PUBLIC
SAP Service and Asset Manager
Document Version: 2305 – 2024-11-22

SAP Service and Asset Manager Quick Start Guide

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Document History

Before you begin reading this guide, be sure that you have the latest version. Find the latest version at https://help.sap.com/docs/SAP_SERVICE_ASSET_MANAGER.

The following table provides an overview of the most important document changes.

Document Version	Date	Description of Changes
1.0	JUN 2023	Original release of the *SAP Service and Asset Manager Quick Start Guide* guide, version 2305

2 SAP Service and Asset Manager Installation Requirements

To configure the infrastructure for the SAP Service and Asset Manager, you need the following system prerequisites:

SAP Back-End Landscape

- SAP S/4HANA on-premise edition:
  - 1610 FPS 01 or higher, 1709, 1809, 1909
  - SAP ERP 6.0 enhancement package 7 or 8
- SAP Netweaver Gateway: SAP_GWFND 7.40 SP17 or later
- Cloud Connector
- SAP Mobile Add-On

> **Note**
>
> The SAP Mobile Add-On, known as Mobile Application Integration Framework, is embedded in SAP S/4HANA 1909.

SAP Business Technology Platform

- SAP Business Technology Platform user account with authorizations included for the SAP Business Technology Platform subaccount
- Cloud Foundry only: *Mobile Services* and *Application Runtime* are provisioned in the SAP Business Technology Platform subaccount
- The application MDK is created in SAP Business Technology Platform Mobile Services

Build the SAP Service and Asset Manager Client

- According to your site needs, obtain either or both the SAP Service and Asset Manager for iOS and the SAP Service and Asset Manager for Android mobile clients
- Download the SAP Service and Asset Manager application from either the iOS App Store or the Android Google Play Store
- Ensure you have either an onboarding URL or QR code

2.1 Supported Languages

The SAP Service and Asset Manager application supports the following languages:

- ar001 - Arabic
- bg_BG - Bulgarian
- zh_hans - Simplified Chinese
- zh_hant - Traditional Chinese
- csCZ - Czech Republic
- daDK - Danish
- nlBE - Dutch
- elGR - Greek
- enUS - English
- frFR - French
- deDE - German
- heIL - Hebrew
- hrHR - Croatian
- huHU - Hungarian
- inID - Indonesian
- itIT - Italian
- jaJP - Japanese
- koKR - Korean
- nbNO - Norwegian
- plPL - Polish
- ptBR - Portugese
- roRO - Romanian
- RuRU - Russian
- srSP - Serbian
- skSK - Slovak
- slSL - Slovenian
- esES - Spanish
- svSE - Swedish
- thTH - Thai
- trTR - Turkish
- viVN - Vietnamese

2.2 SAP S/4HANA or SAP ERP On-Premise System Setup

Procedure

1. **Activate SAP Service and Asset Manager BC sets:**
   a. Use transaction code *SCPR20* to implement the following:

SAP Service and Asset Manager BC Set	Implementation Scenario
/MERP/SAP_SRV_ASSET_MANAGER_<XXXX>>_REF **Note** Replace the *<XXXX>* with the application release version. For example, *2010*.	Standard Plant Maintenance execution business processes. This BC set includes usage of Asset Central, Crew Management, Customer Service, and Field Operations Worker

   b. Click the *Activate* button.

2. **Set up MAIF number range by executing transaction *SNRO*.**

   MAIF uses the *Number Range* object to generate a readable record ID for runtime data. Maintain these number ranges as follows:

Number Range Object	Interval	Usage
/MFND/CS1	01	Client state record ID
/MFND/DQ1	01	Dependent queue record ID
/SYCLO/C_2	01	Push instance record ID

3. **Activate HTTP Services by using transaction *SICF* (HTTP Service Hierarchy Maintenance)**

   Activate HTTP services for the ConfigPanel and the Administration and Monitoring tool using the following information:

ICF Service Path	Description
/default_host/sap/bc/webdynpro/syclo	Activates service node including subnode

   a. Verify that service activation is completed through transaction */SYCLO/ADMIN*.
   b. Activate any other ICF services required for Web Dynpro application as prompted.

4. **Define user roles and authorizations through transaction *PFCG* (Role Maintenance)**

Define the user role with required authorization for SAP Service and Asset Manager and MAIF using the following information:

Authorization	Description
Authorization object: /MERP/SAM Activity: Execute	Regular SAP Service and Asset Manager user
Authorization object: /SMFND/A01 Activity: Delete	Admin user who can run system purge utility programs

2.2.1 Mobile Add-On for SAP S/4HANA

Add the SAP Mobile Add-On for SAP S/4HANA systems alongside the requisite service packs in order to provide the required OData services for specific versions of SAP Service and Asset Manager.

The following versions of Mobile Add-On for SAP S/4HANA are available for compatible SAP S/4HANA 1610 FPS01 systems and newer:

Software Component	Release	Support Package
SAP S/4HANA on-premise edition	1610	Feature Pack Stack (FPS) 01 or higher
SAP S/4HANA on-premise edition	1709	1709
SAP S/4HANA on-premise edition	1809	1809
SAP S/4HANA on-premise edition	1909 (see Note)	1909 (see Note)

> **Note**
>
> Running SAP Service and Asset Manager in SAP S/4HANA on-premise edition 1909 or later doesn't require SAP Mobile Add-On installation. The Mobile Application Integration Framework used by SAP Service and Asset Manager is included as part of SAP S/4HANA 1909 on-premise.

See the checklist found in Installing the SAP Mobile Add-On for SAP S/4HANA 1909 and Earlier Versions for detailed information on installing for 1909 or earlier versions.

2.2.2 SAP Mobile Add-On for SAP ERP

Add the SAP Mobile Add-On for SAP ERP systems alongside the requisite service packs in order to provide the required OData services for specific versions of SAP Service and Asset Manager.

Depending on the version of SAP Service and Asset Manager, the following versions of the SAP Mobile Add-On are available for compatible SAP ECC 6.0 EHP7 SP14 systems and newer:

Ensure that the corresponding SAP Mobile Add-On and service packs are installed for the SAP Service and Asset Manager application you wish to run. For detailed information and instructions regarding the installation

of the SAP Mobile Add-On for ECC 6.0 Systems, see the Mobile Add-On for ERP Installation Guide, and check the following primary notes:

- 2577248: Release Information Note - Mobile Add-On for ERP 6.30 and Support Packages
- 2660361: SAP Asset Manager Mobile Add-On for ERP Installation Primary Note
- 2660862: SAP BTP Mobile Services Setup Info for SAP Service and Asset Manager with SAP ERP System

For detailed information and instructions regarding the configuration of SAP Mobile Add-On, see the SAP Service and Asset Manager Configuration Guide.

After downloading the files for the SAP Mobile Add-On desired support packages from the SAP Software Download Center, load the mobile add-on onto your system through the add-on manager, using the transaction code `SAINT`. Once the add-on is installed, load the support packages into your system through the Support Package Manager (accessed through transaction code `SPAM`).

See the checklist found in Installing the SAP Mobile Add-On for SAP ERP for detailed information on installing the SAP Mobile Add-On for SAP ERP

SAP ERP 6.0 Enhancement Package 7

Software Compnent	Release	Support Package
SAP_ABA	740	SP17 or higher
SAP_APPL	617	SP14 or higher
SAP_BASIS	740	SP17 or higher
SAP_GWFND	740	SP17 or higher
SAP_UI	740	SP17 or higher
IS_UT	617	SP14 or higher

SAP ERP 6.0 Enhancement Package 8

Software Compnent	Release	Support Package
SAP_ABA	750	SP08 or higher
SAP_APPL	618	SP07 or higher
SAP_BASIS	750	SP08 or higher
SAP_GWFND	750	SP08 or higher
SAP_UI	750	SP08 or higher
IS_UT	618	SP07 or higher

2.3 SAP Gateway System Setup

Procedure

1. Check if Gateway is active through transaction *SPRO*.

   Navigate to *IMG* > *SAP Netweaver* > *SAP Gateway* > *OData Channel* > *Configuration* > *Activate or Deactivate SAP Gateway* to check if the Gateway is active.
2. Maintain system alias through transaction *SPRO*.

   Navigate to *IMG* > *SAP Netweaver* > *SAP Gateway* > *OData Channel* > *Configuration* > *Connection Settings* > *SAP Gateway to SAP System* > *Manage SAP System Alias* to check if the Gateway is active.
3. Register and activate the OData service through transaction */IWFND/MAINT_SERVICE*
   a. Click *Add Service* and search for the following technical service name:

Technical Service Name	Usage
/MERP/SAP_SRV_ASSET_MANAGER_<XXXX>	Standard Plant Maintenance scenario

> **Note**
>
> *<XXXX>* is the release version of the application. For example, *2010*.

   b. Click *Add Selective Services* and click *Enter*.
4. Test OData services through transaction */IWFND/GW_CLIENT*

> **Note**
>
> Use HTTP GET method and request URI `/sap/opu/odata/MERP/SAP_SRV_ASSET_MANAGER_<XXXX>/$metadata`.

2.4 SAP Service and Asset Manager Installation Prerequisites

SAP Service and Asset Manager uses the oData service that is provided with the SAP Business Technology Platform Mobile Services.

The oData service provides a universally available service for the SAP Service and Asset Manager application.

Back End Landscape Prerequisites

- Ensure that an SAP Business Technology Platform Mobile Services account with an active mobile services account is available
- A Cloud Connector is required. For more information, see the Setting up the SAP Business Technology Platform Cloud Connector System Mapping [page 26] procedure.
- The correct SAP Mobile Add-On for your system is already installed. For more information, see the following topics:
  - SAP Mobile Add-On for SAP ERP [page 7]
  - Mobile Add-On for SAP S/4HANA [page 7]

> **Note**
>
> If you are using S4HANA 1909 SPS 03 or above, MAIF is included automatically. See the Mobile Application Integratio Framework (MAIF) portal page for more information.

Prerequisites for SAP Service and Asset Manager Application Installation

> **Note**
>
> Your organization may have multiple SAP BTP global accounts with different product licenses associated with them. Please make sure one of those licenses is associated with the global account that end users have access to. If a corresponding license that grants entitlements for SAP Service and Asset Manager is not associated with the global account that end users have access to, SAP Service and Asset Manager will not be a visible application available for use.
>
> If the license for Mobile Execution and SAP Service and Asset Manager is not assigned to the correct global account, please reach out to your account executive. They can correctly assign the product SKU to the global account in which you wish to operate SAP Service and Asset Manager.

- Access to your SAP Business Technology Platform Mobile Services environment
- Administrative access to the Mobile Development Kit
- Access to a computer to build and run the Mobile Development Kit client either in a simulator or on a device
- If using certificate-based authentication, acquire the certificates the IdP expects from mobile devices running the SAP Service and Asset Manager application. See the SAP Cloud Identity Services - Identity Authentication portal page for complete information on working with certificates and Identity Providers. If you optionally enable certificate based authentication, the Mobile Development Kit client passes the certificate to the IdP for use in authentication as long as the IdP supports and asks for certificates, and certificates are present on the mobile device.

Software Prerequisites

For all prerequisite and installation information for the Mobile Development Kit, see the SAP Mobile Services, mobile development kit portal page.

License Matrix for Cloud Foundry and Neo Platforms

Platform	Required Services
Cloud Foundry	• Application Runtime • Mobile Services • SAP Business Application Studio
Neo	• Mobile Services • Mobile Development Kit SAP Web IDE

3 Working with the Mobile Development Kit

Reference information to help you understand the files and metadata in your project.

