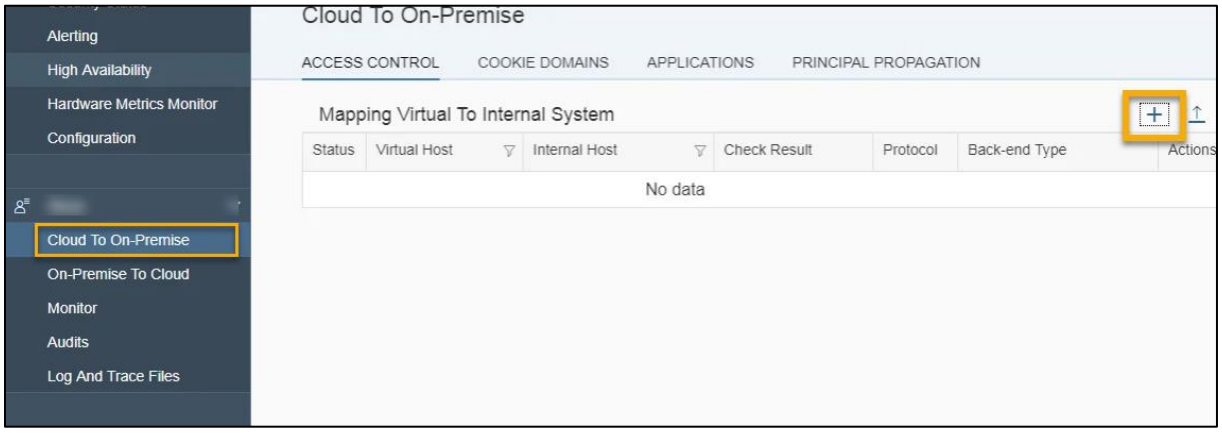

Abbildung 8: Cloud Connector – Cloud To On-Premise Mapping

Klicken Sie sich nun durch die Dialogfolge und wählen für die jeweiligen Parameter folgende Werte aus:

Back-end Type	:	ABAP System
Protocol	:	HTTPS
Internal Host, Internal Port	:	URL / Hostname und HTTPS Port des S4 Systems
Virtual Host, Virtual Port	:	Virtuelle/r URL / Hostname und HTTPS Port (frei wählbar)
Host in Request Header	:	Use Virtual Host
Principal Type	:	None
Description	:	(Optional) Tragen Sie bei Bedarf eine Beschreibung ein.

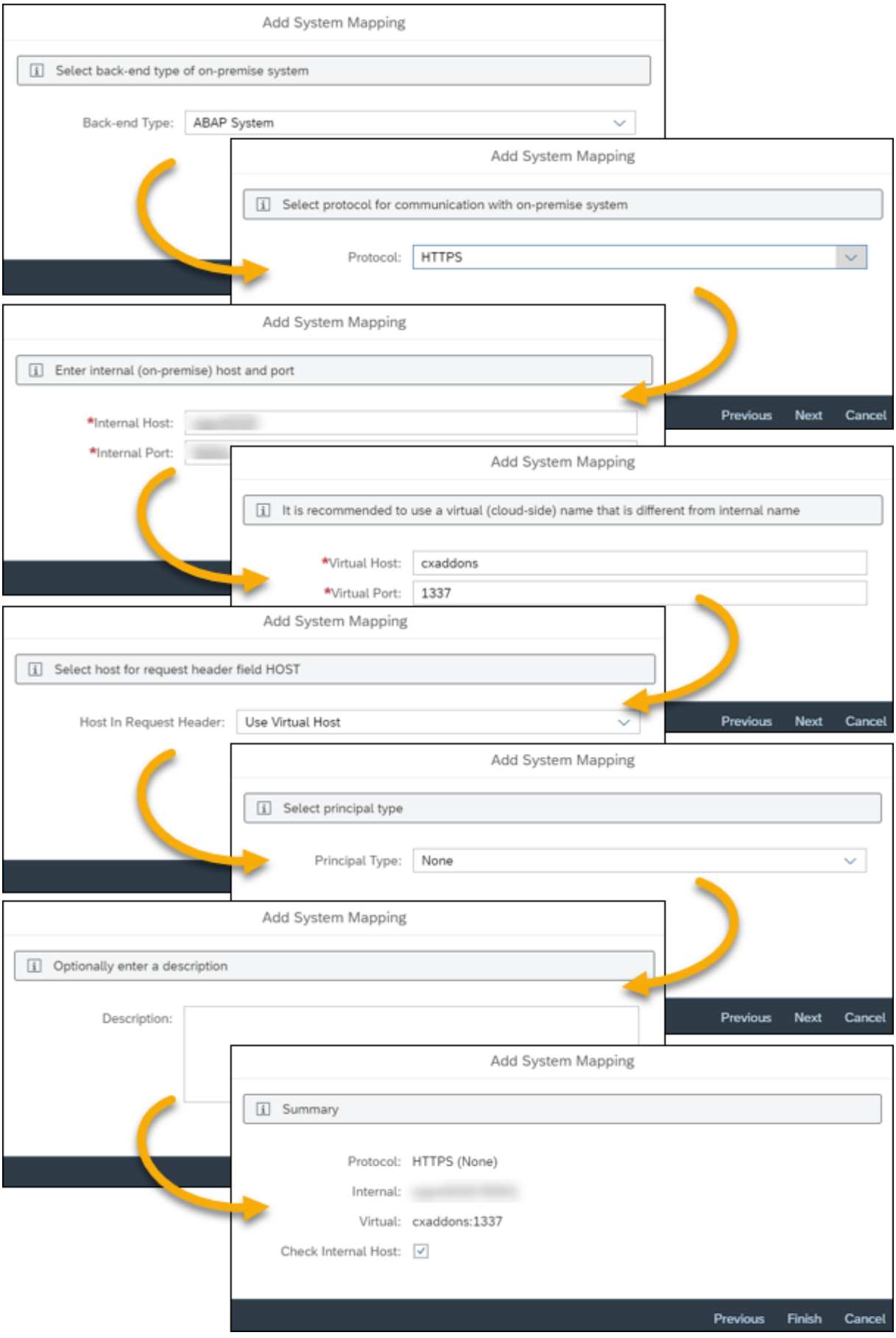

Abbildung 9: Cloud Connector – System Mapping Einstellungen

Bestätigen Sie die zuvor getroffenen Eingaben am Ende und wählen Sie „Check Internal Host“ aus, um direkt beim Speichern des Mappings die Verbindung zu testen. Alternativ können Sie dazu auch die in der untenstehenden Abbildung markierte Schaltfläche rechts verwenden:

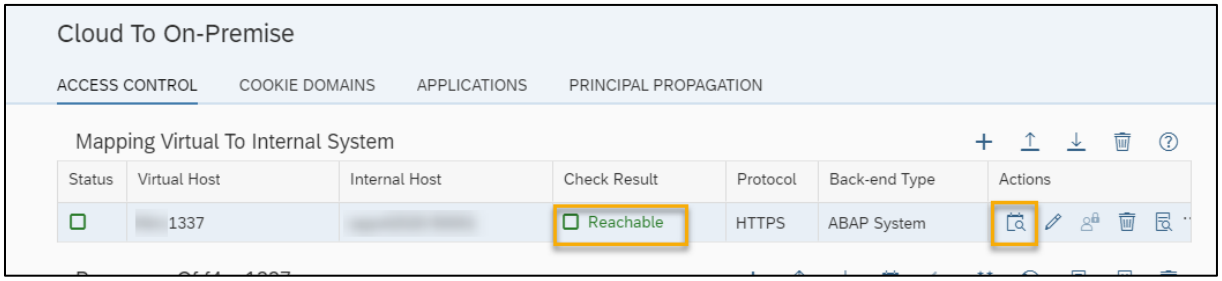

Abbildung 10: Cloud Connector – System Mapping erfolgreich abgeschlossen

3.5 Bestimmung der Ressourcen

Als nächstes müssen die Ressourcen angegeben werden, auf die über den Cloud Connector der Zugriff gewährt wird.

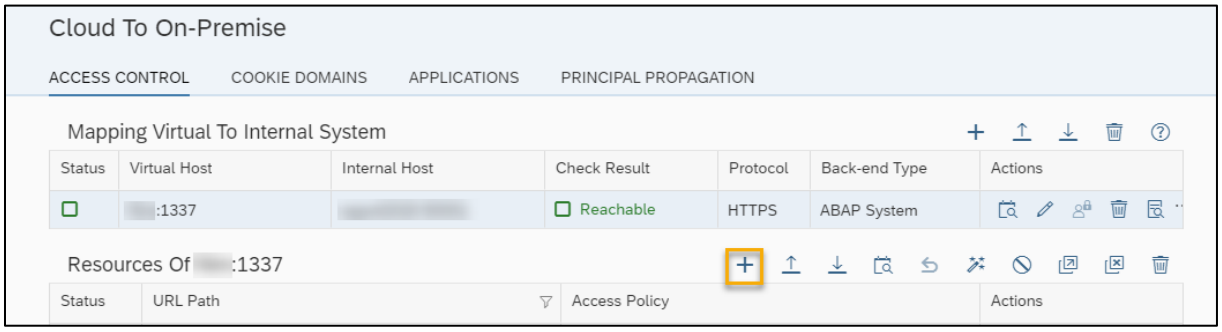

Abbildung 11: Cloud Connector – Ressourcen

Für maiConnect S4 wird Zugriff auf die Ressource /sap/opu/odata benötigt. Fügen Sie über die „+“ Schaltfläche folgenden Eintrag hinzu:

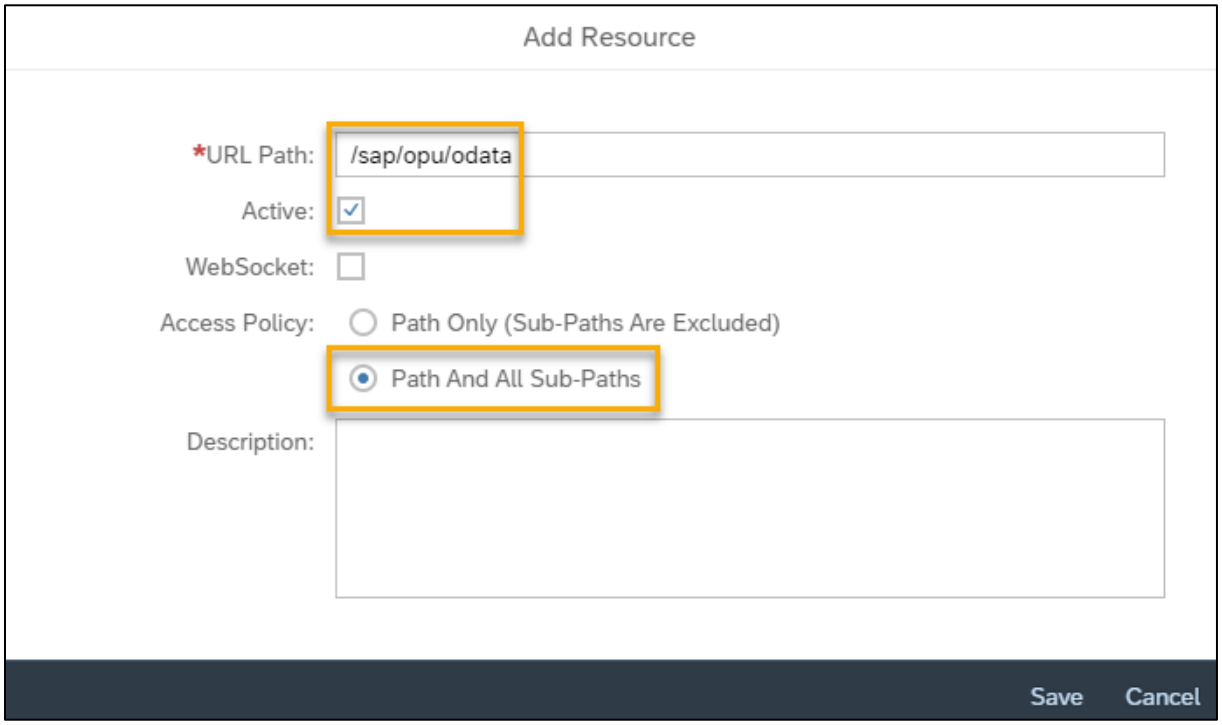

Abbildung 12: Cloud Connector – Ressource hinzufügen

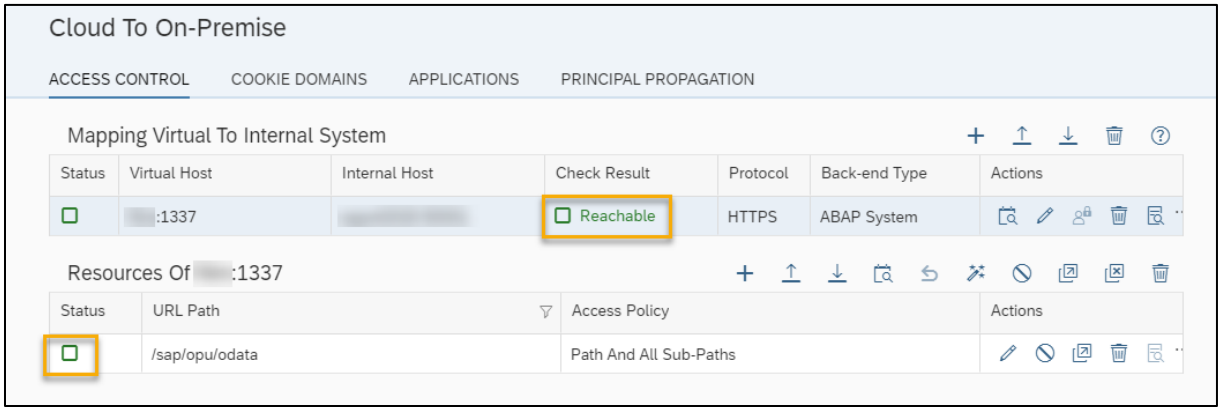

Abbildung 13: Cloud Connector – Einrichtung erfolgreich abgeschlossen

Nachdem Sie die Ressource hinzugefügt haben, ist die Einrichtung des Cloud Connectors abgeschlossen. Die obige Abbildung zeigt, wie es aussehen sollte.

3.6 Bereitstellen der Kommunikationsinformationen

Um die Verbindung herstellen zu können, muss nun im SAP BTP Cockpit eine Destination angelegt werden. Dazu benötigt Ihr Deployment Consultant von Nagarro ES folgende Daten von Ihnen:

Virtual Host, Virtual Port

SAP Mandant

SAP Kommunikations-Benutzer, Password

Siehe Kapitel 4.1 für weitere Informationen zum Kommunikationsbenutzer.

Sie können uns diese Daten gern via E-Mail oder als Textnachricht zukommen lassen – alternativ können wir auch eine Websession organisieren, bei der Sie die Daten via Screensharing selbst eintragen. Kontaktieren Sie uns einfach über support@cxaddons.com, um das weitere Vorgehen zu besprechen.

4 Einstellungen im SAP-System

Um die weiteren Einstellungen durchzuführen, erhalten Sie von Nagarro ES einen Transport, den Sie importieren müssen.

4.1 Kommunikationsbenutzer

Die maiConnect-Änderungen im SAP-System werden zentral von einem Systembenutzer (bezeichnet als „Kommunikationsbenutzer“) durchgeführt. Dieser Benutzer benötigt die entsprechenden Berechtigungen, um Aktivitäten und Geschäftspartner anzeigen und ändern zu können.

Dieser Benutzer muss den Benutzertyp „System“ haben. Es ist nicht notwendig, dass dieser Benutzer ein Dialog-Benutzer ist.

Die bereitgestellten Transporte enthalten einen Customizing-Transport, mit dem eine separate Rolle im SAP-System angelegt wird. Diese Rolle beinhaltet alle notwendigen Berechtigungen für den Kommunikationsbenutzer.