Structure of .mdkproject

- **BrandedSettings.json:** Runtime configurations such as security settings, URLs for connecting to the SAP Business Technology Platform Mobile Services, and more
- **MDKProject.json:** Build time configurations such as the application name, version, and bundle ID
- **App_Resources:** Any custom resources used by the application, such as all of your action bar images that are customized for your application.
- **demo:** To make an OData service available in demo mode, include the `.udb` and `.rq.udb` files for that service in this directory
  Currently the SAP Service and Asset Manager application can't take the demo UDBs created by the most recent SAP Business Technology Platform SDK and use them with an older SAP Business Technology Platform SDK version.
  Therefore, use the Android UDBs for demo mode, for both the iOS and Android applications. Failure to do so results in the inability to perform Update or Create OData actions, such as:
  - Changing the mobile status of any work orders
  - Creating reminders
- **extensions:** Include any extensions used by the application in this directory
- **metadata:** Built in metadata for the application

Configuring the MDKProject.json File

The `MDKProject.json` file contains settings that you can only configure before running the `create-client.command`:

- **AppName:** Determines the name of the application project and the app as it appears on a mobile device
- **AppVersion:** The client project application version
- **BaseProject:** The `metadata` subdirectory under the `.mdkproject` structure that contains the main application metadata. The main application metadata is the MDK application, which includes one or more component MDK applications. The component applications are only required if you are adding components to your base application, such as Meter Management or Field Operations Worker.
- **BundleID:** Uniquely identifies the resulting MDK client application on the device. Only one instance of a bundle ID can be installed on a device at a time. If you attempt to install a second application using the same bundle ID, it will overwrite the existing application.
- **Externals:** A list of NPM nodules that should not be included in the application bundle. Use this option for dependencies you expect to be in the environment when the application is built.
  Note that the modules `file-system` and `ui/dialogs` are automatically used as externals as they are already included in the client application.

- **URLScheme:** Allows you to specify a custom URL scheme that opens the client. If the URL includes connection settings such as URL parameters, these settings override the settings used by the client. Defaults to *mdkclient*.

Application Version and Notes on the Settings App

The Mobile Development Kit client tracks several versions, which you can view in the iOS *Settings* menu. These versions are identified as the *application* version, the *definitions* version, and the *frameworks* versions for the frameworks used in the client build.

When generating a client project, you can specify the application version. Specifying the application version allows you to version the client itself, which can be useful if you change extension controls or other branded settings. To specify the application version, specify the `AppVersion` property in the `MDKProject.json` file before running `create.client.command`.

To further customize the entry of your application in the iOS *Settings* menu, you can manually edit `<ProjectDirectory>/app/App_Resources/iOS/Settings.bundle/Root.plist` after the script has completed. You can add new entries, but do not remove existing entries or the application may not function correctly.

For more information, see Implementing an iOS Settings Bundle .

3.1 Setting Up the SAP Business Application Studio

Use the SAP Business Application Studio to edit application metadata and deploy the bundle to SAP BTP services on Cloud Foundry.

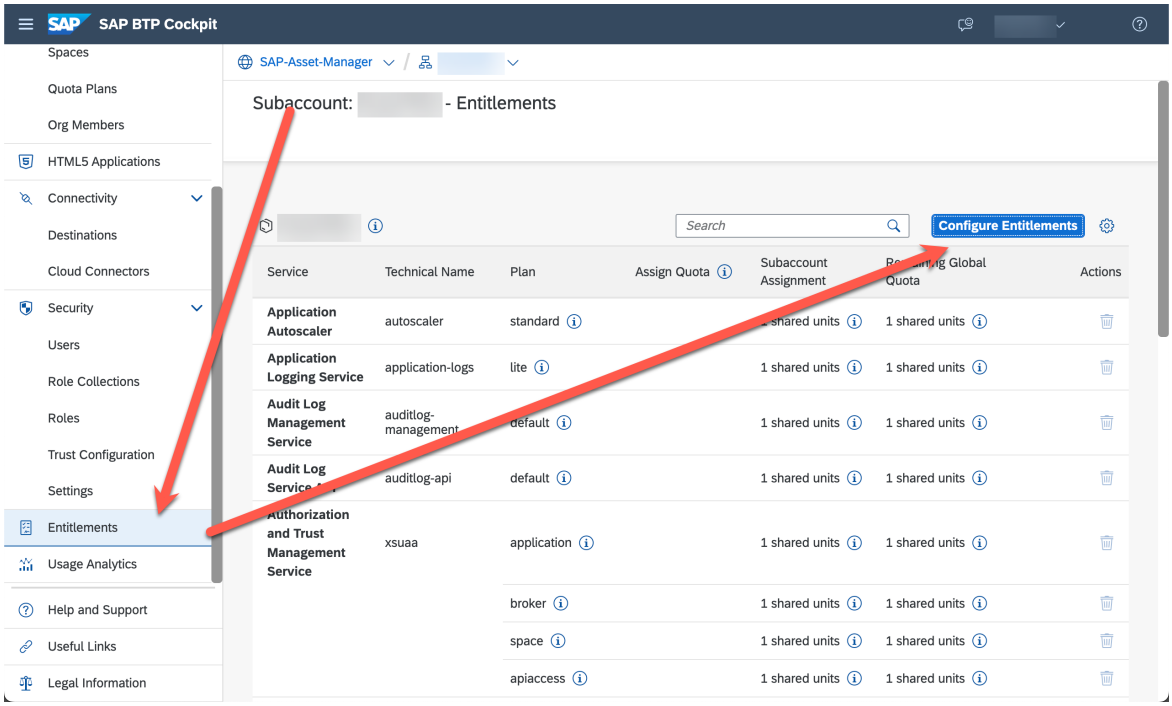
Prerequisites

Context

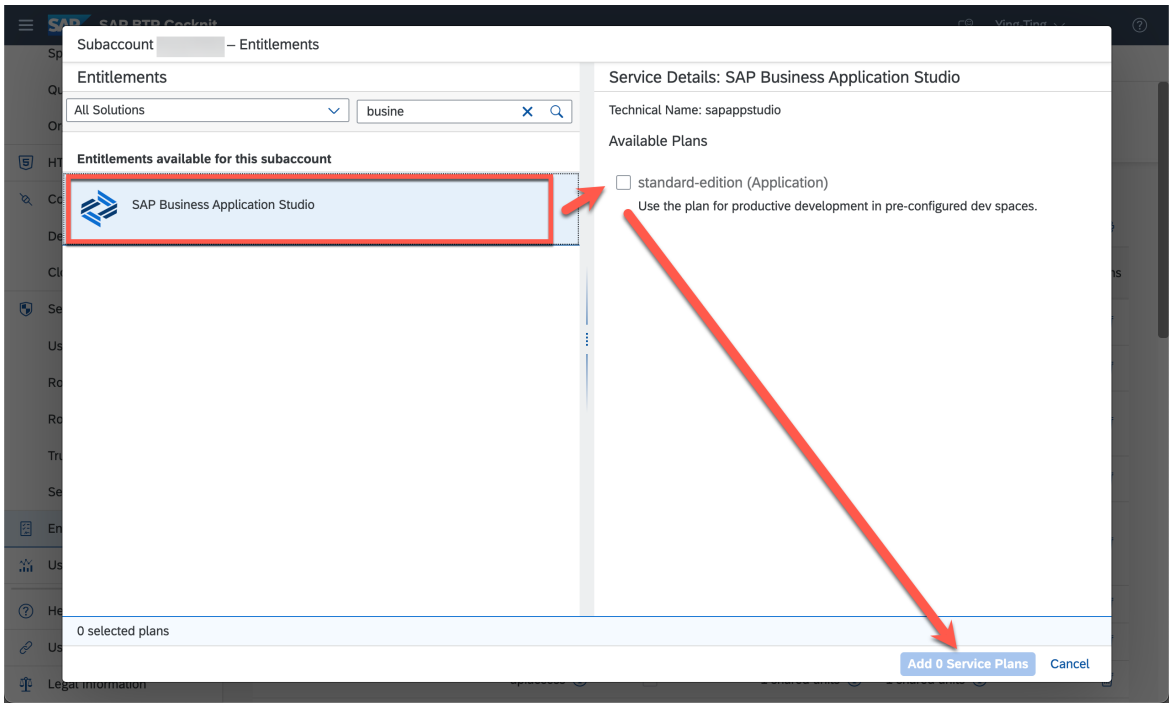
See the SAP Business Application Studio portal page for detailed information.

Procedure

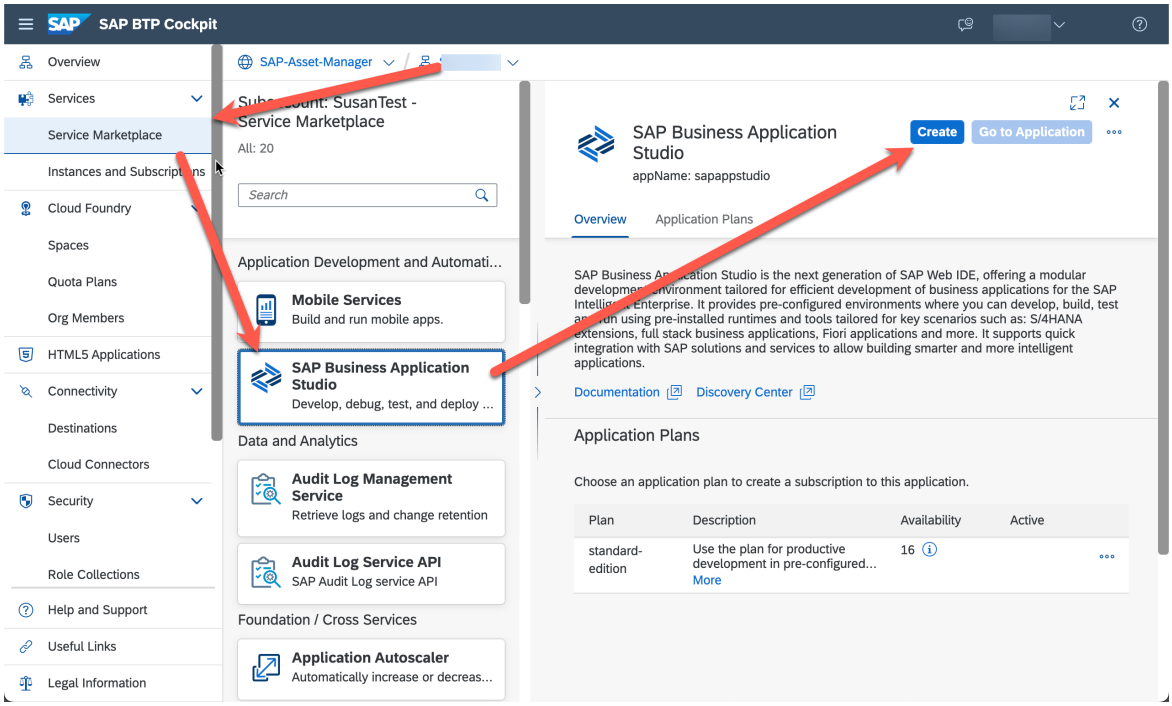
1. Navigate to the *subaccount* > *Entitlements tab*. Select *Configure Entitlements* to add the ability to subscribe to SAP Business Application Studio to the subaccount.



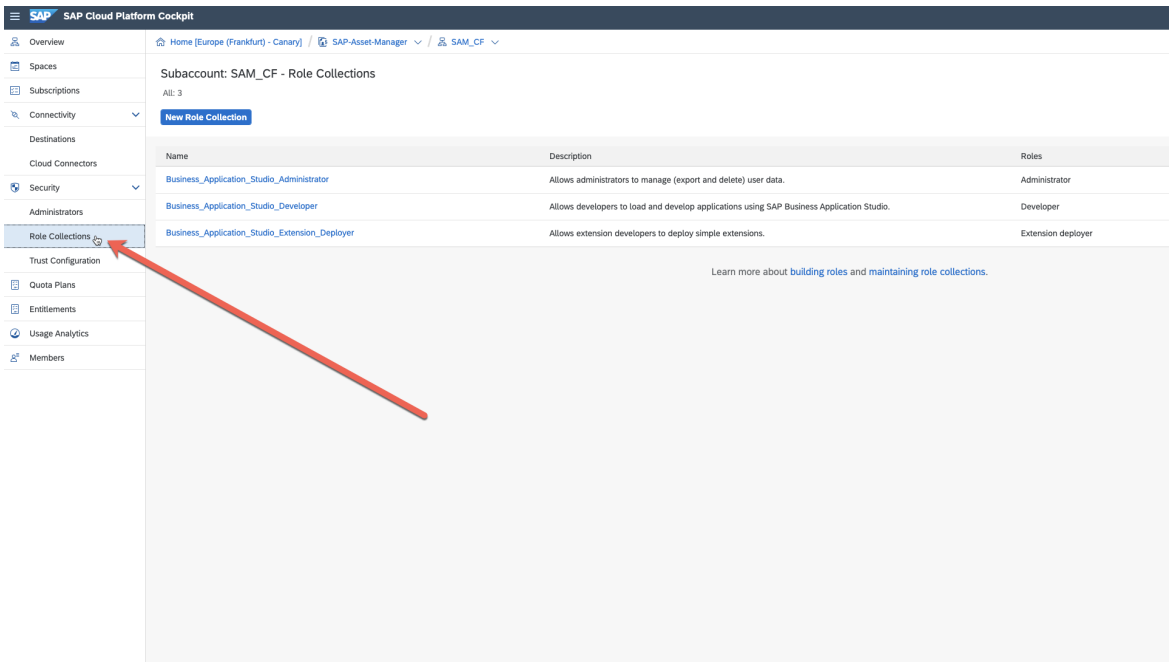
2. Search for and add it to the entitlements.