Der Name der Rolle lautet:

- /NAG/SAP_MAICONNECT

4.2 Aktivierung der OData Services

Die folgenden OData Services müssen im SAP-System aktiviert sein, damit maiConnect funktioniert:

- /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

Führen Sie dazu die Transaktion **/N/IWFND/MAINT_SERVICE** aus oder (falls die Transaktion nicht verfügbar ist) führen Sie die Transaktion **SE38** und dort den Report */IWFND/R_MGW_REGISTRATION* aus. Hier wählen Sie die Option „Service hinzufügen“ aus:

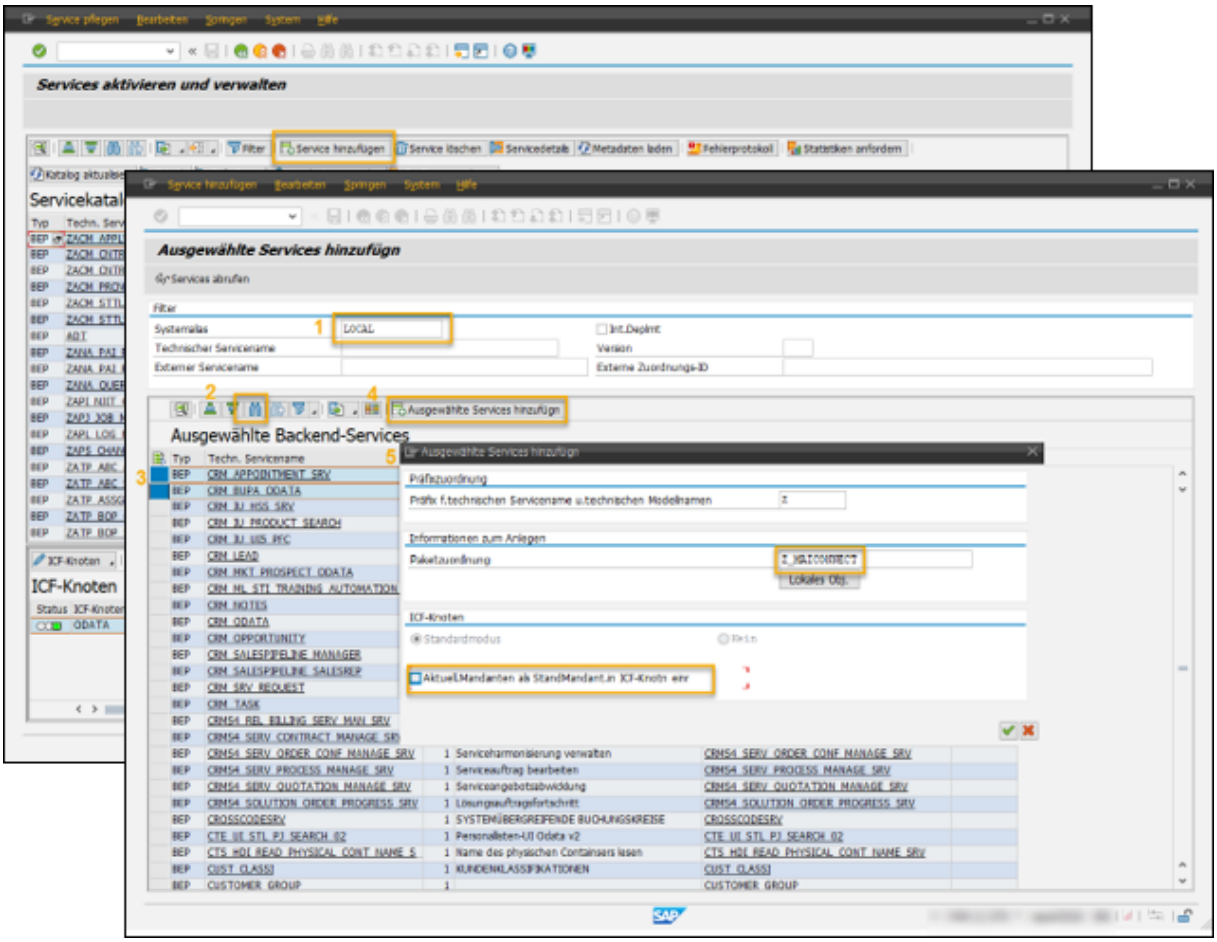

Abbildung 14: SAP – OData Services hinzufügen

(1) Geben Sie als Systemalias „LOCAL“ ein und bestätigen mit <ENTER>

(2) Über die Suchhilfe können Sie die Services suchen

(3) Markieren Sie die Services

(4) Fügen Sie die Services hinzu

(5) Wählen Sie als Präfix ‚Z‘, ordnen Sie es einem Paket zu und bestätigen Sie die Eingaben

Im nächsten Schritt müssen Sie die Änderungen in einen Transportauftrag schreiben.

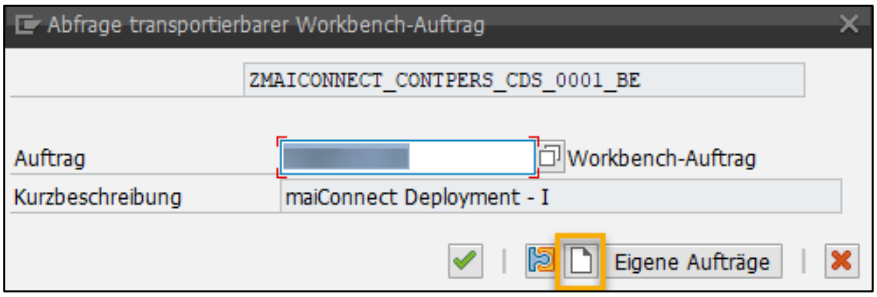

Abbildung 15: SAP – Hinzufügen zum Transportauftrag

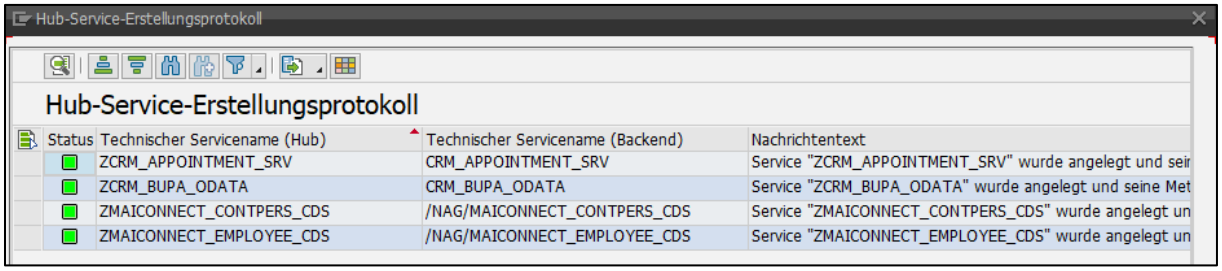

Abbildung 16: SAP – Übersicht über aktivierte Services

Anschließend müssen Sie diesen 6 OData Services über die **SPRO** noch den Systemalias „*LOCAL*“ zuweisen. Das geht unter:

SAP NetWeaver > Gateway > OData Channel > Administration > Allgemeine Einstellungen > SAP-Systemaliasse zu OData Service zuweisen.

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

4.3 Vorgangsarten definieren

Alle Vorgangsarten, für die Termine oder auch Aufgaben in Richtung Exchange synchronisiert werden sollen, müssen via Transaktion SM30 in den entsprechenden Tabellen gepflegt werden. Dabei ist insbesondere die Textart wichtig. Dies ist der Text, der im jeweiligen Outlook-Termin dann im Notizfeld angezeigt wird.

Führen Sie die Transaktion **SM30** aus und lassen Sie sich die entsprechende Tabelle anzeigen. Anschließend können Sie hier einen neuen Eintrag für jede relevante Vorgangsart anlegen.

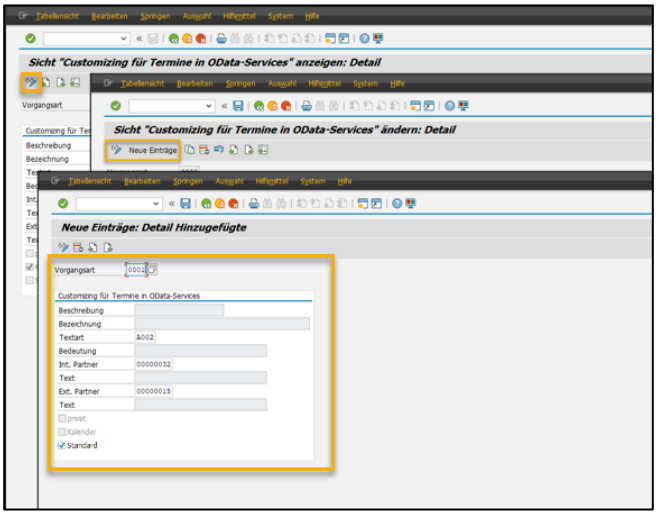

Abbildung 17: SAP – Vorgangsarten definieren

Termine: CRMV_APPT_OD

Aufgaben: CRMV_TASK_OD

Achten Sie bitte darauf, für Termine nur Vorgangsarten vom Bus-Typ 2000126 hinzuzufügen – und für Aufgaben nur Vorgangsarten vom Bus-Typ 2000125.

4.4 Events aktivieren & zuweisen

Führen Sie Transaktion **SM30** aus und öffnen Sie die Tabelle *CRMV_FUNC_ASSIGN* zur Pflege. Dort legen Sie bitte den Eintrag wie in der folgenden Abbildung dargestellt, an:

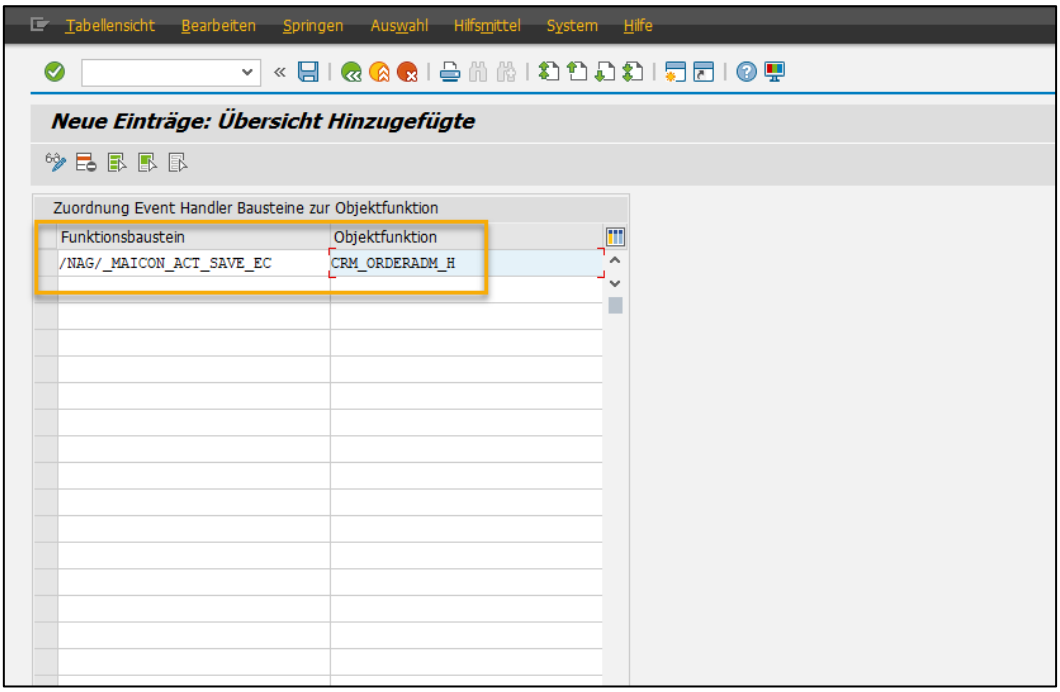

Abbildung 18: SAP – Event Handler Baustein Zuordnung

Bestätigen Sie die Eingabe mit <Enter> und fügen Sie die Anpassung einem Transportauftrag hinzu. Anschließend führen Sie die Transaktion **CRMV_EVENT** aus, klicken auf die Schaltfläche „Callback zu Typ/Obj./Ereignis“, wechseln in den Änderungsmodus und fügen einen neuen Eintrag hinzu.

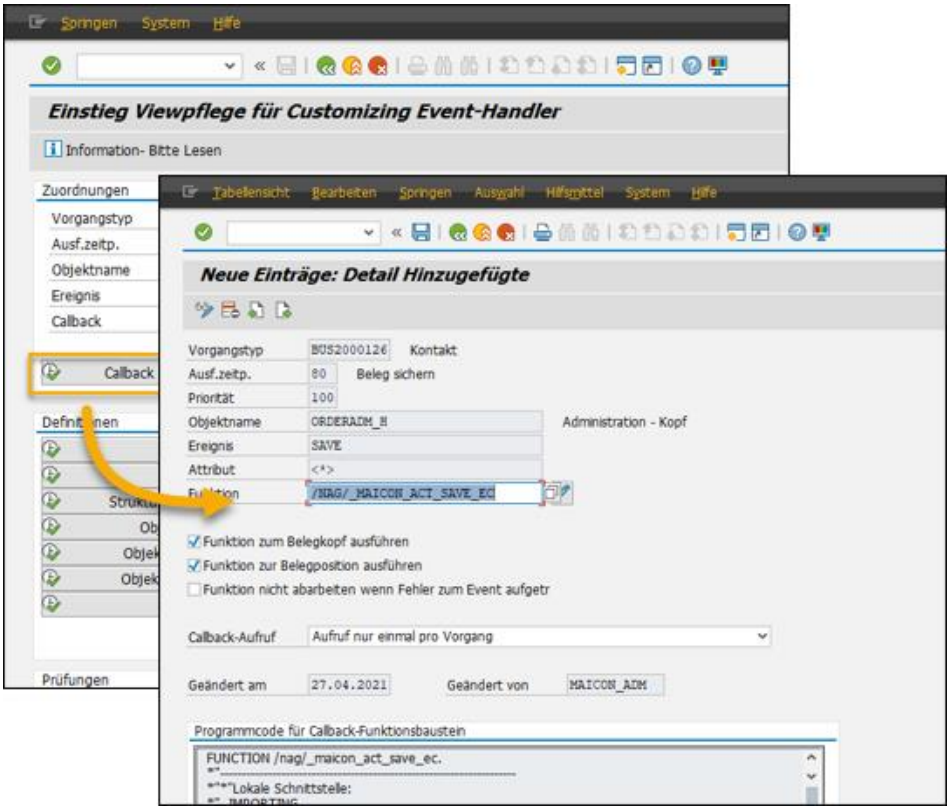

Abbildung 19: SAP – Hinzufügen eines Events

4.5 Einrichten der RFC Verbindung

Führen Sie Transaktion **SM59** aus und legen dort eine neue http-Verbindung zu ext. Server an. Dabei handelt es sich um die maiConnect Verbindung zur SAP BTP.

Öffnen Sie die angelegte Verbindung, wechseln zum Reiter „Technische Einstellungen“ und tragen Sie dort den Host ein, den Sie von Nagarro ES erhalten haben (endet auf …hana.ondemand.com). Als Port tragen Sie bitte *443* ein – den Pfadpräfix lassen Sie frei.

Falls Sie einen Proxy zwischengeschaltet haben, tragen Sie hier bitte die entsprechenden Daten mit ein.