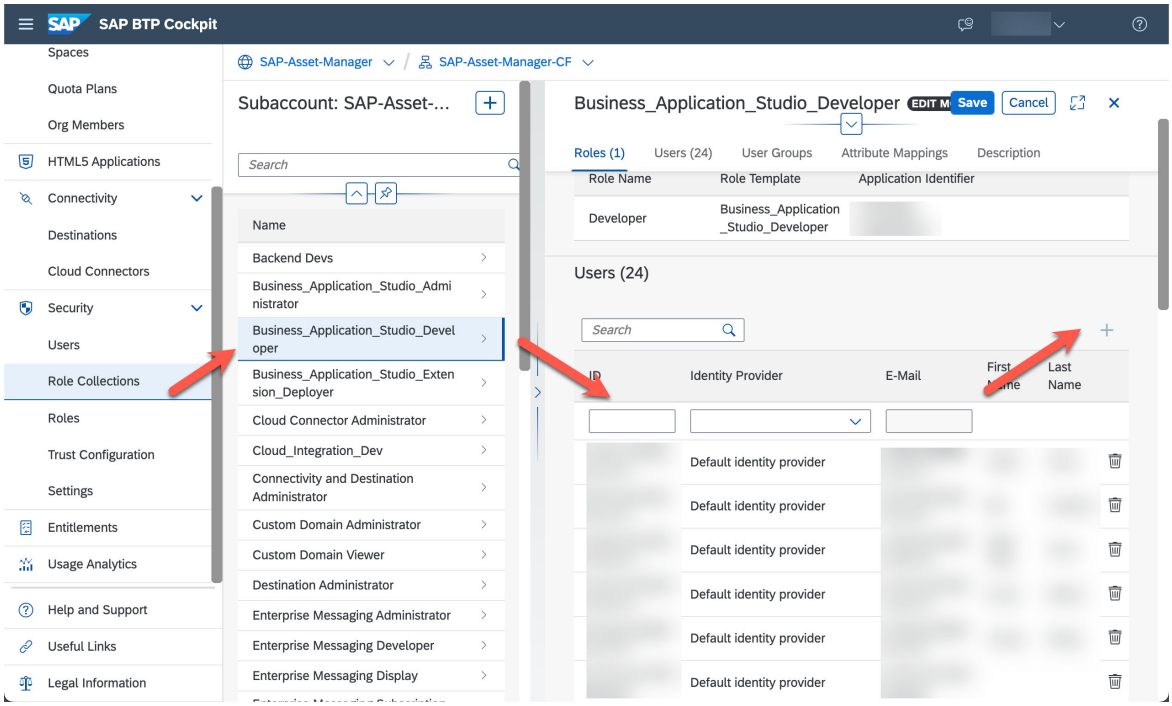
3. Save the changes to the subaccount.
4. Navigate to the *Service Marketplace tab* on the Cloud Foundry subaccount on which you're setting up the SAP Business Application Studio. Create a subscription to the service.



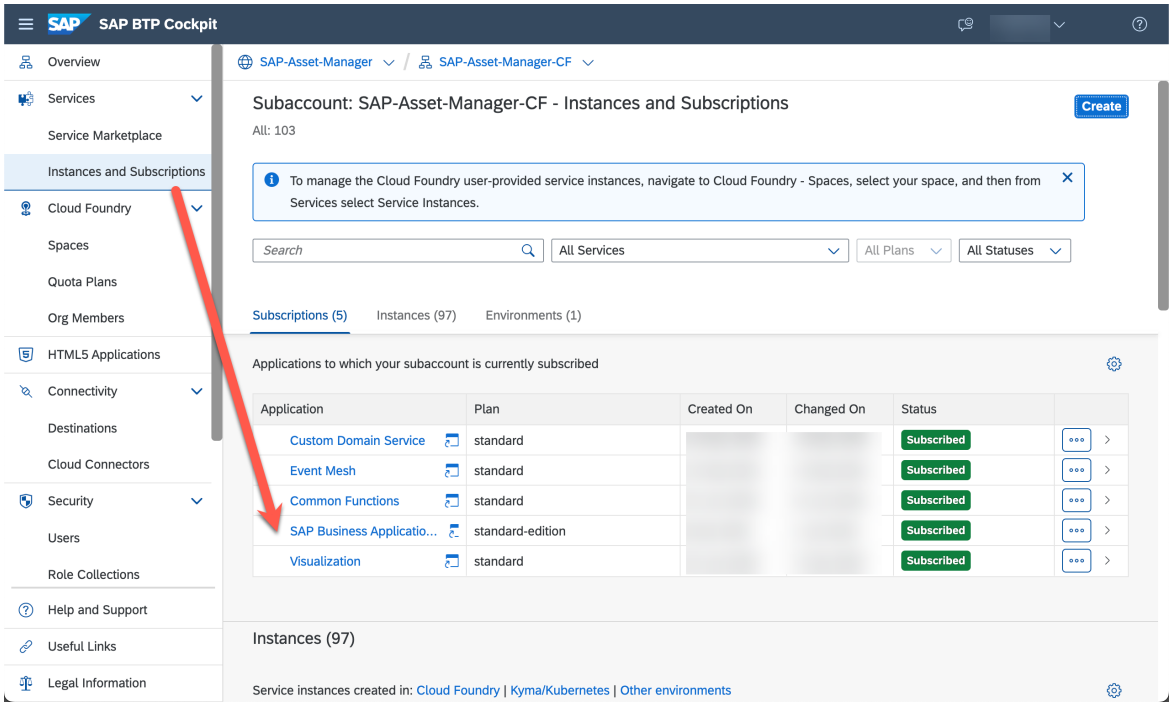
5. Navigate to the *Role Collections tab* in your subaccount to ensure that the SAP Business Application Studio roles are created.



6. Select each *Name* in the *Role Collections* of the subaccount to add users to the collections. Enter the email address you want to add to the roles. Then select the + button to assign the roles from the SAP Business Application Studio



7. Navigate to the *Instances and Subscriptions tab* and click on the link for . To begin working, select the *Create Dev Space* button to open a workspace.



8. Give your space a meaningful name, select SAP Business Technology Platform Mobile Services for the type of app, and create your dev space. Activate whichever extensions you wish to use, and wait for your space to finish installation.
9. Once the space has finished installation, navigate into it by selecting the space name.

> → Tip
>
> Chrome works better than Safari when attempting to access your space.

3.1.1 Creating a New Mobile Development Kit Application in SAP Business Application Studio

The SAP Business Application Studio in SAP Business Application Studio is equivalent to the VS Code extension (minus debugging), plus the graphical editors from the SAP Web IDE.

> ⓘ Note
>
> By default, all Mobile Development Kit objects will open in the graphical editors. Select *Code Editor* if you prefer the VS Code method of editing.

To create a new Mobile Development Kit application in SAP Business Application Studio, use the following steps:

1. Select *File* > *New Project from Template*. This opens up the *Template* page.
2. Select *MDK Project* and click *Next*.
3. Select from one of the Mobile Development Kit template types (Empty, Base, List Detail, or CRUD), and proceed through the rest of the wizard.
4. If you have zipped metadata, import it into SAP Business Application Studio by unzipping it and dragging the uncompressed folder into the SAP Business Application Studio *Explorer* view.

3.2 Enabling the SAP Web IDE in theMobile Development Kit

Procedure

1. Log in to the SAP Business Technology Platform Cockpit and from *Home* > *Region*, click the *Region* in which your account is based.
2. Select your *Global Account*. From the Global Account page, select the *Subaccounts* tab on the left side. Then select the subaccount where you wish to deploy your applications.
3. Find the *SAP Web IDE Full-Stack* tile. If it is not *Enabled*, enable it. Then click *Go to Service*.

   The SAP Web IDE Full-Stack browser opens.
4. Click the *Preferences* icon () on the left.
5. Click *Extensions*. Ensure the *Mobile Services App Development Tools* editor tile is enabled. If not, enable it by clicking the radio button at the top right of the tile. After enabling the tool, click *Save*.

   The SAP Web IDE prompts to refresh. Refresh the SAP Web IDE to view the new tile.

6. Click the *MDK Development* icon. If the Mobile Development Kit icon does not appear, ensure it is enabled. After enabling, refresh the SAP Web IDE.

Next Steps

Proceed to the Importing Metadata Definitions to the SAP Web IDE Mobile Development Kit [page 18] procedure.

3.2.1 Importing Metadata Definitions to the SAP Web IDE Mobile Development Kit

You can import a project and its resources from your local file system to the SAP Web IDE Mobile Development Kit workspace.

Prerequisites

Ensure that the SAP Service and Asset Manager 2305 and Mobile Development Kit 4.3.2 installation files are downloaded from the SAP Download Center.

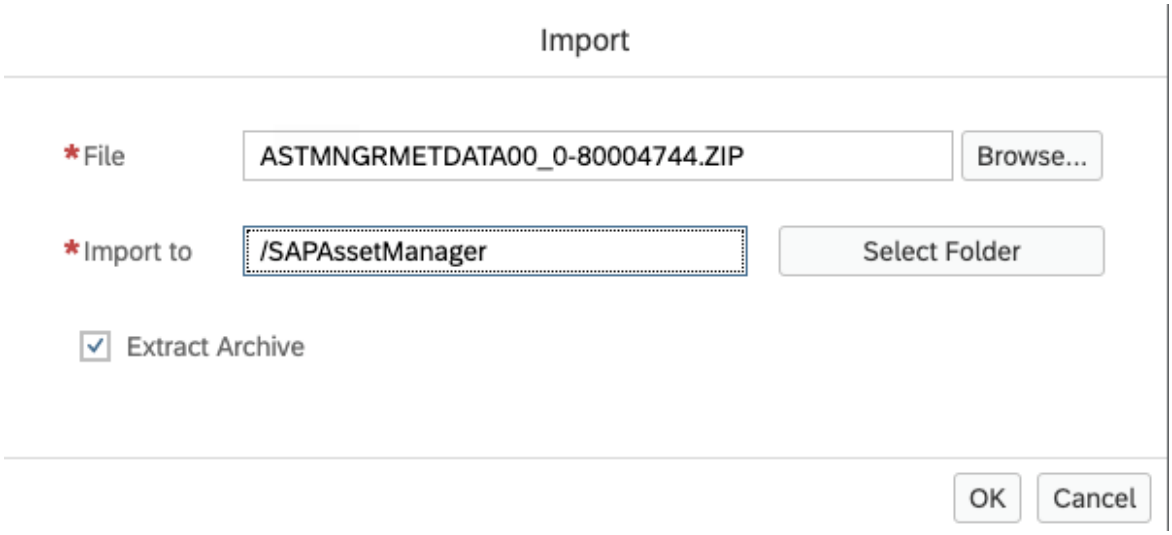
If an earlier version of the Mobile Development Kit is already installed on your back-end system when compared to your version of the SAP Service and Asset Manager application that you are attempting to install, you must also import and deploy the current version of the Mobile Development Kit to the SAP Web IDE.