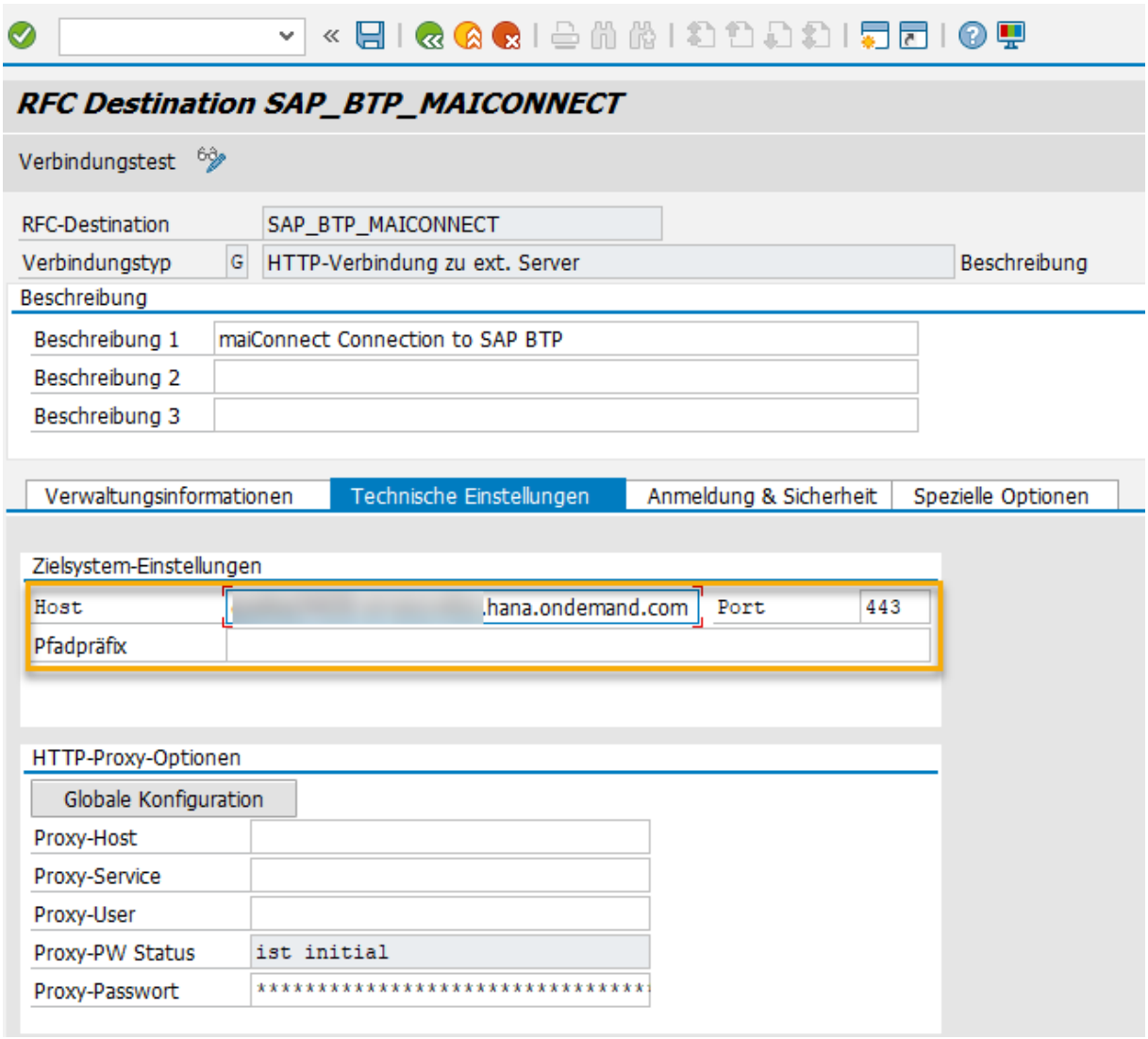

Abbildung 20: SAP – RFC Verbindung – Technische Einstellungen

Wechseln Sie nun zum Reiter „Anmeldung & Sicherheit“, tragen den P- oder S-User für die Basic Authentication mit ein (nehmen Sie den gleichen Benutzer, wie auch schon bei der Einrichtung des Cloud Connectors in Kapitel 3.3) und aktivieren SSL:

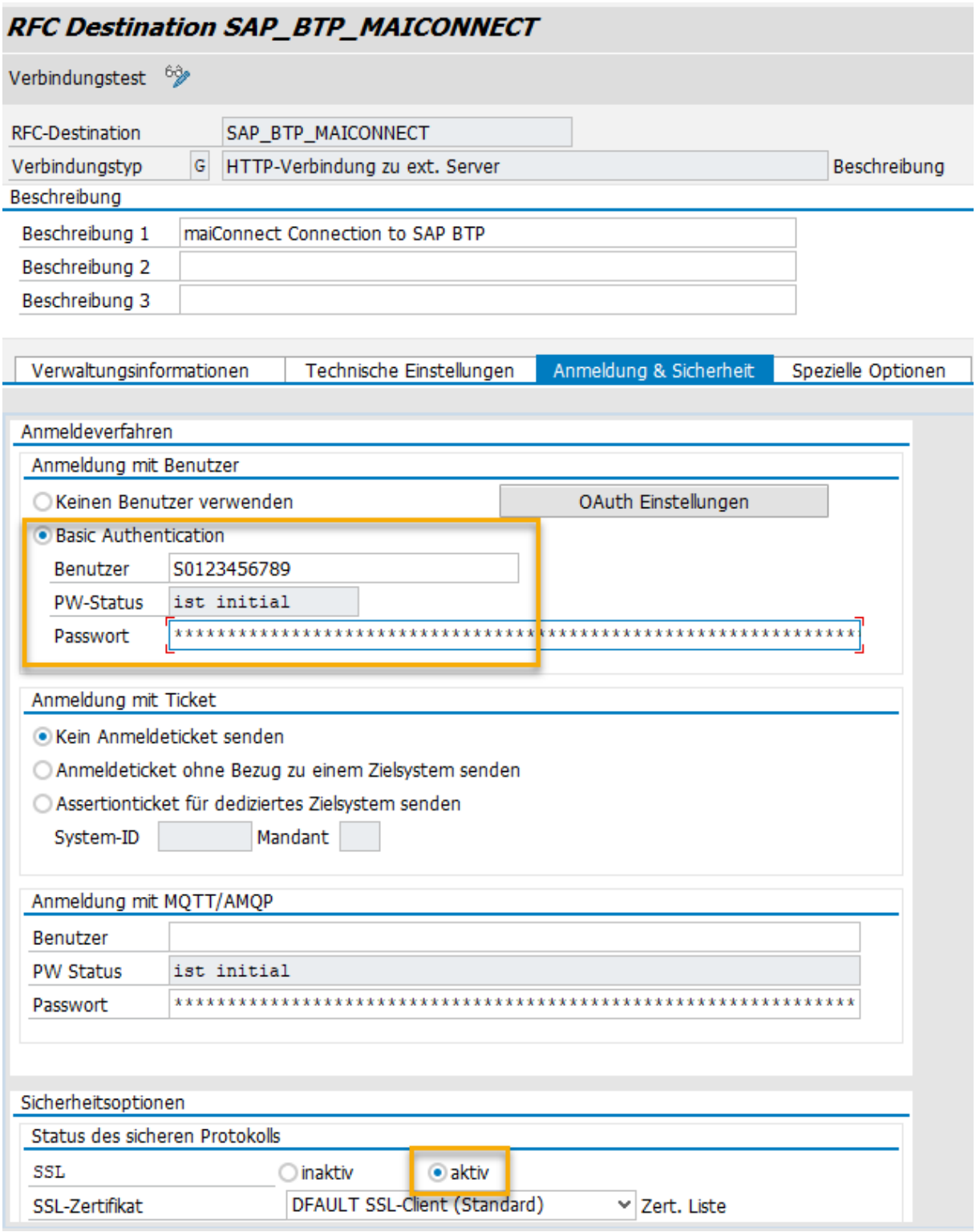

Abbildung 21: SAP – RFC Verbindung – Anmeldung & Sicherheit

Anschließend können Sie einen Verbindungstest durchführen.

Führen Sie nun Transaktion **SM30** aus und öffnen die Tabelle */NAG/MAICONDESTI*. Hier fügen Sie bitte einen Eintrag mit dem Namen der soeben angelegten RFC Verbindung hinzu und speichern die Einstellung:

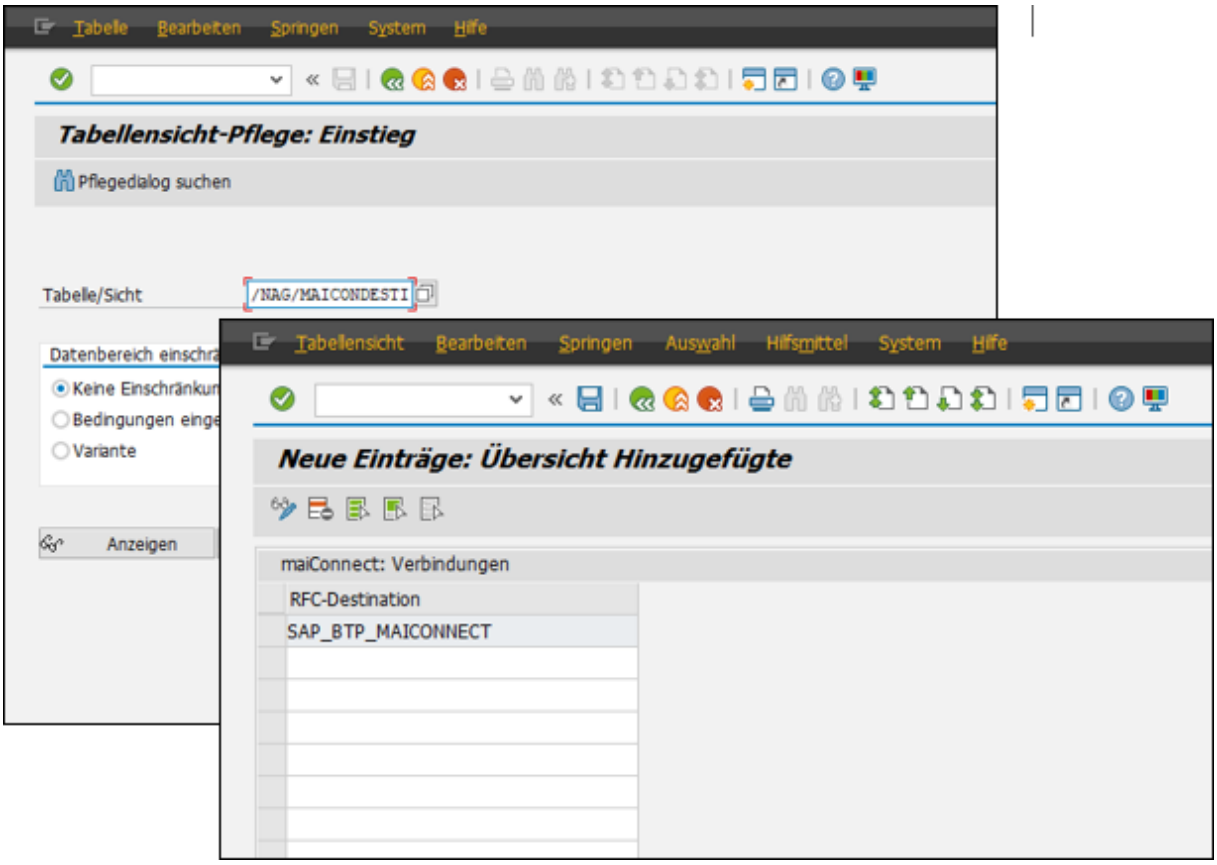

Abbildung 22: SAP - Pflege der RFC Verbindung

Bitte beachten Sie, dass die Einträge dieser Tabelle nicht transportiert werden. Daher muss der entsprechende Eintrag in jedem System, in dem maiConnect eingesetzt wird, manuell gepflegt werden.

4.6 Customizing für die Synchronisation von Kontakten

Die in diesem Kapitel beschriebenen Customizing Einstellungen werden nur benötigt, wenn die Synchronisation von Kontakten als Feature genutzt werden soll. Falls die Kontaktsynchronisation nicht genutzt wird, können Sie mit den Einstellungen im nächsten Kapitel fortfahren.

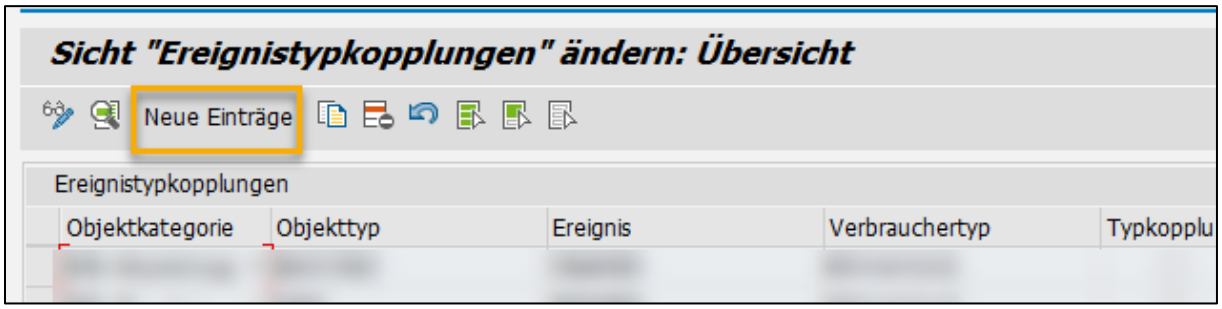

Abbildung 23: Transaktion SWE2 – Hinzufügen von Einträgen für das Customizing

Führen Sie die Transaktion SWE2 aus und legen Sie hier über die Schaltfläche „Neue Einträge“ drei einzelne Einträge an. In den folgenden Abbildungen ist dargestellt, welche Details Sie jeweils angeben müssen.

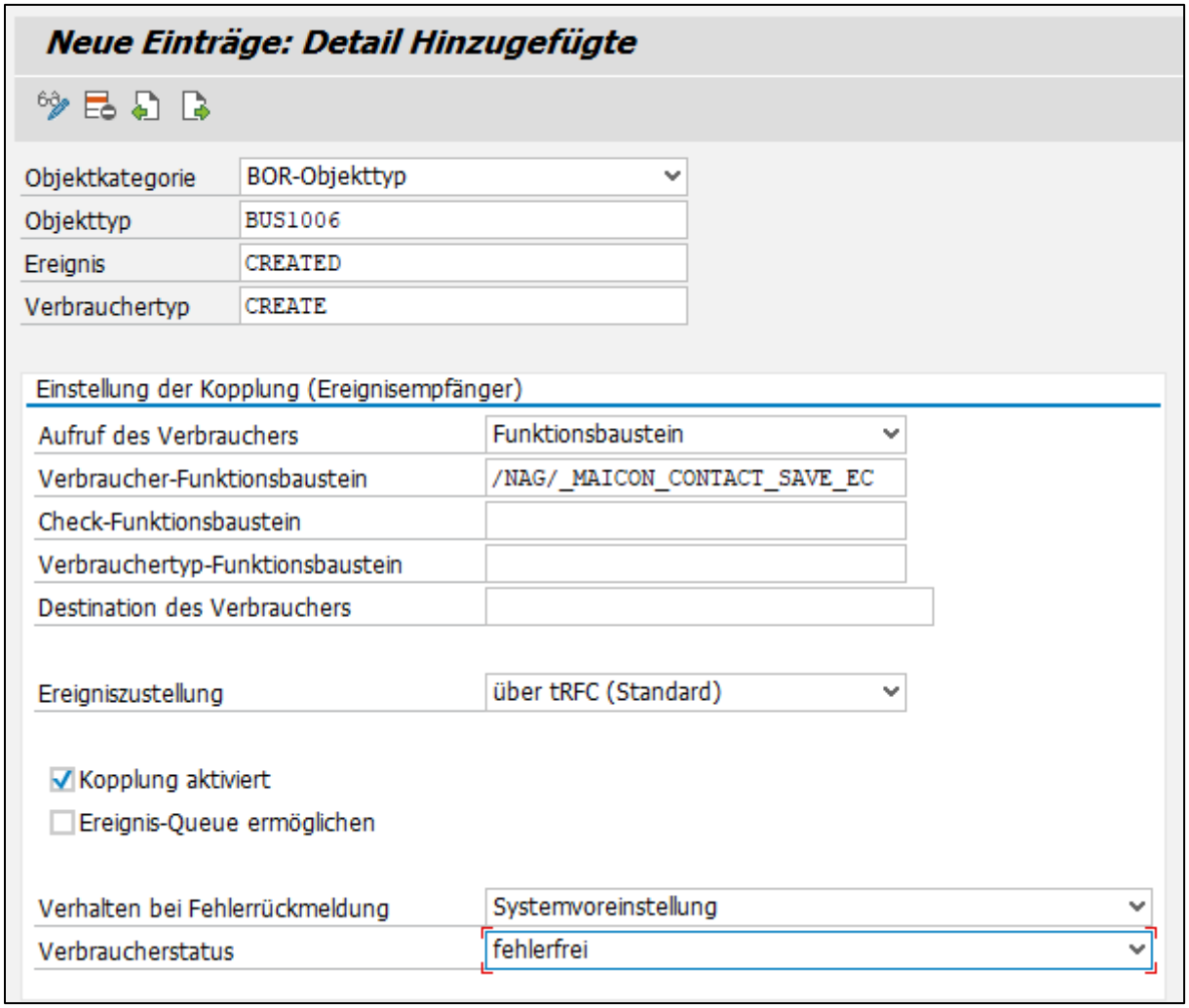

Abbildung 24: SWE2 Eintrag - Anlage

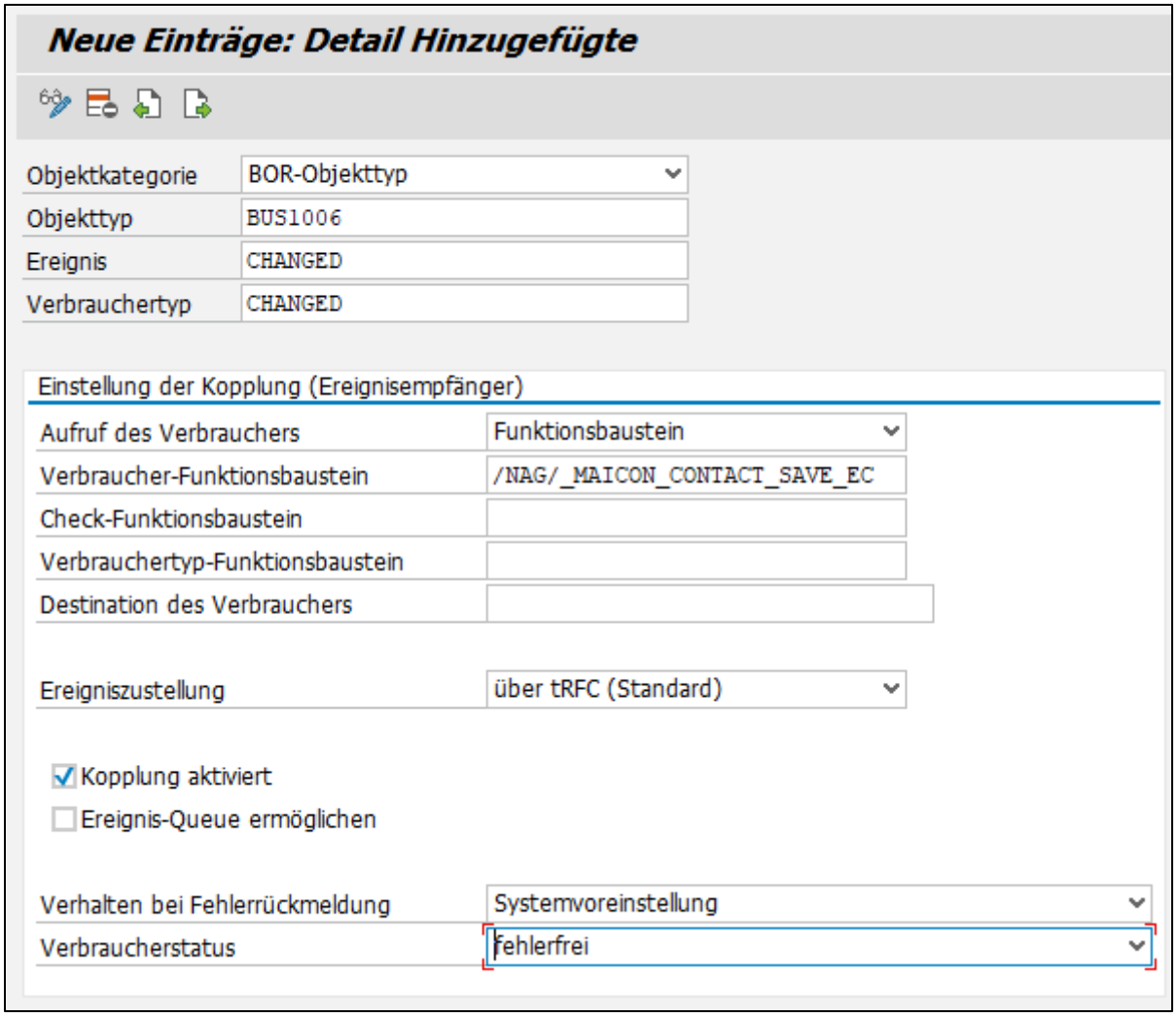

Abbildung 25: SWE2 Eintrag – Änderungen / Updates

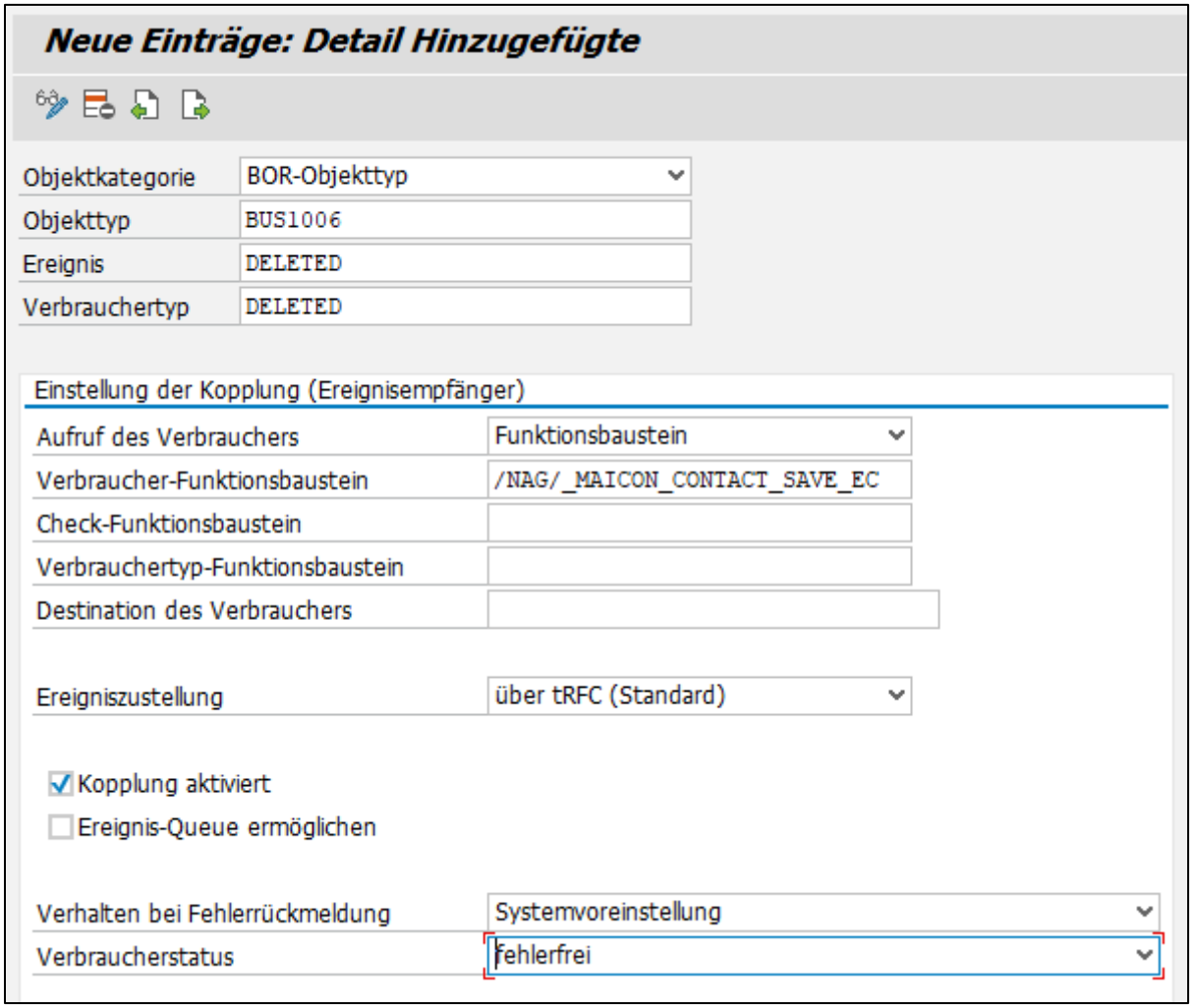

Abbildung 26: SWE2 Eintrag – Löschen

Am Ende speichern Sie diese drei neu erstellten Einträge.

BAdI Implementierung aktivieren

Wenn etwas an den für die Synchronisation relevanten Beziehungen geändert wird, wird kein SAP Standardevent aufgerufen. Um diesen Fall abzudecken, muss nun noch eine BAdI Implementierung angelegt / aktiviert werden.

In der Transaktion SE18 lassen Sie sich bitte das BAdI *BUPA_RELATSHP_UPDATE* anzeigen:

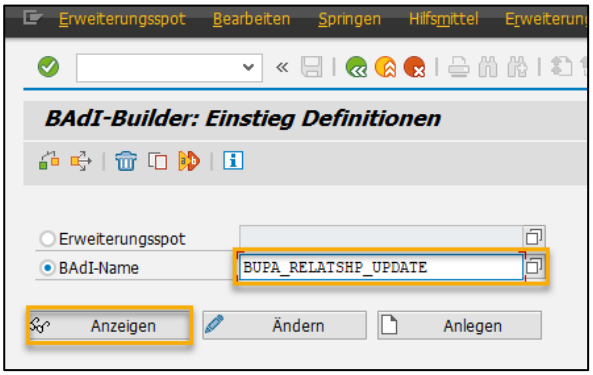

Abbildung 27: SE18

Über die Menüzeile wählen Sie bitte die Option „Implementierung – Anlegen“:

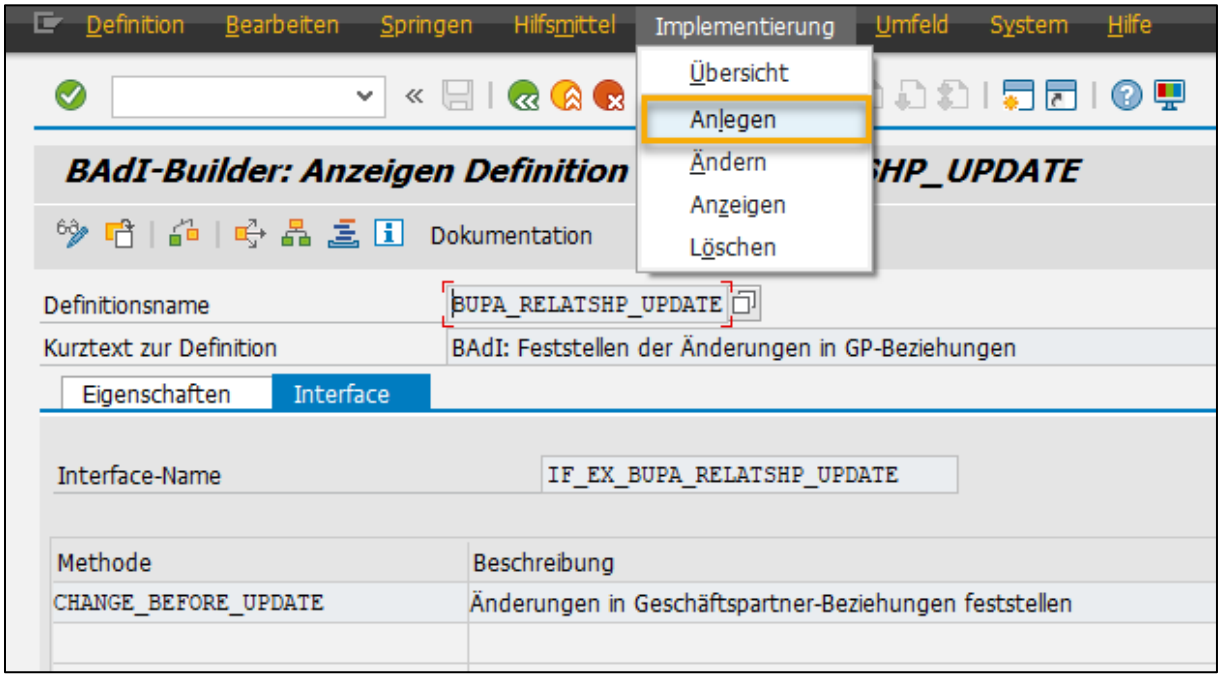

Abbildung 28: BAdI Implementierung anlegen

Vergeben Sie anschließend einen passenden Namen für die Implementierung:

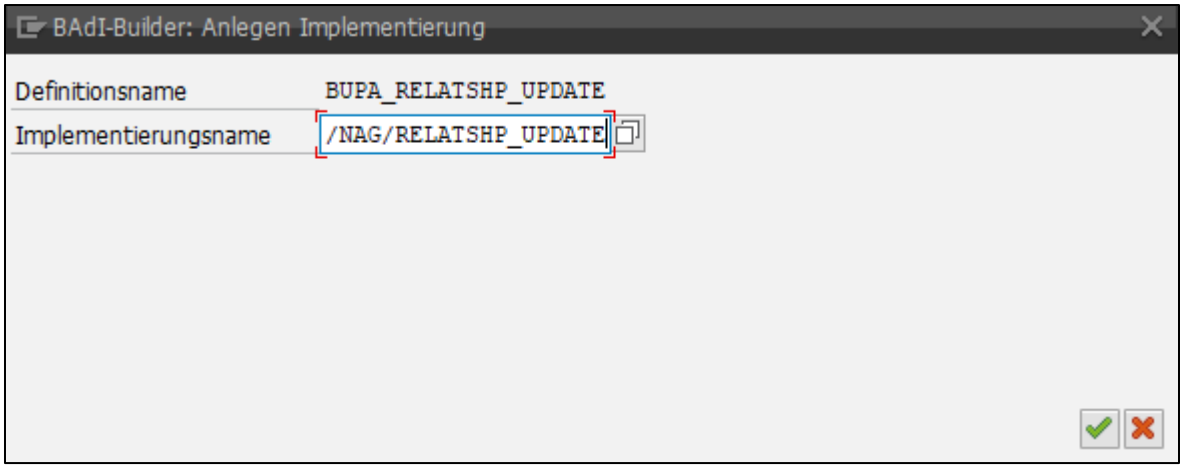

Abbildung 29: Implementierungsname vergeben

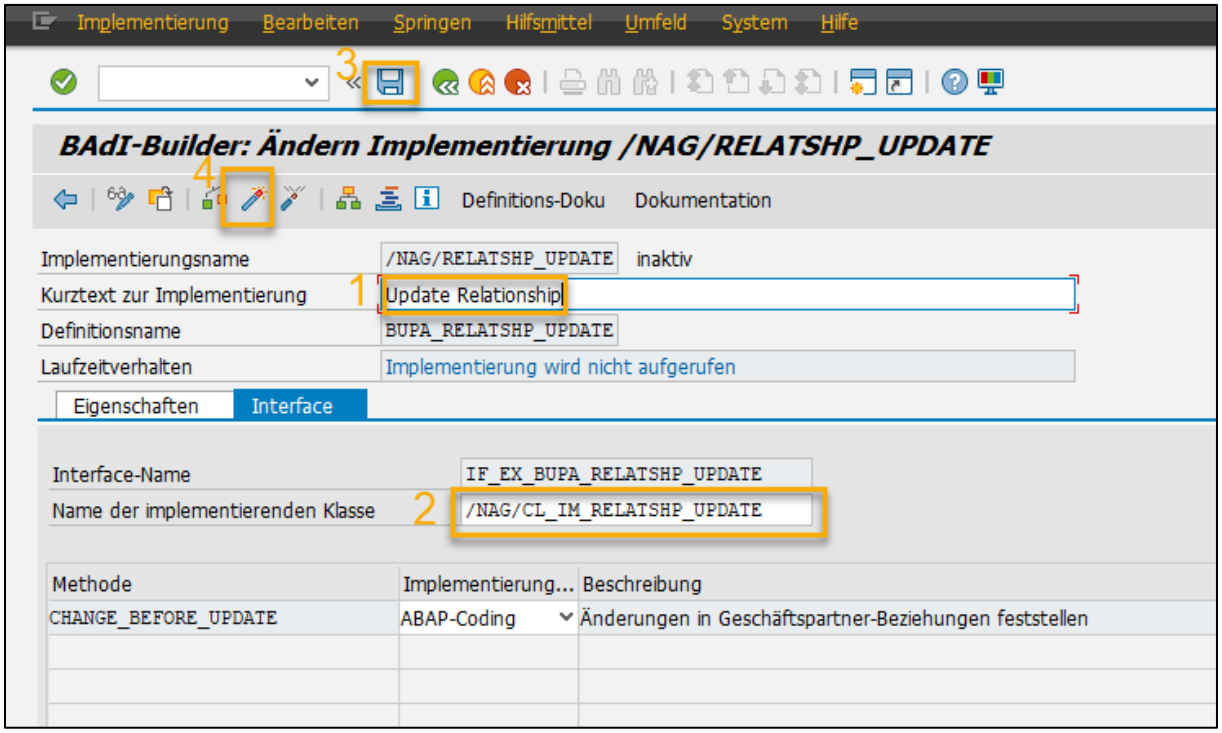

Abbildung 30: Implementierung einrichten und aktivieren

Tragen Sie einen Kurztext ein (1), kontrollieren Sie, ob als Name der zu implementierenden Klasse */NAG/CL_IM_RELATSHP_UPDATE* (2) hinterlegt ist (oder korrigieren Sie dies entsprechend) und speichern Sie die Einstellungen (3). Hierbei muss gegebenenfalls ein Transporteintrag hinterlegt werden.