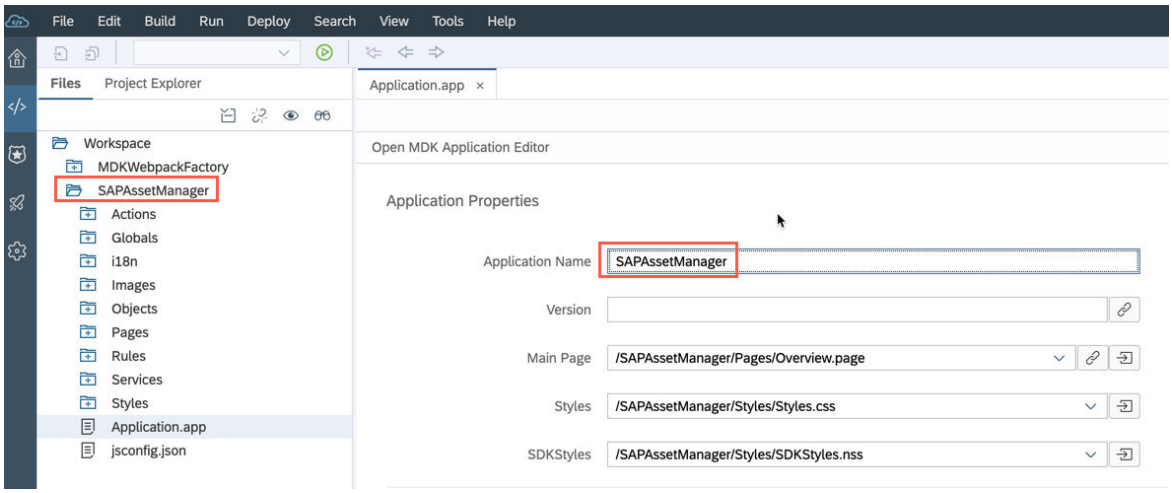
Procedure

1. Click the *MDK Development* icon ( ).
2. Select the folder to which you want to import your project from your Mobile Development Kit workspace.
3. Import your project. Select *File* > *Import* > *From File System* from the main menu. Alternatively, you can right-click on your *Workspace* folder and choose *Import* from the menu choices.

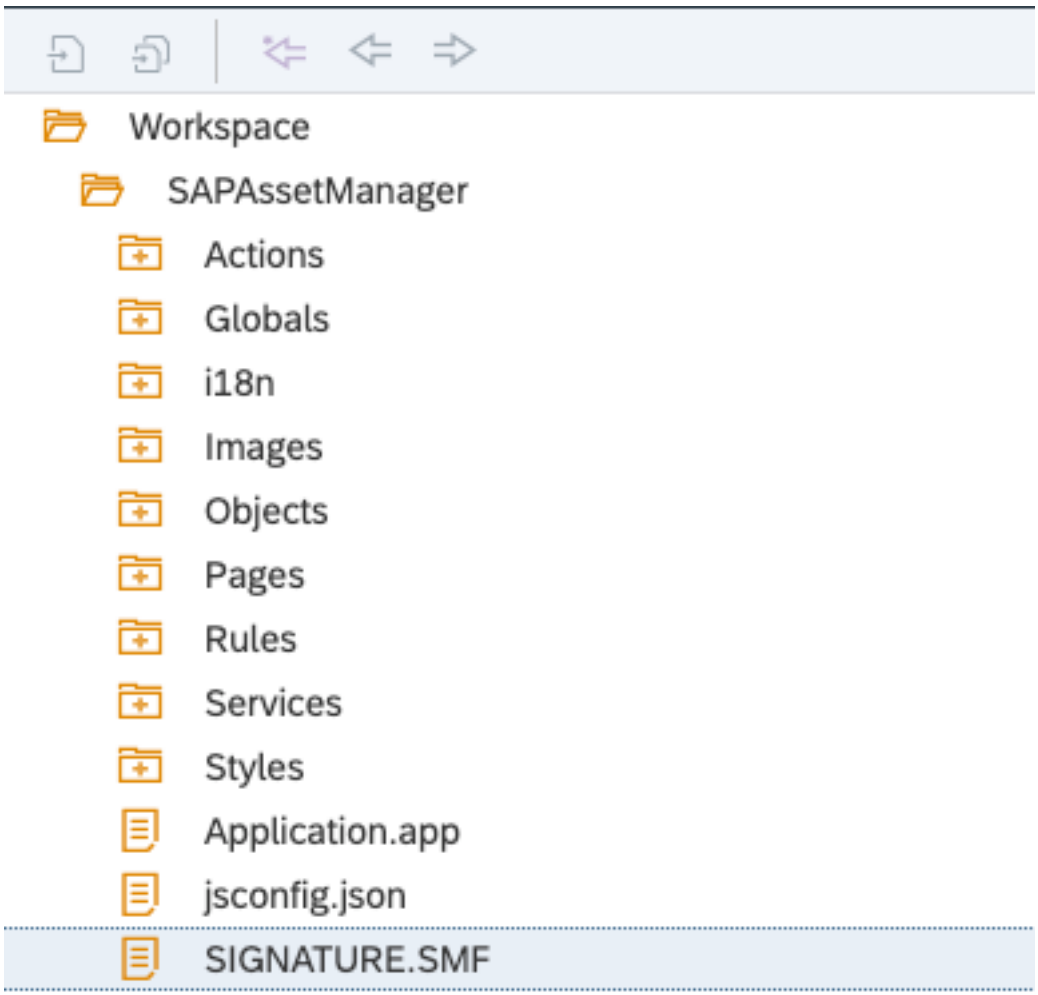
   An Import window displays.
4. Click the *Browse* button and browse to the folder where your ZIP file is located. If the folder listed in the *Import to* field is incorrect, click the *Select Folder* button to choose the correct folder. If you're importing an entire project, the top-level folder is the correct folder.
5. You can optionally change the `<Import To>` folder name to *SAPAssetManager*, but it's not required.

   If you decide to leave the folder name as-is, once the import is complete, hit refresh on your browser to reload the SAP Web IDE. After refreshing, the folder name shows up and correctly matches the *Application Name* in your `Application.app` file.





6. Delete the `SIGNATURE.SMF` file.



7. Check the *Extract Archive* checkbox and click *OK*.

   The project is imported into the selected folder with the same name as the `<Import To>` field.

> ⓘ Note
>
> If the target folder already exists in your workspace, you're prompted to approve the overwriting of the existing files.

3.2.2 Deploying Metadata Definitions to Mobile Services

Prerequisites

In the SAP Business Technology Platform Cockpit, ensure that the *mobileservices* destination has the additional property of *WebIDEUseage* set with the property of *mobile*.

> **Note**
>
> SAP Service and Asset Manager metadata versions 2105 or older are not compatible with Mobile Development Kit 6.x. See the Migrating SAP Service and Asset Manager 2105 or Earlier Metadata to Mobile Development Kit 6.x procedure found in the *Upgrading SAP Asset Manager* guide for more details.

Context

Once your desired changes to the metadata definitions for the Mobile Development Kit are complete, use the Mobile Services app development tools deployment feature to deploy the metadata definitions to your application in Mobile Services. Then, when you change the SAP Service and Asset Manager application, and redeploy the metadata files in the Mobile Development Kit editor, a timer looks for new definitions within the bundle.

Procedure

1. Click the *Development* icon ().
2. From your Mobile Development Kit workspace, select the folder from which you want to deploy your project.
3. Right-click and select *File* > *MDK Deploy and Activate*.

   A ZIP file is created of your application definitions.
4. Select the options you would like to deploy with and click *Next*.
5. In the `<Destination Name>` field, select *mobileservices*. In the `<Application ID>` field, select the desired application ID you want to deploy to. Click *Next*.

Results

The `bundle.js` is uploaded from the SAP Web IDE to Mobile Services.

3.2.3 Importing and Deploying an Application through the SAP Web IDE

If the extension or installation of additional components onto your application is required, then the SAP Web IDE is a required deployment.

Find more information at the documentation for the SAP Web IDE Full-Stack.

To deploy an application from the SAP Web IDE to the SAP BTP services instance:

1. Ensure that the *mobileservices* destination in the SAP Business Technology Platform subaccount has the value *mobile* added to the *WebIDEUsage* property.
2. Ensure that the *Mobile Services App Development Tools* is enabled by checking the *Settings* tab in the *Extensions* section in the SAP Web IDE.
3. Download the SAP Service and Asset Manager metadata from the SAP Marketplace. Import the application into the SAP Web IDE.
4. Once the metadata is imported, load the metadata to the MDK perspective.
   Right-click on the app, and select *MDK Deploy and Activate*. Deploy the app to the mobile application.
5. Once the app is loaded, use the connection link builder in the SAP Web IDE to build an onboarding link for the mobile device using the information retrieved from the building of the mobile application.
6. Once the link is built, send the link to the mobile device with SAP Service and Asset Manager installed.
7. Connect to the mobile app, sign in, and update the mobile application when prompted.

4 Installing SAP Service and Asset Manager

Use the procedures and subprocedures found in this chapter to quickly install SAP Service and Asset Manager. Before installation, see the SAP Service and Asset Manager Installation Requirements [page 4] topic and subtopics to ensure your system meets installation requirements.

Setting Up the Cloud Connector [page 23]

SAP BTP services - Setting Up a Cloud Foundry Environment, Single Instance [page 27]
Establish an SAP Business Technology Platform Cloud Foundry account with the requisite individual services.

Opening the SAP BTP services App Creator [page 30]

Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application [page 34]

4.1 Setting Up the Cloud Connector

Prerequisites

Meet the following requirements before beginning this procedure:

- **HTTP Configuration:** SAP Business Technology Platform Mobile Services communicates with the back end using HTTP/OData service
- **Principal Propagation:** Principal propagation to an ABAP system must be configured
- **Certificate User Mapping in ABAP system:** X.509 certificate must be mapped to named user in the SAP ABAP system

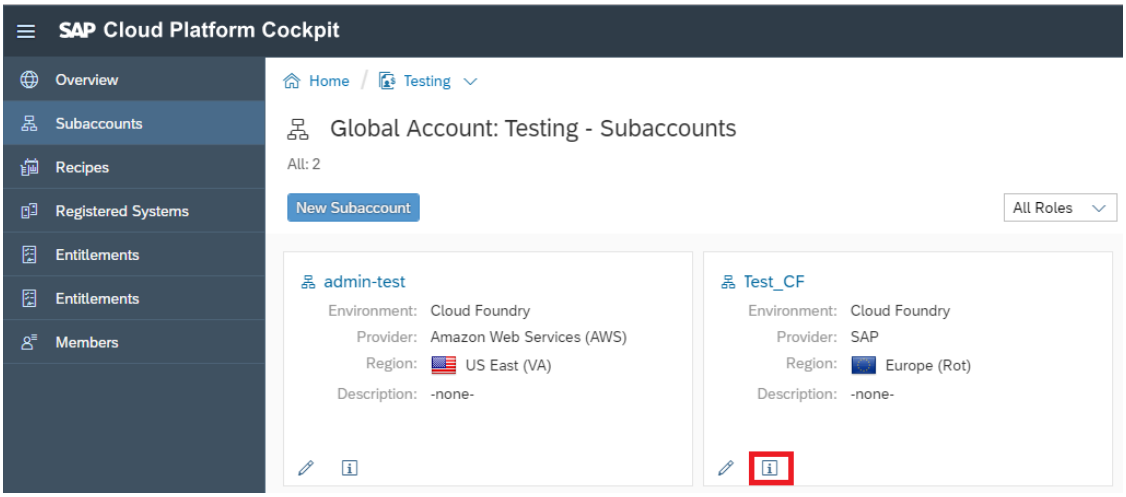
Context

For detailed information on installing and configuring the Cloud Connector, see the following links:

- SAP Development Tools for Cloud
- SAP Business Technology Platform Connectivity – Cloud Connector

Procedure

1. **Find your subaccount ID:** To set up your subaccount, you must know the subaccount ID.
   a. Open the SAP Business Technology Platform Cockpit.
   b. Navigate to the subaccount list of the global account containing your subaccount: choose *Home* > *<Your Global Account>* > *Subaccounts*.
   c. Find your subaccount in the list. Choose the *Info* icon in the subaccount tile to display the subaccount ID.



2. **Add subaccount:**
   a. The `<Region>` field specifies the SAP Business Technology Platform region that should be used, for example, **`Europe (Rot)`**. Choose the one you need from the drop-down list.
   b. For `<Subaccount>` and `<Subaccount User>` (user/password), enter the values you obtained when you registered your account on SAP Business Technology Platform.

> **Note**
>
> Enter the subaccount **ID** as `<Subaccount>`, rather than its actual (technical) name. See the previous step to determine your subaccount ID. As `<Subaccount User>` provide your **`Login E-mail`** instead of a user ID.

   c. (Optional) You can define a `<Display Name>` that allows you to easily recognize a specific subaccount in the UI compared to the technical subaccount name.
   d. (Optional) You can define a `<Location ID>` that identifies the location of this Cloud Connector for a specific subaccount.
   e. (Optional) You can provide a `<Description>` of the subaccount that is shown when clicking on the *Details* icon in the *Actions* column.
   f. *Save* your changes.
3. **Configure access control: to allow your cloud applications to access a certain backend system through HTTP, specify this system in the Cloud Connector.**
   a. Choose *Cloud To On Premise* from your *Subaccount* menu in the SAP Business Technology Platform Cockpit. Then choose *Add*.