Anschließend aktivieren Sie die BAdI Implementierung (4).

5 Exchange Server Einstellungen

Folgende Einstellungen müssen am Microsoft Exchange Server durch den entsprechenden Administrator durchgeführt werden.

5.1 EWS und lokale Authentifizierung aktivieren

5.1.1 Lokaler Exchange Server

Am Exchange Server müssen die **EWS**, sowie für die EWS die **Anonymous Authentication** und **Basic Authentication** aktiviert werden.

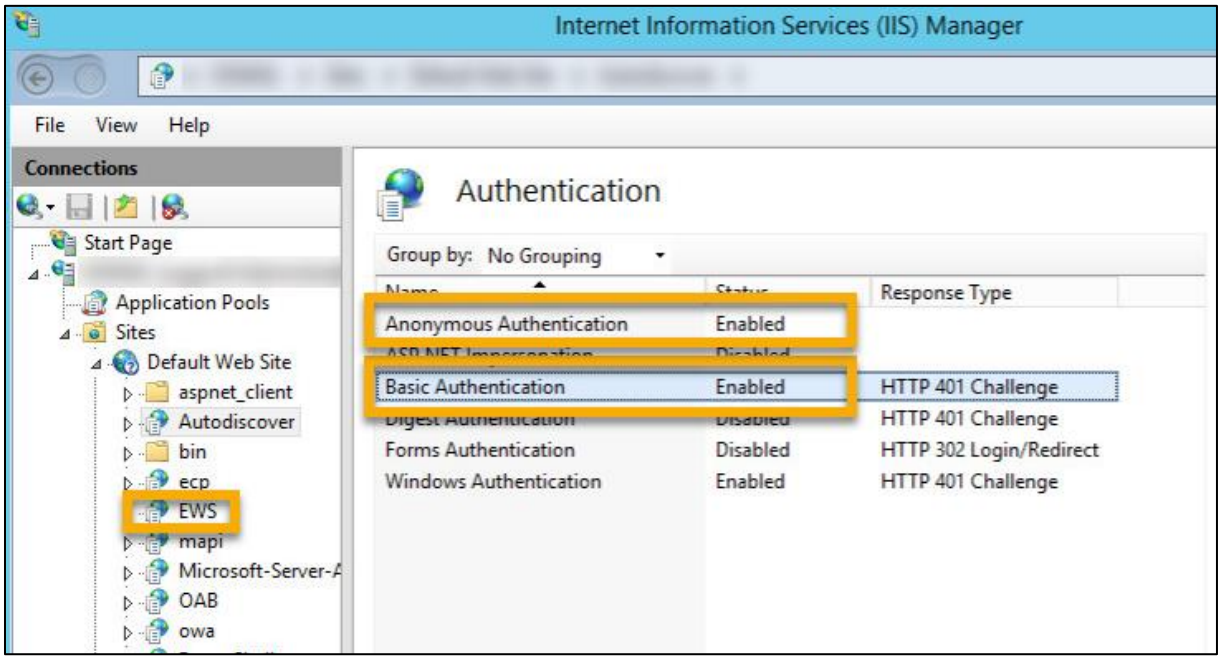

Abbildung 31: Exchange Server – IIS Konfiguration (Beispiel)

Die Einrichtung der Berechtigungen für einen Exchange OnPrem Server ist in Kapitel 5.2.1 beschrieben.

5.1.2 Office 365

In einem Cloud Szenario muss bei Exchange Online **OAuth** aktiviert sein. Das ist standardmäßig der Fall.

Die Einrichtung von OAuth ist im Kapitel 5.2.2 detailliert beschrieben.

5.2 Postfachzugriff einrichten

Um den Zugriff zu gewährleisten, kann entweder ein dedizierter Service-User (Im Sinne eines Kommunikationsbenutzers) oder OAuth verwendet werden.

Bitte beachten Sie, dass der Zugriff über einen Service-User nur bei Exchange onPrem möglich ist. Bei Office 365 wird von Microsoft nur noch der Zugriff über OAuth unterstützt.

5.2.1 Dedizierter Service-User (Exchange onPrem)

Um Änderungen in der Groupware zu verbuchen, verwendet maiConnect einen dedizierten Exchange-User. Dazu muss dieser User über die notwendigen Zugriffsrechte für die Postfächer der Nutzer verfügen.

Die Rechte können dabei auf verschiedene Arten vergeben werden, die sich in dem benötigten Aufwand und der nachträglich nötigen Pflege teilweise stark unterscheiden. Die hier aufgezählten Methoden sind als Beispiele zu verstehen und können für die jeweiligen Bedürfnisse angepasst, erweitert und kombiniert werden. Je nach Exchange-Version und Systemumgebung sind bestimmte Methoden eventuell nicht verfügbar.

5.2.1.1 Rechte auf Postfach-Datenbank-Ebene

Es wird ein zentraler Exchange Benutzer benötigt, der Lese- und Schreibberechtigung auf alle Outlook-Postfächer besitzt. Diese Berechtigung kann über den folgenden Befehl erteilt werden:

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

Dieser Befehl erteilt nur auf das *MailboxDatabase01* Objekt Zugriff - nicht auf die Active Directory Objekte. Gibt es mehrere Mailbox-Datenbanken, so muss der Befehl für jede Datenbank einzeln ausgeführt werden. Allerdings wird über diesen Befehl nur der Zugriff auf alle aktuell existierenden Postfächer erteilt; wird ein neues Postfach hinzugefügt, so muss der Befehl erneut ausgeführt werden. Diese lässt sich gegebenenfalls als Skript einplanen.

5.2.1.2 Rechtevergabe via RBAC

Sofern die RBAC-Rollen angelegt sind, müssen in der Exchange Management Shell zwei Befehle abgesetzt werden (angepasst an die Umgebung):

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

An dieser Stelle wird eine Beschränkung auf eine Teilgruppe der Nutzer des Exchange-Systems angelegt. Anschließend können mithilfe dieser Beschränkung die Zugriffsrechte zugewiesen werden:

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

Die Zuweisung der *ApplicationImpersonation* Rolle kann auch ohne *CustomRecipientWriteScope* erfolgen und bezieht sich dann auf alle Nutzer. Alternativ kann der *CustomRecipientWriteScope* entsprechend der Bedürfnisse (z.B. eingeschränkt auf eine Nutzergruppe) angepasst werden, um die Zugriffsrechte des Service-Users einzuschränken.

5.2.1.3 Einzelzugriff auf Postfächer einrichten

Soll der Zugriff des Exchange Admin Users auf die Postfächer für jedes Postfach gesondert geregelt werden, so muss dieser für die nötigen Zugriffsberechtigungen auf die einzelnen Ordner (Kalender, Aufgaben & Kontakte) erhalten.

Dies kann automatisiert über ein Skript erfolgen, wie im Folgenden kurz beschrieben - oder direkt aus den Postfächern der Anwender.

Skript

Mit dem folgenden Skript kann der Zugriff auf den Kalender aller Benutzer eingerichtet werden:

```
$rooms = Get-Mailbox -RecipientTypeDetails UserMailbox

$rooms | %{Add-MailboxFolderPermission $_":\Kalender" -User folderrights -
AccessRights Owner}
```

Analog auf Englisch:

```
$rooms = Get-Mailbox -RecipientTypeDetails UserMailbox

$rooms | %{Add-MailboxFolderPermission $_":\Calendar" -User folderrights -
AccessRights Owner}
```

Alternativ für ein Postfach:

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

Oder als expliziter Vollzugriff:

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

5.2.2 Autorisierung per OAuth (Office 365)

Wird Office365 verwendet, kann die Autorisierung auch über OAuth erfolgen. Dazu muss maiConnect als Applikation im entsprechenden Azure Active Directory über das Azure Portal https://portal.azure.com/ registriert werden.

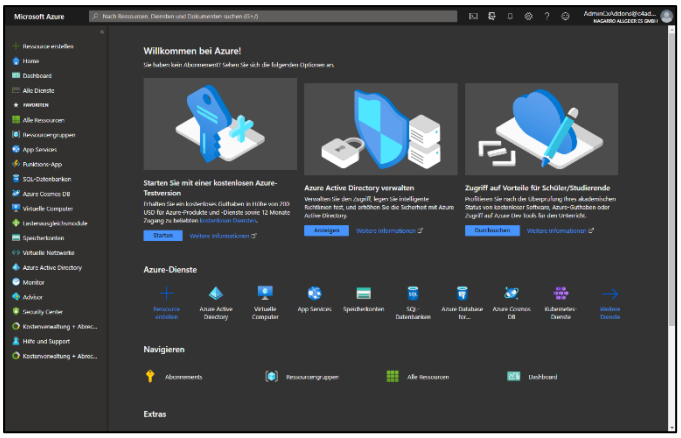

Abbildung 32: Azure Portal - Startseite

5.2.2.1 Registrierung im Azure Portal

Loggen Sie sich mit einem Benutzer, der über Administrator-Berechtigungen verfügt, ein. Navigieren Sie nun zu “Azure Active Directory" -> "App-Registrierungen". Klicken Sie “+ Neue Registrierung":

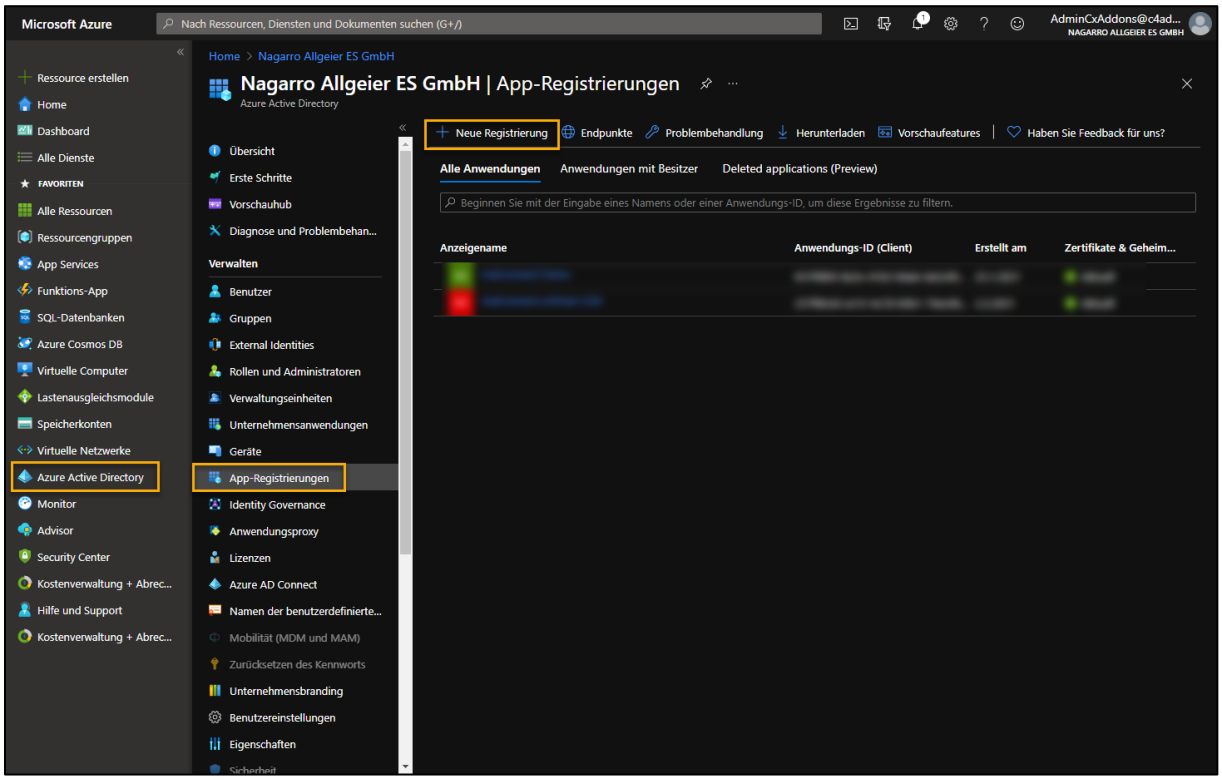

Abbildung 33: Azure Portal – App-Registrierungen

Geben Sie der Applikation einen Namen (z.B. “maiConnect”), wählen Sie einen unterstützten Kontotyp und lassen Sie das Feld „Umleitungs-URI“ frei. Klicken Sie auf “Registrieren”.

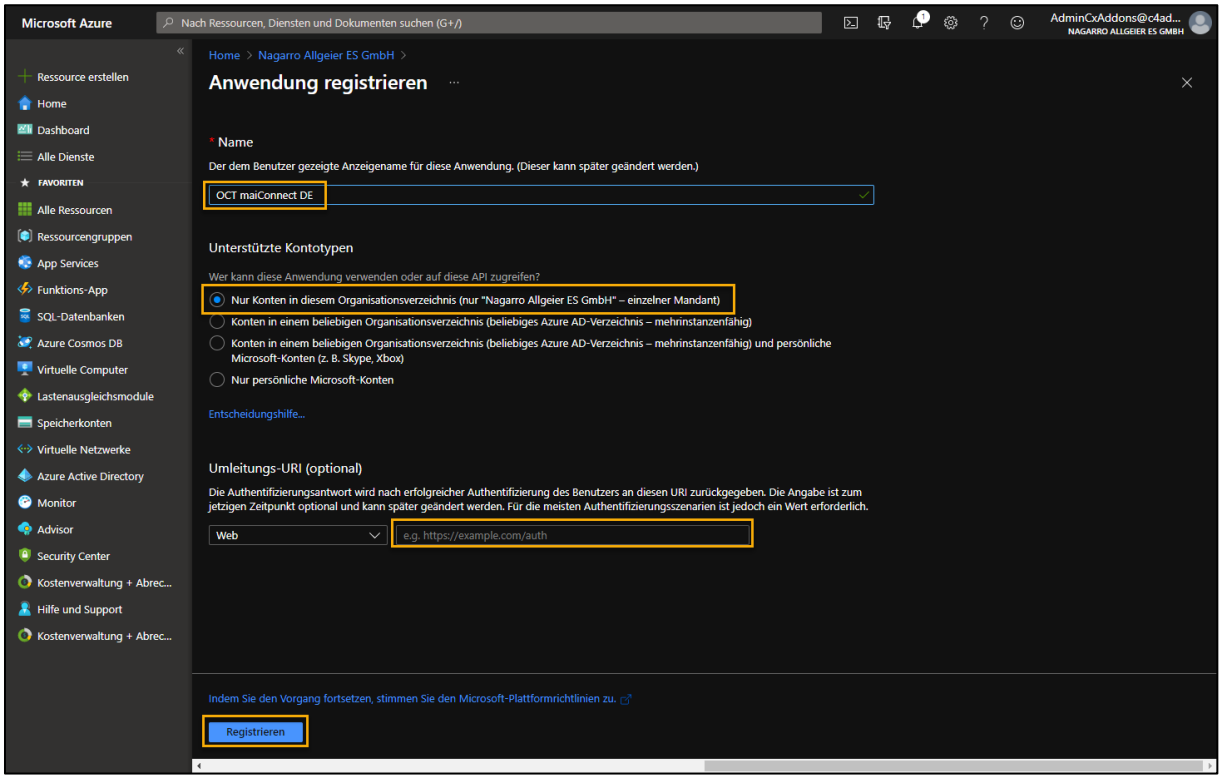

Abbildung 34: Azure Portal – Neue Anwendung registrieren

Mit einem Klick auf den Namen der neu registrierten Applikation kann sie geöffnet werden:

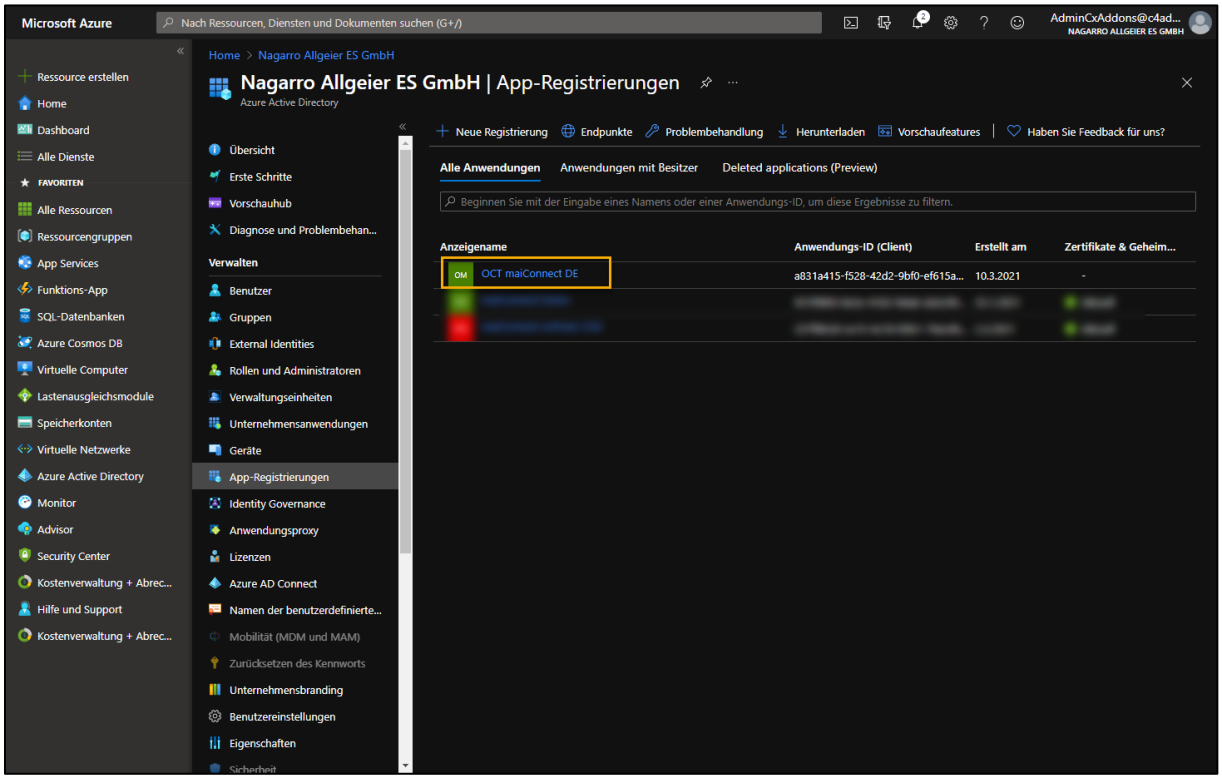

Abbildung 35: Azure Portal – Neu registrierte Anwendung öffnen

Navigieren Sie nun zu den „API-Berechtigungen“:

Abbildung 36: Azure Portal - Übersicht der neu registrierten Anwendung

Fügen Sie über die entsprechende Schaltfläche eine neue Berechtigung hinzu:

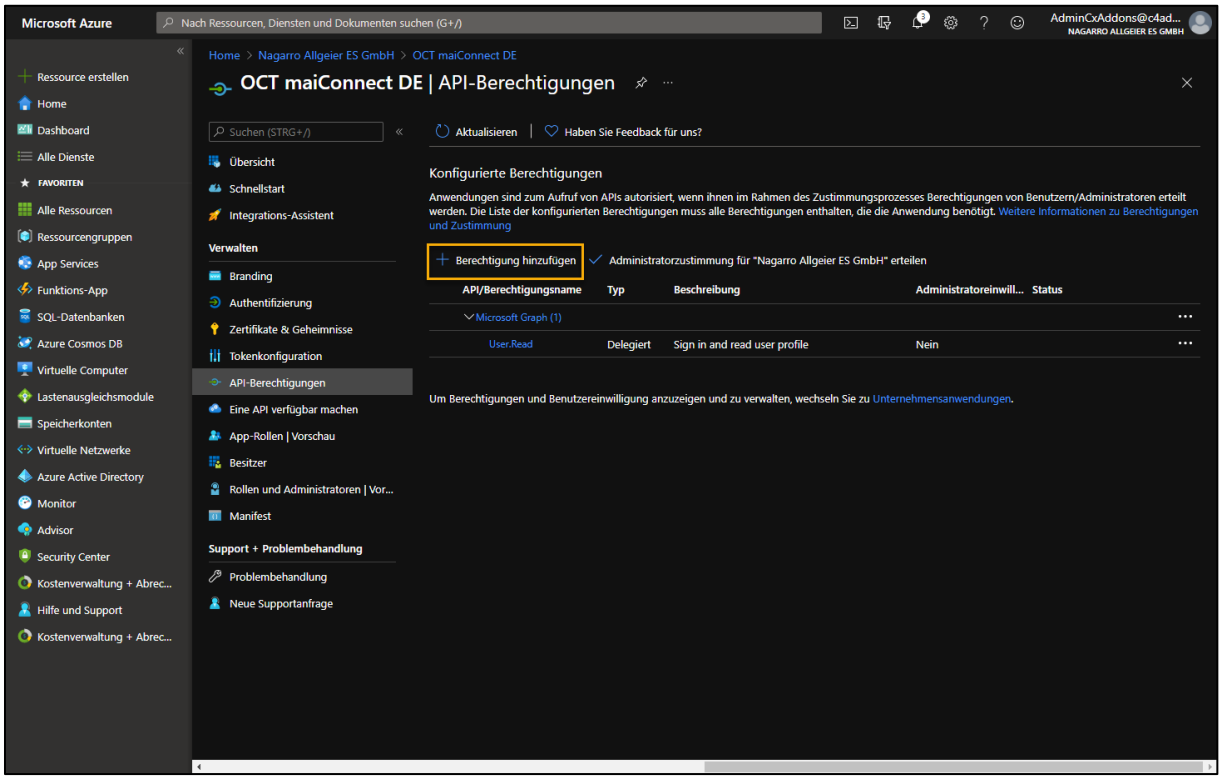

Abbildung 37: Azure Portal – Berechtigung hinzufügen

Wählen Sie zunächst “Von meiner Organisation verwendete APIs” und filtern dann nach “office”. Anschließend können Sie aus den Suchergebnissen den Eintrag „Office 365 Exchange Online“ wählen.

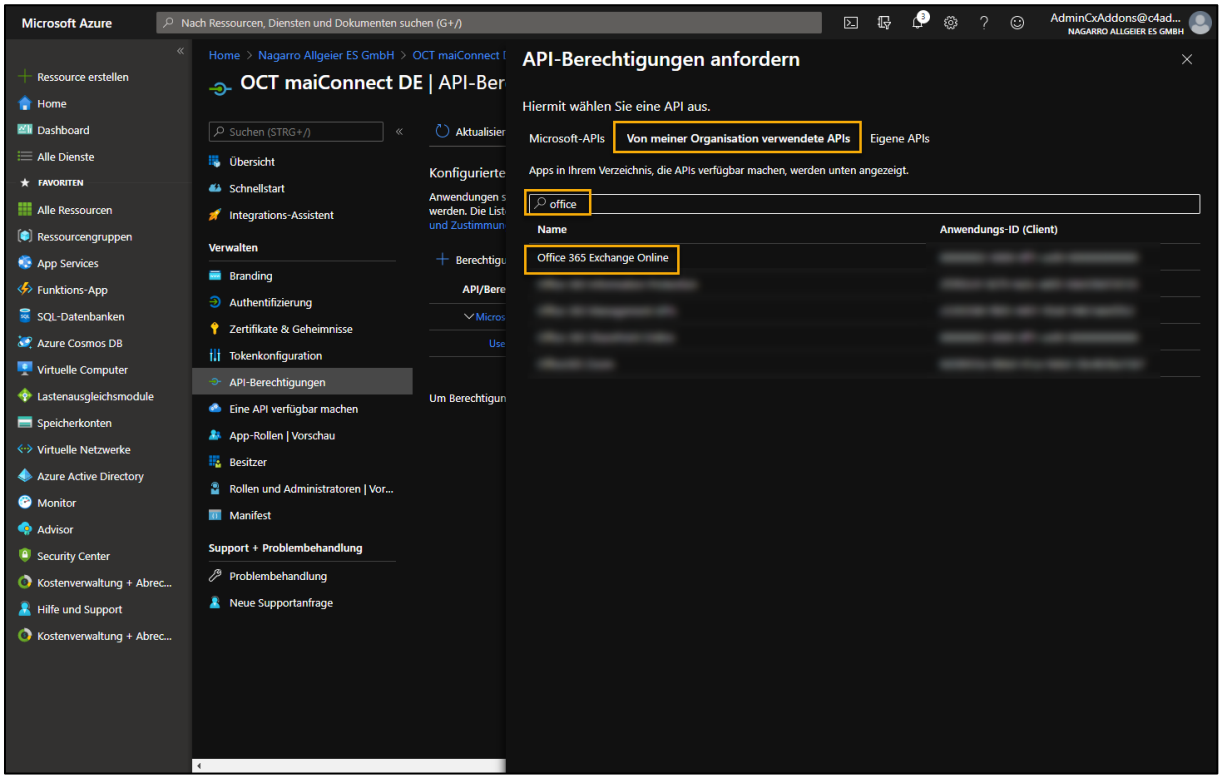

Abbildung 38: Azure Portal – Von meiner Organisation verwendete APIs

Wählen Sie nun “Anwendungsberechtigungen” und setzen Sie das Häkchen vor „full_access_as_app“. Bestätigen Sie die Wahl mit der Schaltfläche am unteren Rand.

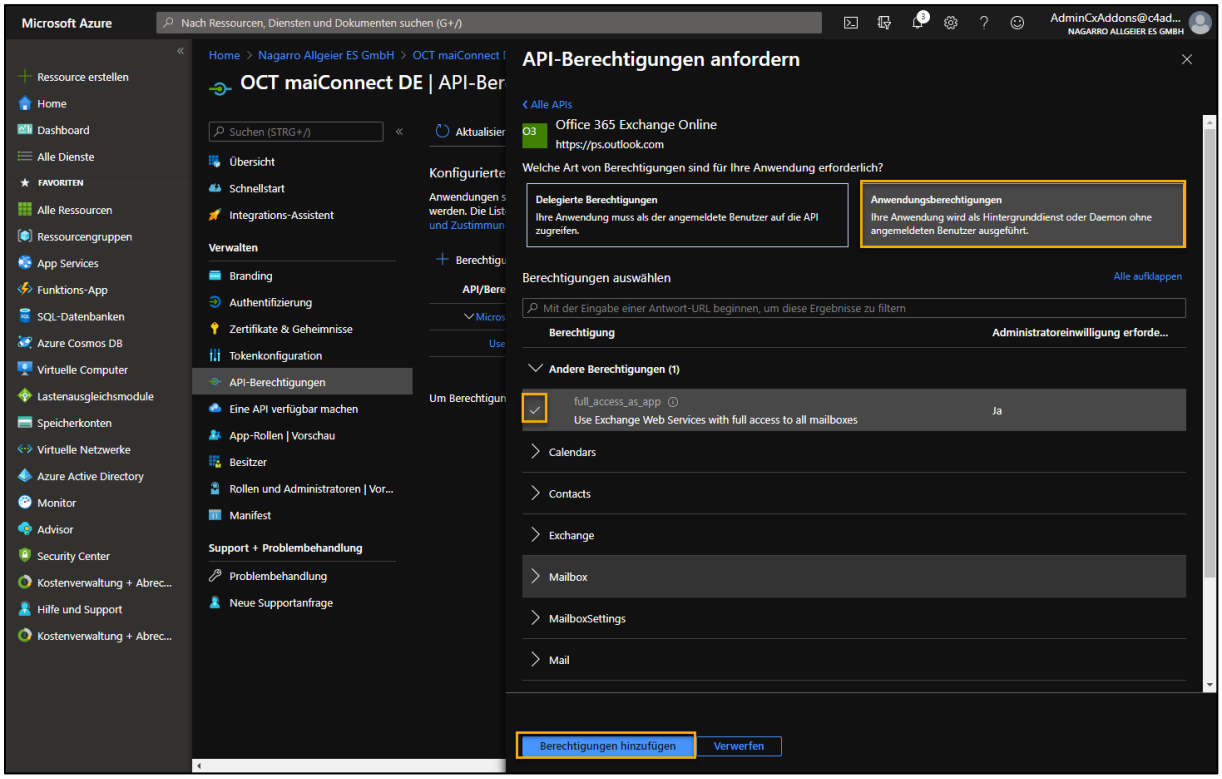

Abbildung 39: Azure Portal - Anwendungsberechtigungen

Im nächsten Schritt muss die Administratorzustimmung für die gerade zugewiesene Berechtigungen erteilt werden.