      A wizard opens to guide you through adding required values.

b. Select *ABAP System* for `<Backend Type>` and click *Next*.
c. Select *HTTP* for `<Protocol>` and click *Next*.
d. Your `<Internal Host>` is *<Backend On-Premise Server Name>*. Your `<Internal Port>` is *<Backend On-Premise Port Number>*. Click *Next*.

> **Note**
>
> Find your internal host and internal port through the SAP GUI by running transaction *SMICM* and navigating to *go to* > *Service (ICM Monitor) - Service*.

e. Your `<Virtual Host>` is *<Name displayed in SAP Business Technology Platform>*. Your `<Virtual Port>` is *<Port number displayed in SAP Business Technology Platform>*. Click *Next*.
f. Select *None* for `<Principal Type>` and click *Next*.
g. Select *Use Virtual Host* for `<Host in Request Header>` and click *Next*.
h. Enter an optional `<Description>` and click *Next*. Click *Finish* on the summary screen.

4. **Add a resource:** In addition to allowing access to a particular host and port, you also must specify which URL paths (*Resources*) are allowed to be invoked on that host.
   a. Click the + icon in the *Resources Accessible On...* section.
   b. Fill the *Add Resource* dialog box fields as follows:
      - `<URL Path:>` sap/opu/odata
      - `<Active:>` Ensure box is checked
      - `<WebSocket:>` Don't check box
      - `<Access Policy:>` Path and All Sub-Paths
      - `<Description:>`Optional description
   c. Click *Save*.

      The *Status* icon is now a green square, indicating the resource is active.
5. Perform an initial Cloud Connector configuration. See Initial Configuration - SAP Help Portal for detailed information.

   Mandatory fields are as follows:

   - Region
   - Subaccount: SAP S/4HANA account name
   - Subaccount user: SAP BTP connection user
   - Password
6. Generate a CA certificate. See Installation of a System Certificate for Mutual Authentication for more information.
7. Set up the trust store with your backend system.
8. Set the System Certificate.

   Mandatory fields are as follows:

   - Common Name
   - Organizational Unit
   - Organization
   - Country
9. Set the Principle Propagation Subject Pattern.

10. Establish the connection between the cloud subaccount and the Cloud Connector.
11. Establish a connection to the on-premise back end system.
12. Establish a Cloud Connector connection for the on-premise system.

Results

You have succesfully set up the Cloud Connector.

Task overview: Installing SAP Service and Asset Manager [page 23]

Related Information

SAP BTP services - Setting Up a Cloud Foundry Environment, Single Instance [page 27]
Opening the SAP BTP services App Creator [page 30]
Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application [page 34]

4.1.1 Setting up the SAP Business Technology Platform Cloud Connector System Mapping

The SAP Business Technology Platform Cloud Connector serves as the link between on-demand applications in the SAP Business Technology Platform and existing on-premise systems.

For general Cloud Connector set up and configuration, see the SAP Business Technology Platform Cloud Connector documentation, specifically Configure Access Control (HTTP). The following topic addresses specific SAP Service and Asset Manager Cloud Connector configurations to make in the Cloud Connector cockpit. Perform these additional configuration modifications after the initial Cloud Connector installation and configuration.

1. Click the *Cloud to On-Premise* link, and in the *Access Control* tab, add your on-premise system in your Cloud to On-Premise mapping as follows:
   - **Protocol:** HTTPS
   - **Back-End Type:** ABAP
   - **Virtual Host:** Your choice
   - **Virtual Port** Your choice
   - **Internal Host:** SAP back-end system
   - **Internal Port:** SAP back-end system
   - **Principle Type:** X.509 Certificate
2. Add a resource to your Cloud to On-Premise account:
   - **URL Path:** `/sap/opu/odata`
   - Click the *Path and all sub-paths* radio button

3. Click the *Principle Propagation* tab and set each of the *Trust Configurations* to *Trusted* (checked).

4.2 SAP BTP services - Setting Up a Cloud Foundry Environment, Single Instance

Establish an SAP Business Technology Platform Cloud Foundry account with the requisite individual services.

Connecting the SAP Business Technology Platform to BTP Mobile Services Cloud Foundry

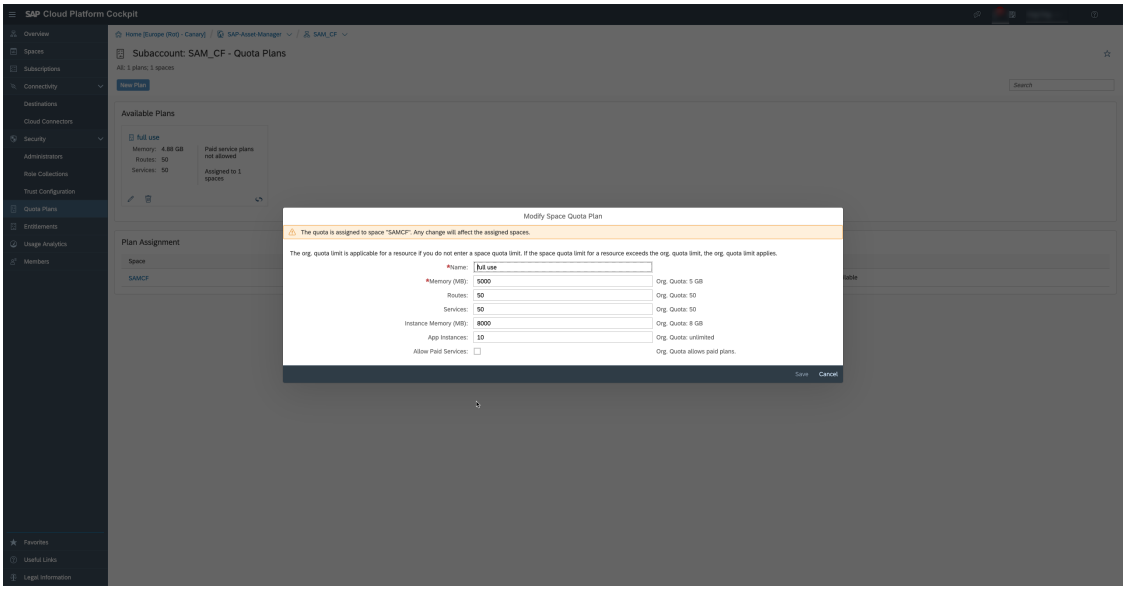
For detailed information on Cloud Foundry, see the Enabling Mobile Services page.

To connect to SAP BTP services Cloud Foundry:

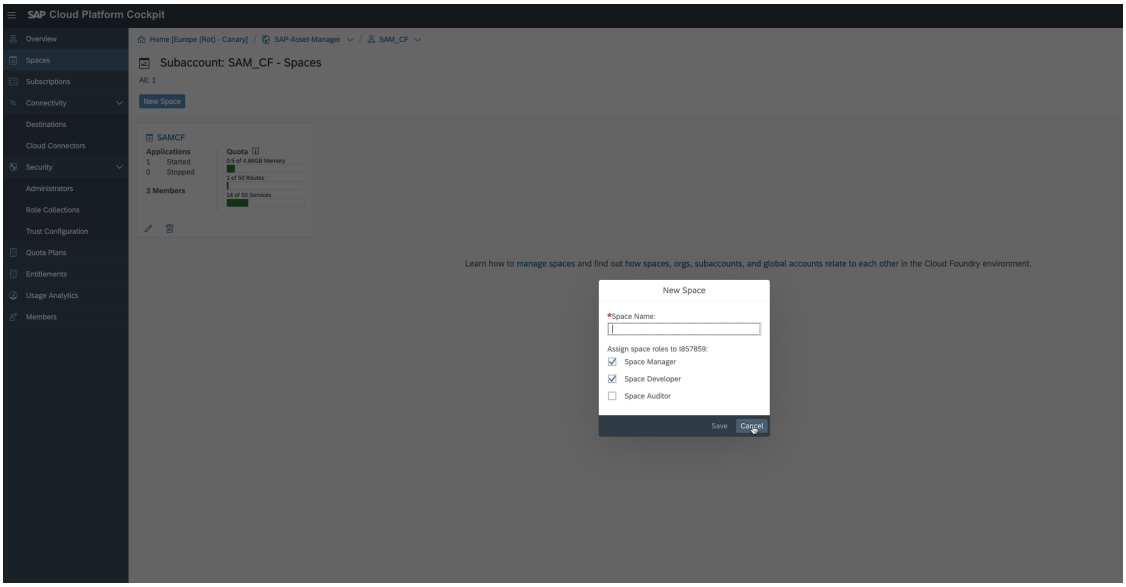
1. Navigate to the SAP BTP cockpit portal page. The SAP Business Technology Platform portal page is the home page where you access your listing of global accounts. You must be logged on to access your accounts.
2. Click your desired global account, for example, SAP Service and Asset Manager.
   You're taken to Global Account Cockpit page.
3. Click the *Subaccounts* tab. Your subaccounts appear. If you don't have any subaccounts created, use the following substeps to create a subaccount:
   - Click the *New Subaccount* button.
   - In both the *Display* and the *Subdomain* fields, type a short, meaningful name.
   - In the *Provider* field, select either *AWS* or *Microsoft Azure*. Currently, *Google Cloud Platform* isn't supported.
   - Click *Create*.
     A new subaccount is created.
4. Click the *Subaccounts Assignment* tab.
5. Select your desired subaccount.
6. Click the *Configure Entitlements* button, then click the *Add Service Plan* button.
   The Entitlements window displays.
7. Select *Mobile Services* on the left to bring up the *Mobile Services* panel on the right.
8. Click the *Standard* checkbox to add it to your plan.
9. Click *Application Runtime* on the left. Then check the *MEMORY* checkbox on the right.
   Application Runtime and *Mobile Services* appear at the bottom of the panel.
10. Click the *Add [Number] Service Plans*.
    You're returned to the *Subassignment Accounts* page.

> **Note**
>
> The amount of application runtime memory required is based on the number of applications you're setting up in the subaccount. For every 5 applications, you need at least 1 GiB of quota. For example, 10 mobile applications require 2 GiB of runtime. See the SAP Asset Manager Sizing Guide for detailed information.

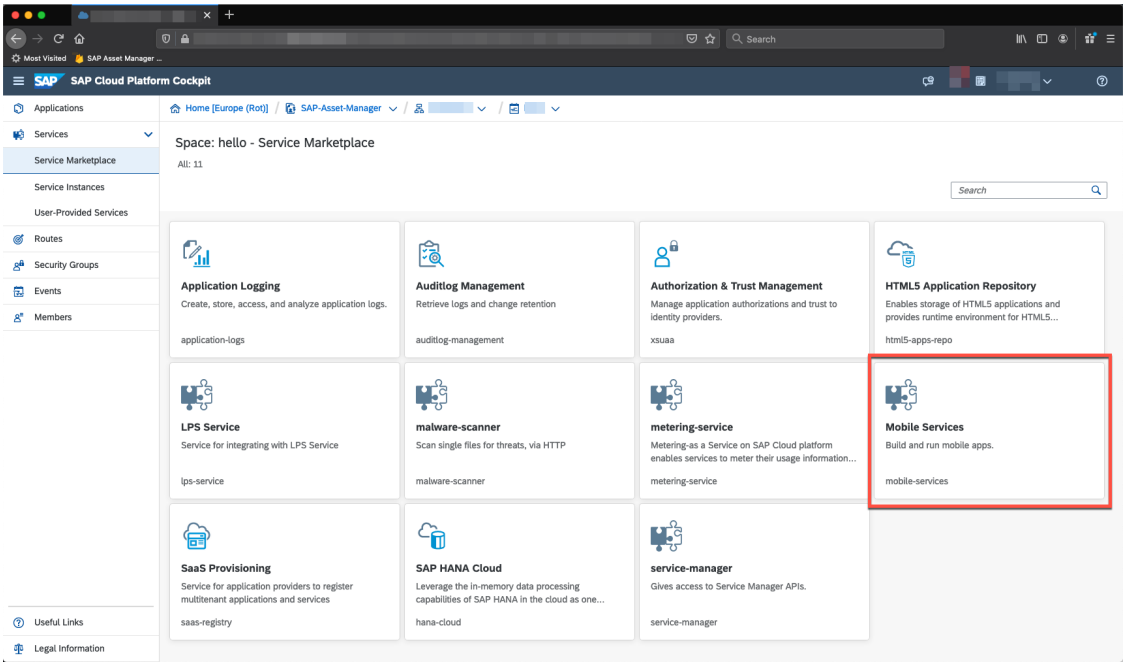
11. Click *Save*.
    The subaccount now has the proper allocation of runtime memory and service plans assigned to it.
12. Click the *Subaccounts* tab and select the subaccount you're working with. Click the *Enable Cloud Foundry* button.
13. When the *Create Cloud Foundry Organization* window displays, click *Create*.
14. Add users that need access to the Cloud Connector as administrators for security roles. Pick the Cloud Foundry region host on the live environment.
15. The number of routes/services that are allowed from the org quota is based on the memory allotted to the subaccount in the *Application Runtime* quota. Each subaccount is assigned 10 routes/services per gigabyte. Create a new plan with the given entitlements for use with the space.
    The quota plan gives your application space shape, so you can access it externally. For more information, see the topics in the chapter Managing Entitlements and Quotas Using the Cockpit in the SAP Business Technology Platform documentation.
    1. Create a new quota plan with the given entitlements for use with the space. For more information, see Create Space Quota Plans Using the Cloud Foundry Command Line Interface in the SAP Business Technology Platform documentation.