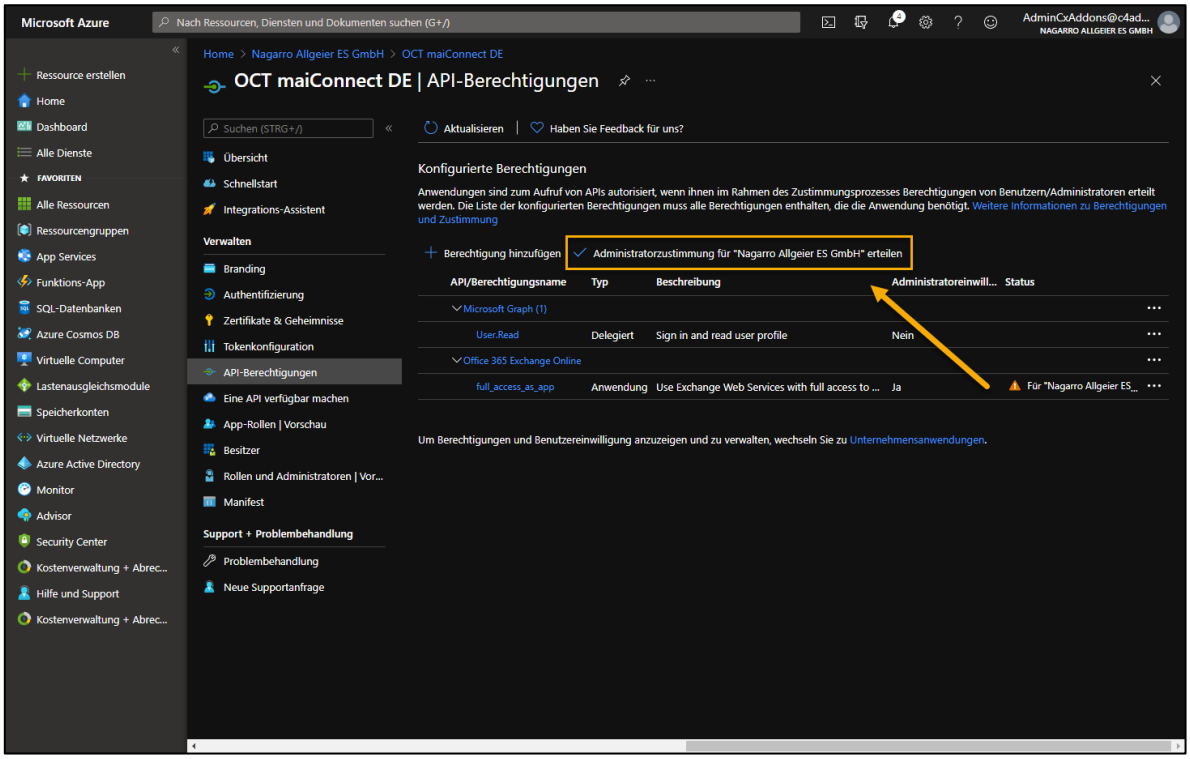

Abbildung 40: Azure Portal - Administratorzustimmung

Nach der Bestätigung im nächsten Popup sollte es so aussehen:

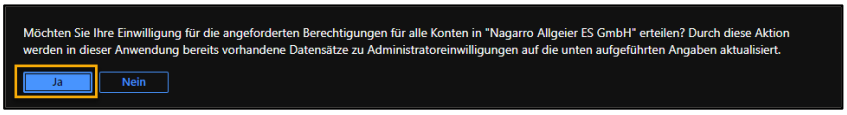

Abbildung 41: Azure Portal – Bestätigen der Berechtigungen

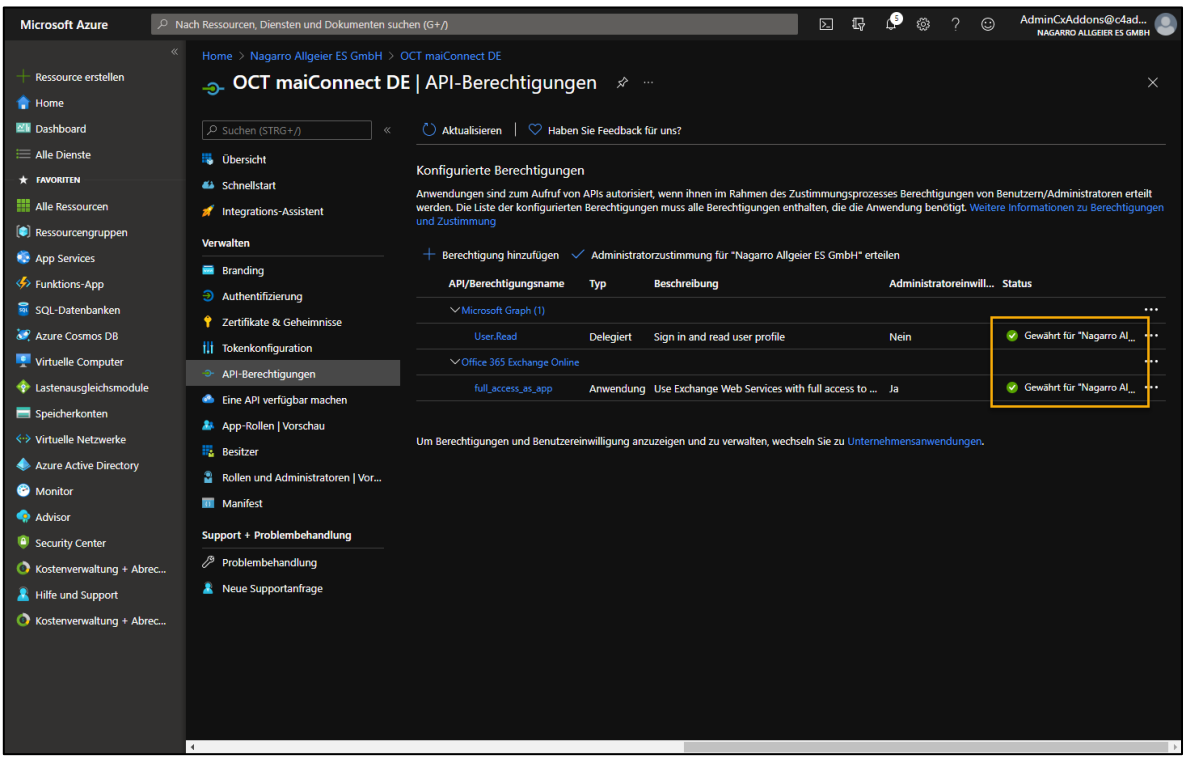

Abbildung 42: Azure Portal - Erfolgreich zugewiesene Berechtigungen

Öffnen Sie nun das “Manifest” und ersetzen Sie den markierten Teil

“keyCredentials”: [ ],

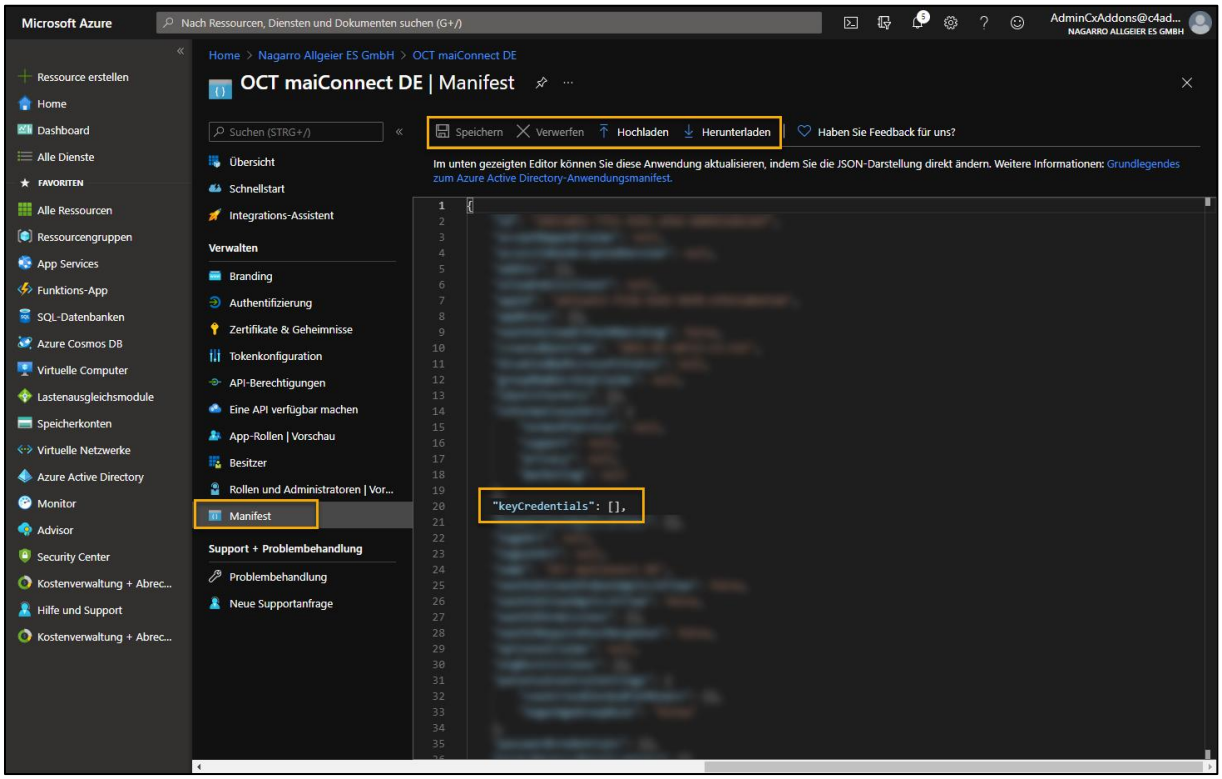

Abbildung 43: Azure Portal - Manifest

mit dem folgenden Code:

```
"keyCredentials": [
    {
      "customKeyIdentifier": "kLqLNhcD5+2/tYSodERz4gkiRPg=",
      "keyId": "5623d3f9-a3fc-44b8-8763-6f429d0c73e9",
      "type": "AsymmetricX509Cert",
      "usage": "Verify",
      "value":
"MIIC4zCCAcugAwIBAgIELnv31TANBgkqhkiG9w0BAQUFADAiMSAwHgYDVQQDExdtYWloaXJv
IEdtYkggbWFpQ29ubmVjdDAeFw0xNjAzMjMxNDQ4MDJaFw0yNjAzMjExNDQ4MDJaMCIxIDAeB
gNVBAMTF21haWhpcm8gR21iSCBtYWlDb25uZWN0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMI
IBCgKCAQEA1vkIAV37wbNN52hVlVAIaUi+Xn/AYcNsNmkNce6xVRdyuElpwkyRGtqpKbfYp1a
KBb9LUbV7U0yILmP0H7PPK4IrYBAGYeXHvyJqRrmGBB8AFgpfpBMxYspKKO7rr4Ze6cWihldX
OumTsehr58VAdJ/64sRwtUr7KFBJOjHfaHAQsGkQvFU4ZapzSmt6c105Dw98ee9HelvsCoMXJ
/ekHziINPZvZSSJJ9eQldF/muj93/FfxmyTADam5USnWLvtJE1W7jWMyHhoMDsHylJiHRCTh/
XEw/Z4SBlZiUi+Qo9c6GJy8C+F2anvrtO+Ly38IRCK2zv8Y4ltOTu8E0iI9QIDAQABoyEwHzA
dBgNVHQ4EFgQUVMnMfq2Rh6uh9rII88vJDU2/aw4wDQYJKoZIhvcNAQEFBQADggEBAGshmdg5
Ra/3Ork1C3w7azbaTbnK9uVqcKrI6T+89kD2lCsPWBlYnVJYDMdV4xn5YqqjfoGVIVnwqVGwC
Cg76Gqkv6Cc6AcXS1sfeR0iyEf8Ywkigpblv+GdixzYbWZV7wJVWItVA2Cw2nlW+O5x5juUqB
jL1t1AFcr7il+ffFVEv10pNBpO0448dAzgKuOrQtX62cD1KCarB+005yDrj5fyMRp5w/7nf9J
pyvn40bPh5pgEDU2IlmjzrVZrmlT81HJn3jUBfV2+iJjLQLxu8DaP6rpsgUvf1qyXGEzx/o9+
TFS01M4JBn4vdPRTon8WOOaRzGVICh1JVGHh112kiyo="
    }
],
```

Dabei können Sie den Text entweder direkt über das Azure Portal bearbeiten oder alternativ das Manifest als JSON Datei herunterladen, diese mit einem Editor öffnen und bearbeiten, sie speichern und die Datei neu hochladen.

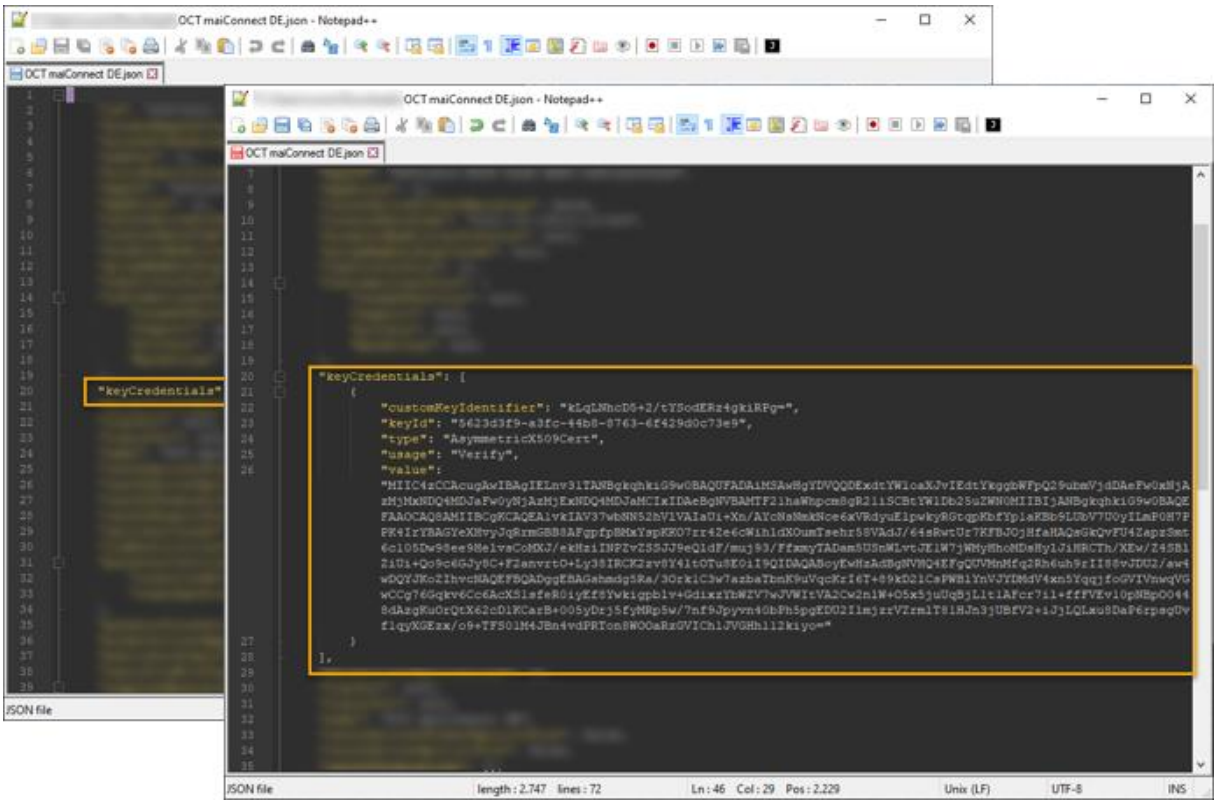

Abbildung 44: Bearbeiten des Manifests im Editor

Stellen Sie sicher, die geänderte Datei am Ende zu speichern:

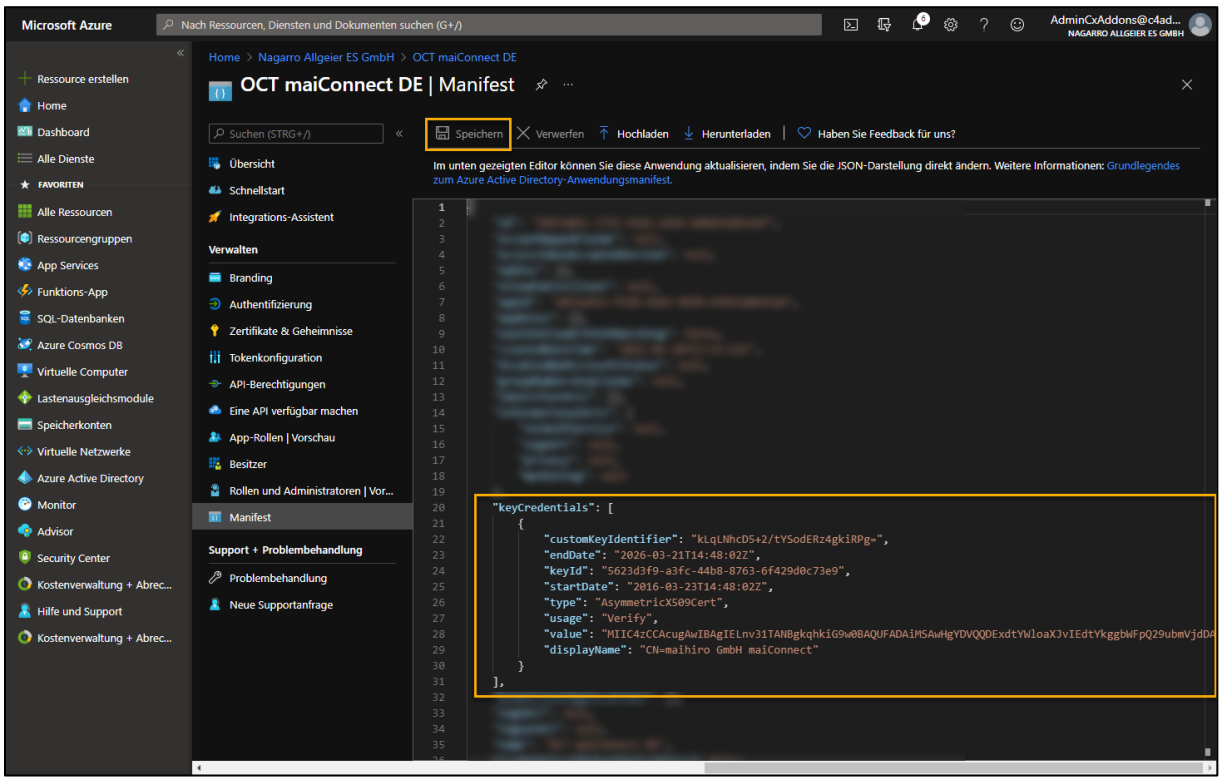

Abbildung 45: Azure Portal – Speichern des aktualisierten Manifests

Gehen Sie nun zurück zur Übersichts-Seite der Applikation und notieren Sie die „Anwendungs-ID (Client)“. Anschließend klicken Sie auf „Endpunkte“:

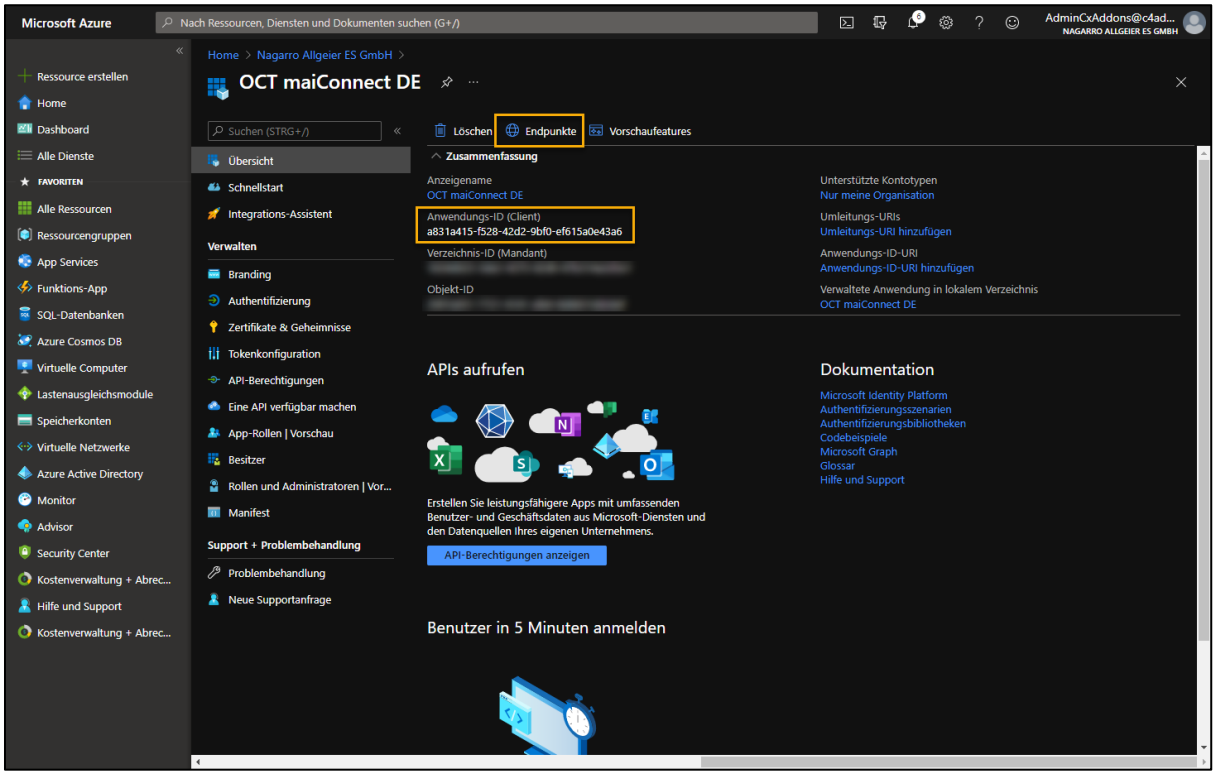

Abbildung 46: Azure Portal – Anwendungs-ID

Aus der Liste von Endpunkten wählen Sie bitte den im unteren Bild markierten aus und stellen Sie diesen zusammen mit der Anwendungs-ID dem Administrator zur Verfügung, der für die maiConnect-Einrichtung verantwortlich ist.

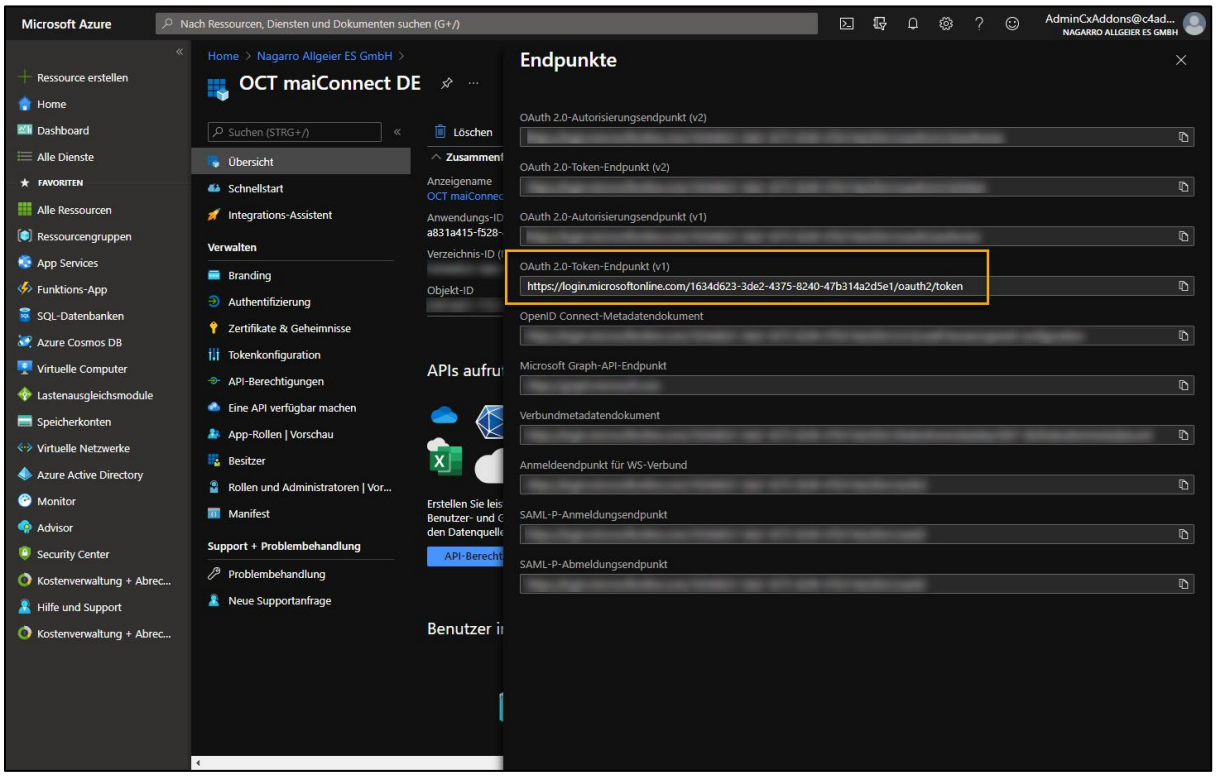

Abbildung 47: Azure Portal – Endpunkte

5.2.3 Hinweis zu den Azure API-Berechtigungen

Entsprechend der obigen Beschreibung im Microsoft Azure erfordert maiConnect für die EWS-Schnittstelle die Anwendungsberechtigung „full_access_as_app“. Das bedeutet, dass die maiConnect-Applikation theoretisch den Zugriff auf alle Postfächer hat.

Über das maiConnect AdminCockpit wird festgelegt, für welche Benutzer die Synchronisation stattfinden soll. Nur für die hier konfigurierten Benutzer findet ein Zugriff auf das Postfach statt. Andere Postfächer sind maiConnect gar nicht bekannt. Darum wird hiermit versichert, dass auf keine anderen Postfächer zugegriffen wird als auf die konfigurierten maiConnect-Benutzer.

Darüber hinaus bietet Microsoft Azure die Möglichkeit über eine ApplicationAccessPolicy den Zugriff auf einzelne Postfächer zu steuern. Siehe dazu die folgende Seite:

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

Um eine neue ApplicationAccessPolicy zu erstellen, muss folgendes Kommando in der Exchange Online PowerShell ausgeführt werden:

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

- AccessRight: DenyAccess (Zugriff verbieten) / RestrictAccess (Zugriff zulassen)
- AppID: ID der Azure AD Applikation
- PolicyScopeGroupId: UPN der User oder Name der Gruppe

Die einfachste Anwendung dieser Richtlinie ist, die Anlage einer RestrictAccess Policy für eine Applikation mit Zugriff auf die notwendigen Postfächer. Zugriff auf nicht in der Richtlinie hinterlegten Postfächer wird unterbunden.

5.3 Exchange Throttling Policy

Über eine Throttling Policy kann die Anzahl der Verbindungen pro Exchange Account begrenzt werden. Besondere Bedeutung hat hier der Parameter *EWSMaxConcurrency*.

Die folgenden Fehler beschreiben, wie eine Throttling Policy für maiConnect festgelegt werden kann.

Bitte beachten Sie, dass Office365 diese Einstellungsmöglichkeiten standardmäßig nicht zulässt und für Exchange 2013 bestimmte Parameter nicht mehr existieren!

Policy Namen anlegen

```
New-ThrottlingPolicy MaiConnect
```

Limitierung für den Service-User entfernen

```
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
```

Service-User der Policy zuweisen

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

5.4 Verbindung zwischen Exchange und SAP BTP

Für den Zugriff auf den Exchange Server verwendet maiConnect die EWS-Schnittstelle (Exchange Web Service) von Microsoft. D.h. Abfragen oder Änderungen werden durch Web Services von der SAP BTP auf dem Exchange Server durchgeführt. Je nach Netzwerk Topografie und Sicherheitsrichtlinien der maiConnect Kunden können diese Web Service Calls über einen Proxy oder eine Firewall laufen, die die Anfrage an den entsprechenden Exchange Server weiterleiten.

Für die Synchronisation von Exchange in Richtung SAP BTP werden Subskriptionen für jedes Postfach angelegt. maiConnect wird dadurch über Änderungen (Anlage, Aktualisierungen oder Löschungen) in einem subskribierten Postfach per Push Notifikationen benachrichtigt. Die Benachrichtigungen werden verarbeitet und eine Antwort an den Exchange Server zurück gesendet. Falls maiConnect nicht antwortet, z.B. aufgrund einer Downtime, schickt der Exchange Server die Anfrage erneut. Sollte nach mehreren Versuchen nicht auf die Nachricht geantwortet werden, wird die Subskription auf dem Exchange Server automatisch gelöscht. Beim Hinzufügen von Benutzern über das maiConnect Admincockpit werden die Subskriptionen automatisch angelegt. Wenn Subskriptionen auf dem Exchange Server für bestimmte Mailboxen gelöscht wurden, läuft in maiConnect ein Hintergrund-Job, der die Subskriptionen erneuert. In dem Fall werden mit Hilfe eines Wasserzeichens alle entgangenen Änderungen repliziert.

Beim Erstellen der Subskription wird eine Callback-URL angegeben, zu der die Benachrichtigungen des Exchange Servers gesendet werden soll. Diese kundenspezifische URL wird für die Einrichtung auf Seiten des S4/HANA Systems benötigt und wird dem Kunden bei der Einrichtung von maiConnect durch Nagarro ES zur Verfügung gestellt.

Siehe diese Info-Grafik von Microsoft zu den Push-Notifications.

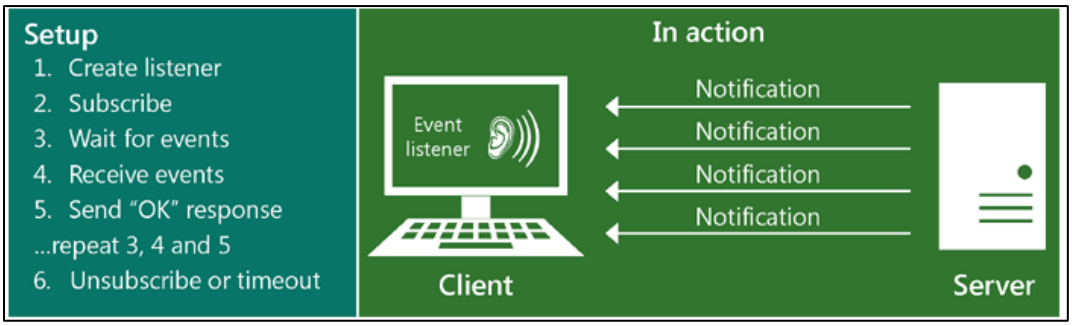

Abbildung 48: Push Benachrichtigungen

Weitere Informationen zu den Push-Benachrichtigungen finden Sie hier:

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

Der Kunde muss gewährleisten, dass die Verbindung von Exchange zur SAP BTP über die EWS sicher ist. Ebenfalls muss von dem Kunden sichergestellt werden, dass die Callback-URL der Subskriptionen vom Exchange Server aus erreichbar ist.

Die Netzwerkumgebung ist kundenspezifisch und daher liegt die Einrichtung der obengenannten Punkte auf Seite des Kunden. Stellen Sie daher bitte sicher, dass die Kommunikation zwischen SAP BTP und Exchange Server nicht durch einen Reverse Proxy oder die Firewall blockiert wird!

Die Kommunikation zwischen SAP BTP und Exchange findet verschlüsselt statt. Die SAP BTP besitzt ein Zertifikat von Baltimore Cybertrust Root. Im Regelfall ist das bei einem Exchange Server bereits vorhanden.

Bei den Push Notifications wird eine Verbindung von Exchange zur SAP BTP aufgebaut. Falls diese nicht zustande kommt, prüfen Sie bitte, ob Baltimore Cybertrust auf dem Exchange als vertrauenswürdig eingestellt ist und ob das Zertifikat aktuell ist.

Wenn die Verbindung zum Exchange Server per SSL mit einem Zertifikat abgesichert ist, dann muss das Zertifikat von bestimmten vertrauenswürdigen Zertifizierungsstellen ausgestellt worden sein. Eine Liste der von SAP akzeptierten Zertifizierungsstellen gibt es hier:

https://wiki.scn.sap.com/wiki/display/CLOUD/Trusted+Certificate+Authorities

Wenn beim Kunden ein Proxy-Server verwendet wird und die Verbindung von Exchange in Richtung SAP BTP nicht erfolgreich hergestellt werden kann, dann muss eine ausgehende Freigabe-Regel im Proxy aktiviert werden, um die Kommunikation zu ermöglichen.

6 Abbildungsverzeichnis