    2. Create a space.



3. Navigate to the *Service Marketplace* in your newly created space and select one of the services related to mobile.



4. Select the *Instances* tab. Create a new instance with a meaningful name and no parameters.
5. Select the instance. Select *Open Dashboard* to open the mobile services. Create an application following the Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application [page 34] procedure

Parent topic: Installing SAP Service and Asset Manager [page 23]

Related Information

Setting Up the Cloud Connector [page 23]
Opening the SAP BTP services App Creator [page 30]
Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application [page 34]

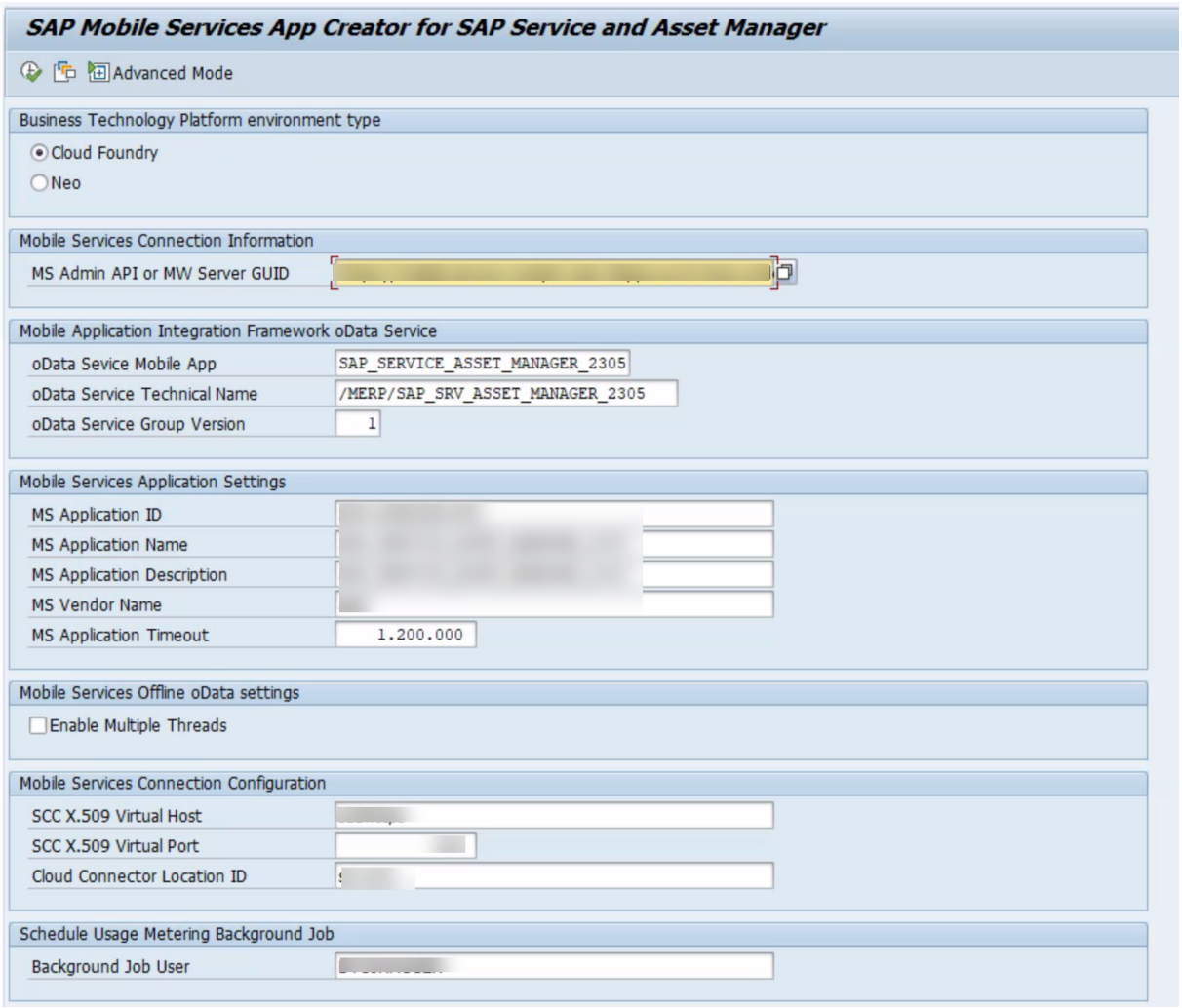
4.3 Opening the SAP BTP services App Creator

In the SAP GUI, use transaction */MERP/CPms_appcreate*. Note that if the transaction is unavailable, reach the application through transaction *SE38* and execute the program */MERP/CORE_CPMS_APPCREATE_PROG*.

The app create program opens in standard mode.

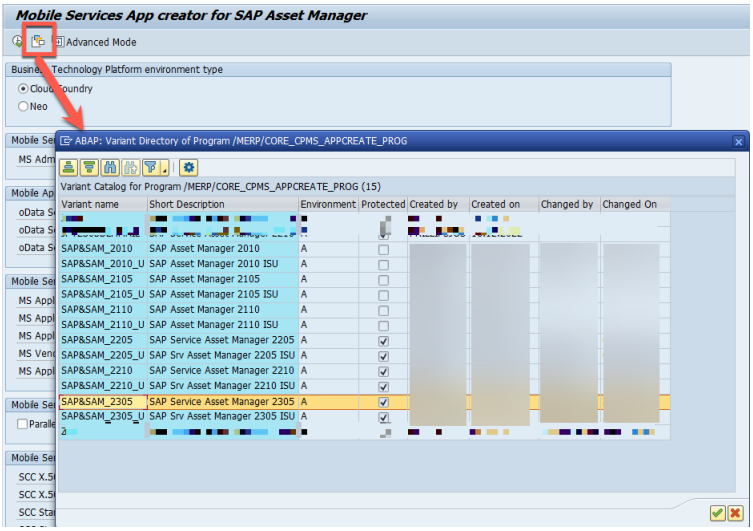
> ⚠ Caution
>
> Please note that currently standard mode is deprecated. This issue is planned to be fixed with 2410 release.

> ⓘ Note
>
> For most applications, standard mode is sufficient for successful execution of mobile app generation.

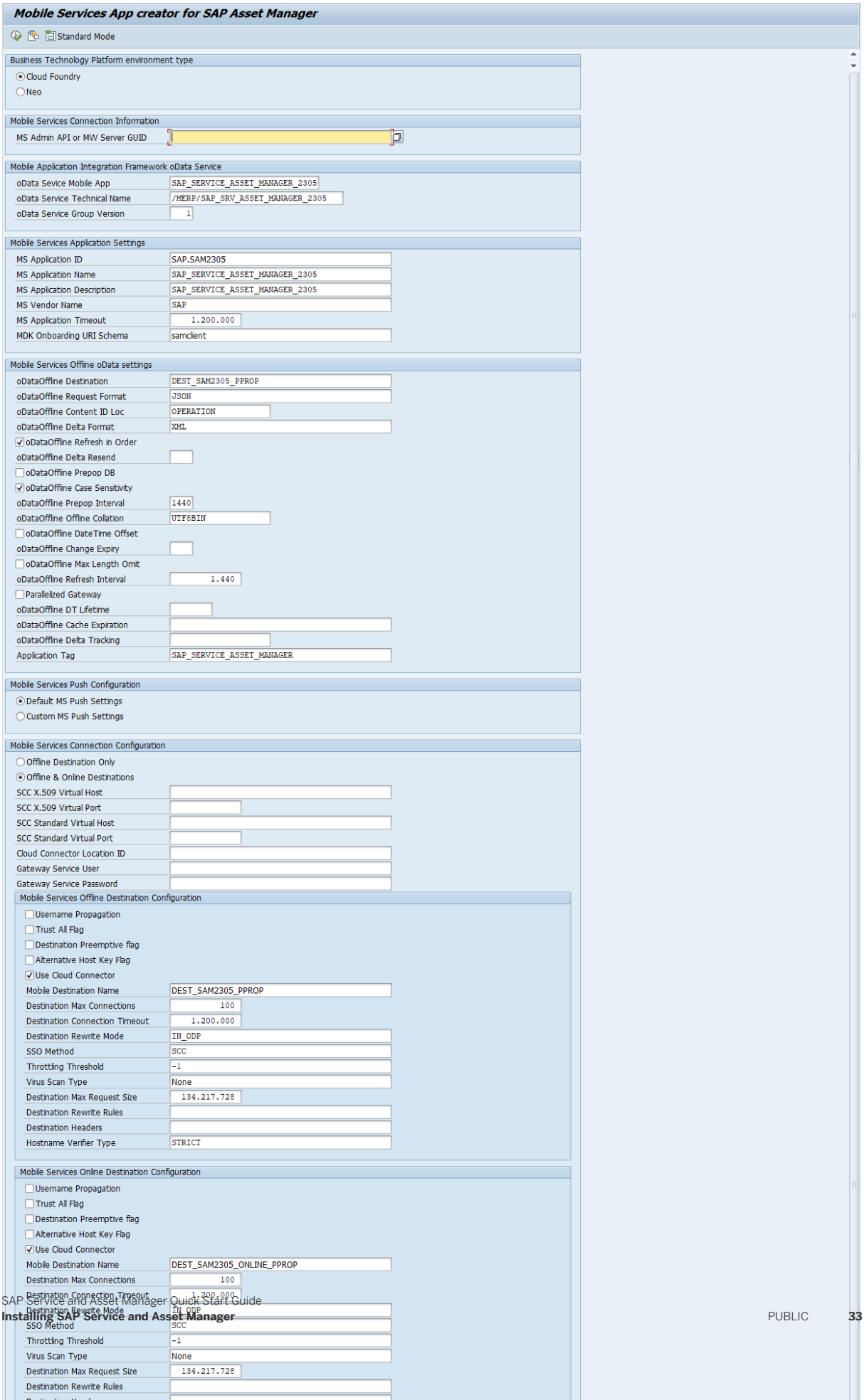


Selecting the Proper Variant and Mode

If needed, open the list of variants available for the application and select a variant specific to the version of the installed Mobile Application Integration Framework application.



Once you've selected the correct variant, determine if you need to use advanced mode rather than standard mode. Advanced mode is necessary if the SAP Gateway being called by SAP BTP services is not using the default *SAP-Client* to retrieve the data for use with the corresponding application.


Mobile Services App creator for SAP Asset Manager
Standard Mode
Business Technology Platform environment type
Cloud Foundry
Neo
Mobile Services Connection Information
MS Admin API or MW Server GUID
Mobile Application Integration Framework oData Service
oData Sevice Mobile App
SAP_SERVICE_ASSET_MANAGER_2305
oData Service Technical Name
/MERP/SAP_SRV_ASSET_MANAGER_2305
oData Service Group Version
1
Mobile Services Application Settings
MS Application ID
SAP.SAM2305
MS Application Name
SAP_SERVICE_ASSET_MANAGER_2305
MS Application Description
SAP_SERVICE_ASSET_MANAGER_2305
MS Vendor Name
SAP
MS Application Timeout
1.200.000
MDK Onboarding URI Schema
samclient
Mobile Services Offline oData settings
oDataOffline Destination
DEST_SAM2305_PPROP
oDataOffline Request Format
JSON
oDataOffline Content ID Loc
OPERATION
oDataOffline Delta Format
XML
oDataOffline Refresh in Order
oDataOffline Delta Resend
oDataOffline Prepop DB
oDataOffline Case Sensitivity
oDataOffline Prepop Interval
1440
oDataOffline Offline Collation
UTF8BIN
oDataOffline DateTime Offset
oDataOffline Change Expiry
oDataOffline Max Length Omit
oDataOffline Refresh Interval
1.440
Parallelized Gateway
oDataOffline DT Lifetime
oDataOffline Cache Expiration
oDataOffline Delta Tracking
Application Tag
SAP_SERVICE_ASSET_MANAGER
Mobile Services Push Configuration
Default MS Push Settings
Custom MS Push Settings
Mobile Services Connection Configuration
Offline Destination Only
Offline & Online Destinations
SCC X.509 Virtual Host
SCC X.509 Virtual Port
SCC Standard Virtual Host
SCC Standard Virtual Port
Cloud Connector Location ID
Gateway Service User
Gateway Service Password
Mobile Services Offline Destination Configuration
Username Propagation
Trust All Flag
Destination Preemptive flag
Alternative Host Key Flag
Use Cloud Connector
Mobile Destination Name
DEST_SAM2305_PPROP
Destination Max Connections
100
Destination Connection Timeout
1.200.000
Destination Rewrite Mode
IN_ODP
SSO Method
SCC
Throttling Threshold
-1
Virus Scan Type
None
Destination Max Request Size
134.217.728
Destination Rewrite Rules
Destination Headers
Hostname Verifier Type
STRICT
Mobile Services Online Destination Configuration
Username Propagation
Trust All Flag
Destination Preemptive flag
Alternative Host Key Flag
Use Cloud Connector
Mobile Destination Name
DEST_SAM2305_ONLINE_PPROP
Destination Max Connections
100
Destination Connection Timeout
1.200.000
Destination Rewrite Mode
IN_ODP
SSO Method
SCC
Throttling Threshold
-1
Virus Scan Type
None
Destination Max Request Size
134.217.728
Destination Rewrite Rules

Parent topic: Installing SAP Service and Asset Manager [page 23]

Related Information

Setting Up the Cloud Connector [page 23]
SAP BTP services - Setting Up a Cloud Foundry Environment, Single Instance [page 27]
Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application [page 34]

4.4 Using the SAP Business Technology Platform Mobile Services App Creator to Create an Application

Before you use the App Creator, be sure you've read and are following 2978807: MAIF to CPms Multi-Virtualhost Support.

The Mobile Application Integration Framework (MAIF) includes a tool to automate the integration of SAP BTP services on Cloud Foundry alongside SAP Service and Asset Manager on-premise definitions. The tool is available in the following versions of MAIF:

App Creator Tool Availability

SAP Version	Mobile Application Integration Framework
S4HANA 2021	Included
S4HANA 2020	Included
S4HANA 1909 SPS 03	Included
S4HANA 1809	SAP Mobile Add-On SP08
S4HANA 1709	SAP Mobile Add-On SP08
S4HANA 1610 FPS 01	SAP Mobile Add-On SP08
SAP ECC 6 EHP 8	SAP Mobile Add-On SP07
SAP ECC 6 EHP 7 SP 14	SAP Mobile Add-On SP07

See the following subtopics for detailed information on the fields shown in the App Creator program:

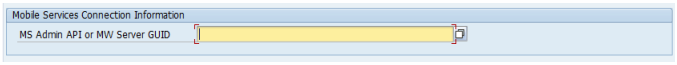
- Defining the SAP BTP services Connection Information [page 35]
- Defining the Mobile Application Integration Framework OData Service [page 38]
- Defining the SAP BTP services Application Settings [page 38]
- Defining the Mobile Service Offline OData Settings [page 39]
- Defining the Mobile Services Connection Configuration [page 41]

Parent topic: Installing SAP Service and Asset Manager [page 23]

Related Information

Setting Up the Cloud Connector [page 23]
SAP BTP services - Setting Up a Cloud Foundry Environment, Single Instance [page 27]
Opening the SAP BTP services App Creator [page 30]

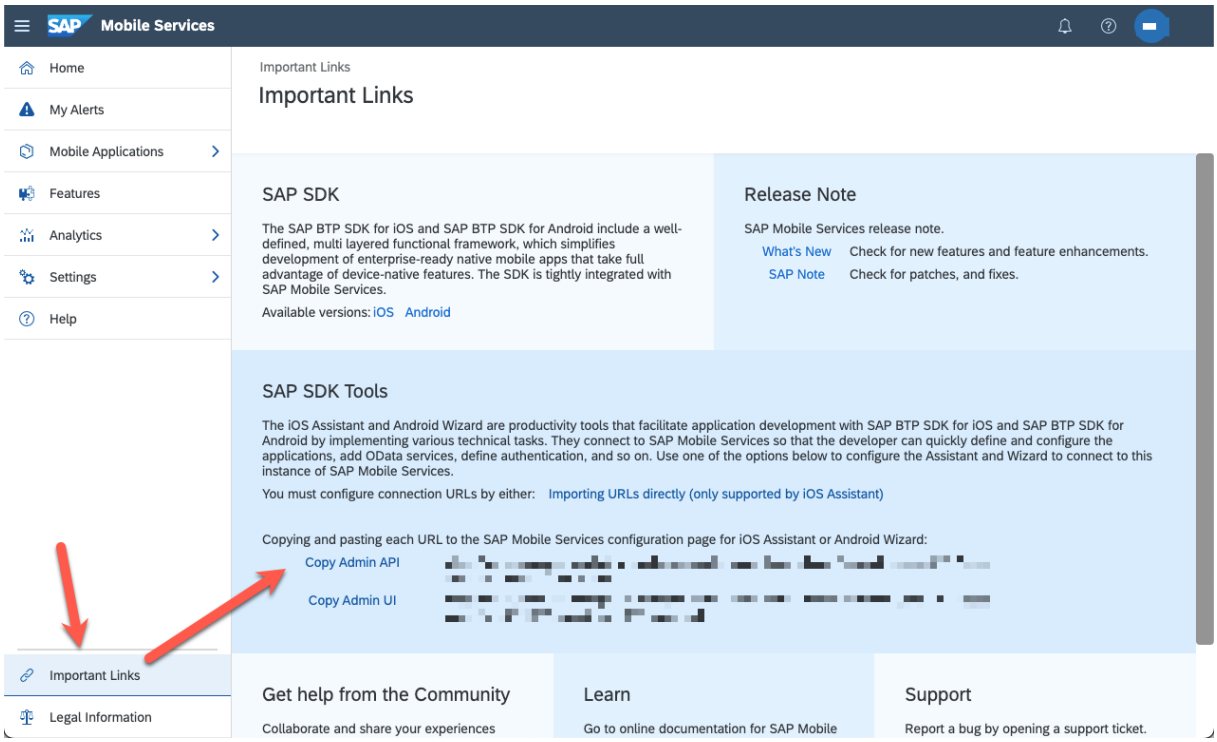
4.4.1 Defining the SAP BTP services Connection Information



There are two ways to use the application:

- Direct connection: If your back end system allows outbound HTTPs connections, you can connect directly to SAP BTP services
- RFC connection: Use this method if your back end system is locked behind a firewall that disallows direct outbound HTTs connections and needs to be routed through a proxy. Establishing an RFC connection requires populating the *Mobile Services Connection Information* with the *Middleware Server GUID*.

Retrieve the *Admin API* from the *Important Links* section, regardless of which method you're using to connect.



Option 1: Directly Connecting to SAP BTP services from the Back End System

For systems that do not require outbound proxies or special certificate configurations, you can copy the *Admin API* directly from the *Important Links* section of SAP BTP services. Paste the Admin API into the *MS Admin API* or *MW Server GUID* field.

Option 2: Establishing RFC Connection Information for the SAP BTP services App Creator

> **Note**
>
> To correctly configure metrics reporting, complete the RFC Connection: Integrating SAP Cloud Reporting for MAIF-Based Mobile Applications on SAP BTP services for Cloud Foundry procedure before establishing an RFC connection through the App Creator program.

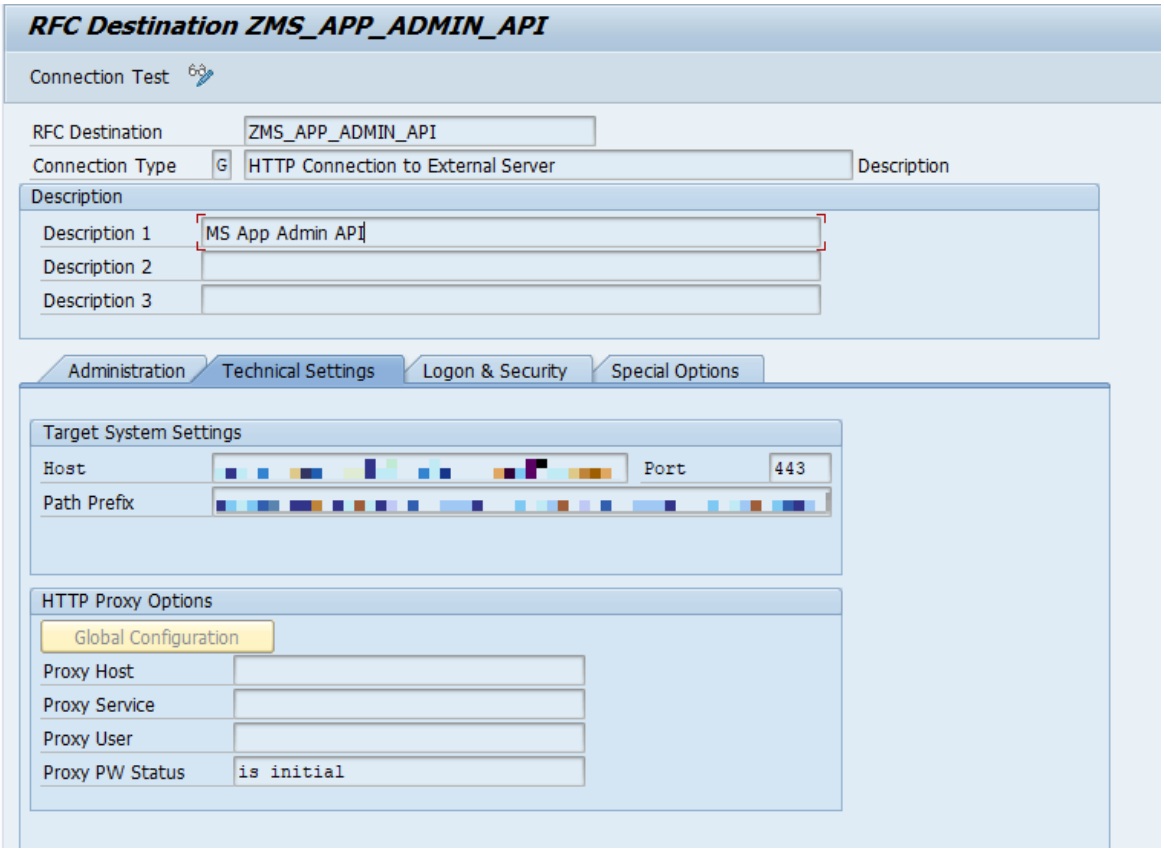
An option is available to define the special settings in an RFC connection using transaction *SM59* that wraps the connection with the middleware server GUID to reference by the calling application. Use this option for systems that require outbound proxies or special certificate configurations not captured by the standard direct HTTPs outbound communication methods that SAP back end systems use.

The middleware server GUID is generated when a middleware server is defined in the Administration Portal. The defined middleware server should point to the MS Admin API URL, with */app* appended.

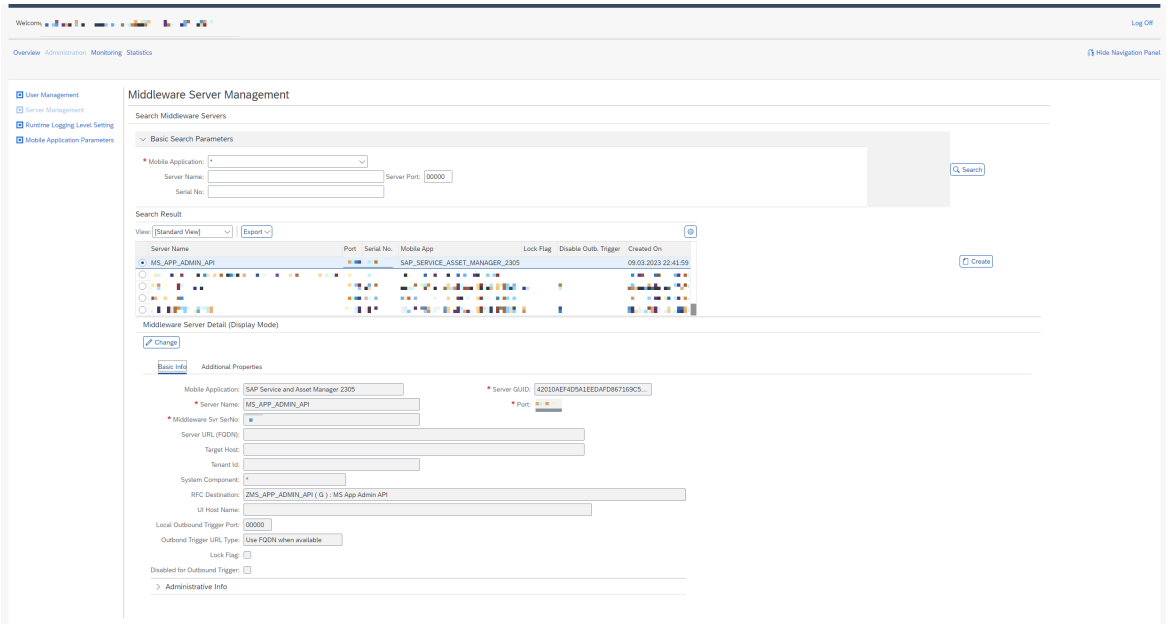
Use the F4 help to return a list of all defined middleware servers.

1. Open the *Configuration of RFC Connections* using transaction *SM59*.
2. Create an RFC destination of type *G*:
    1. Retrieve the hostname of the admin API without any of the path following the hostname. Populate the information into the *Host* field.
    2. Populate the *Path Prefix* field with the rest of the path in the admin API. Append *app* to it with no trailing slash.
    3. Complete the *HTTP Proxy Options* as required by your firewall rules.
    4. Enable the SSL connection settings.

    See the following screenshot for an example of RFC destination settings with the following settings:
    - Connection Type: G
    - Target Host: mobile-service-example.hana.ondemand.com
    - Port (Service No.): 443
    - Path Prefix: /cockpit/v1/org/ExampleOrg/space/ExampleSpace/app
    - SSL: Active



3. Open the *Administration Portal* using transaction */syclo/admin*.
4. Select the *Administration* tab.
5. Click *Server Management*, then click *Create*.
6. Create a meaningful server name.
7. Provide the *RFC Destination* or the *UI Host Name* and *Server URL* pointing to the MS Admin API created in *Step 2*.
8. Select the mobile application for which you are creating a mobile services application.
   See the following screenshot for an example of the middleware server management configuration with the following settings:
   - UI Host Name: https://mobile-service-example.hana.ondemand.com
   - Server URL: /cockpit/v1/org/ExampleOrg/space/ExampleSpace/app



9. Save your changes.

4.4.2 Defining the Mobile Application Integration Framework OData Service

Mobile Application Integration Framework oData Service	
oData Sevice Mobile App	SAP_SERVICE_ASSET_MANAGER_2305
oData Service Technical Name	/MERP/SAP_SRV_ASSET_MANAGER_2305
oData Service Group Version	1

Your MAIF mobile app selection corresponds to an application that serves as an OData service to mobile devices through the definitions defined in */syclo/configpanel*.

> **Note**
>
> The MAIF mobile app must correspond to the application serving as an OData service for proper generation of mobile app settings in SAP BTP services.

4.4.3 Defining the SAP BTP services Application Settings

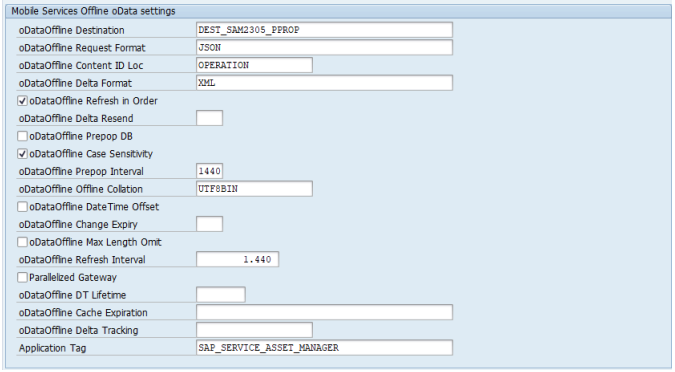
Mobile Services Application Settings	
MS Application ID	SAP.SAM2305
MS Application Name	SAP_SERVICE_ASSET_MANAGER_2305
MS Application Description	SAP_SERVICE_ASSET_MANAGER_2305
MS Vendor Name	SAP
MS Application Timeout	1.200.000
MDK Onboarding URI Schema	samclient

Mobile Services Application Settings

Field Name	Description	Standard or Advanced View
MS Application ID	Unique identifier for your cloud platform instance of SAP BTP services to identify a series of configurations associated with a given, defined, mobile application. The application ID must be unique per instance of mobile services admin API.	Standard
MS Application Name	Any text displayed on the SAP BTP cockpit for administration	Standard
MS Application Description	Any text displayed on the SAP BTP cockpit for administration	Standard
MS Vendor Name	Name of the vendor providing the application definitions	Standard
MS Application Timeout	Amount of time before a mobile device connected to the mobile application in SAP BTP services should wait before being considered timed out	Standard
MDK Onboarding URI Schema	Defines how the SAP BTP services app will generate a QR code for onboarding of mobile devices to the mobile application. Depending on the version of the mobile application client you are using, this value needs to correspond with the client that will launch the mobile application when the QR code is scanned. Common examples are *mdkclient* for the SAP Mobile Development Kit client or *samclient* for the SAP Service and Asset Manager application downloaded from the iOS App Store or Android Play Store.	Advanced

4.4.4 Defining the Mobile Service Offline OData Settings

If the SAP Gateway connected to the back end SAP system is running as a parallelized gateway or a gateway hub, select this option to ensure the proper generation of data is being sent to the mobile devices.



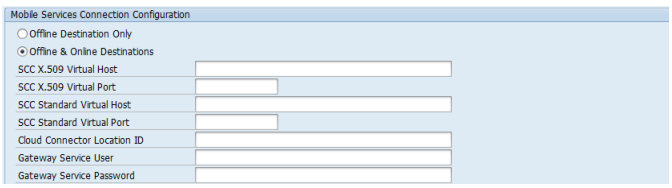
Mobile Services Application Settings

Field Name	Description	Standard or Advanced View
Application Tag	Application tag that is appended to all attempts at synchronizing SAP mobile applications using the Mobile Application Integration Framework and the SAP back end system. Application tags are used to count licensed users in a given environment and must stay consistent. If the application tag is incorrectly generated in a production environment, the connection to SAP Cloud Reporting for reporting usage metrics could be conpromised. The application could fail due to failed licensing checks. See Configuring Customer Usage Metrics for more information.	Advanced
oDataOffline Destination	The mobile services destination which the oDataOffline service uses to sync local versions of mobile device databases that allow mobile applications to work offline. This field must match the mobile destination name as listed in Defining the Mobile Services Connection Configuration [page 41]	Advanced
oDataOffline Request Format	Format with which mobile services requests data that will be populated in the local mobile databases from the back end SAP system. JSON is the standard value for MAIF support applications.	Advanced
oDataOffline Content ID Location	The contentID type of files downloaded by the oDataOffline Service. Choose either MIME or OPERATION based on your system setup.	Advanced
oDataOffline Delta Format	Format with which mobile services requests data that is populated in the local mobile databases from the SAP back end systems during a delta sync (all subsequent syncs that occur after the mobile device has completed onboarding). Depending on the SAP Gateway version, JSON may or may not be supported. XML is always supported.	Advanced
oDataOffline Refresh in Order	Determines whether or not mobile services will respect the order of oData entities as defined by the MAIF configuration. This flag must remain ON for all MAIF-supported applications.	Advanced
oDataOffline Delta Resend	Not used by MAIF applications. For more information, see the *max_delta_resends* row in the Application Configuration File topic.	Advanced
oDataOffline Prepopulate DB	Not used by MAIF applications. For more information, see the *prepopulate_offline_db* row in the Application Configuration File topic.	Advanced

Field Name	Description	Standard or Advanced View
oDataOffline Case Sensitivity	Determines whether or not data transmitted to mobile services retains its case during data transmission. For proper functionality of MAIF-supported applications, this flag must remain ON.	Advanced
oDataOffline DateTime Offset	Not used by MAIF applications. For more information, see the *json_datetimeoffset_in_utc* row in the Application Configuration File topic.	Advanced
oDataOffline Change Expiry	Not used by MAIF applications. For more information, see the *local_change_expiry* row in the Application Configuration File topic.	Advanced
oDataOffline Max Length Omit	Not used by MAIF applications. For more information, see the *allow_omitting_max_length_facet* row in the Application Configuration File topic.	Advanced
oDataOffline Refresh Interval	Maximum amount of time to cache entities in the oDataOffline sync database. Value is set to *1440* by default.	Advanced
oDataOffline DT Lifetime	Lifetime of the delta tokens generated in oDataOffline. MAIF-supported applications use delta tokens managed and generated by the SAP back end system, so this field is not used.	Advanced
oDataOffline Cache Expiration	Maximum amount of time to cache the oDataOffline database	Advanced
oDataOffline Delta Tracking	Flag to determine whether or not mobile services tracks changes between cached data on mobile services and the SAP back end system. This field is not used in MAIF-supported applications.	Advanced

4.4.5 Defining the Mobile Services Connection Configuration

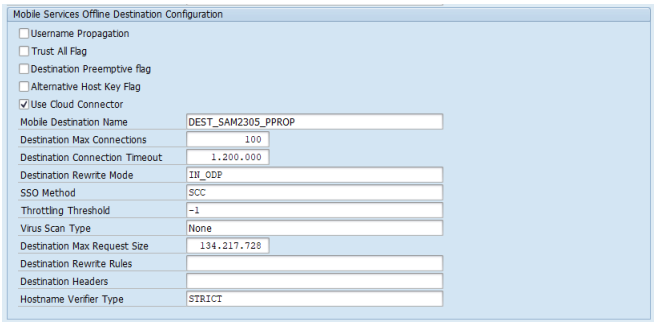
The following topic only goes over the interaction of how the mobile services application creator bundled with MAIF utilizes these definitions for use with supported mobile applications. For detailed information regarding mobile services connectivity definitions, see the Defining Connectivity topic in the *SAP Mobile Services Administration* guide.



Mobile Services Connection Configuration

Field Name	Description	Standard or Advanced View
SCC X.509 Virtual Host	The virtual host defined by the Cloud Connector that allows an SAP BTP resource to identify a specific SAP Gateway server, configured with principal propagation through x.509 certificate generation.	Standard
SCC X.509 Virtual Port	Port assigned to the virtual host	Standard
SCC Standard Virtual Host	No longer in use	Standard
SCC Standard Virtual Port	No longer in use	Standard
Cloud Connector Location ID	Location ID used to identify a given connection between a Cloud Connector and an SAP BTP subaccount. Can also be labled *Cloud Connector ID* **Note** This is the location ID and not the cloud connector ID	Standard
Gateway Service User	Technical user allowed to perform an HTTPS ping against the SAP Gateway for connectivity testing purposes.	Standard
Gateway Service Password	Password for the Gateway Service User	Standard
Offline Destination Only	Does not create the online destination in the mobile services application. For more information, see the *Mobile Services Offline Destination Configuration* section in this topic.	Advanced
Offline and Online Destinations	Creates both online and offline destinations. For more information, see the *Mobile Services Offline Destination Configuration*and the *Mobile Services Online Destination Configuration* sections in this topic.	Advanced

Mobile Services Offline Destination Configuration



Mobile applications supported by the Mobile Application Integration Framework support offline destinations by default. Offline destinations are OData services provided by MAIF for complete download and sync with

the mobile app. The services automatically handle data distribution, conflict resolution, and mobile offline application usage.

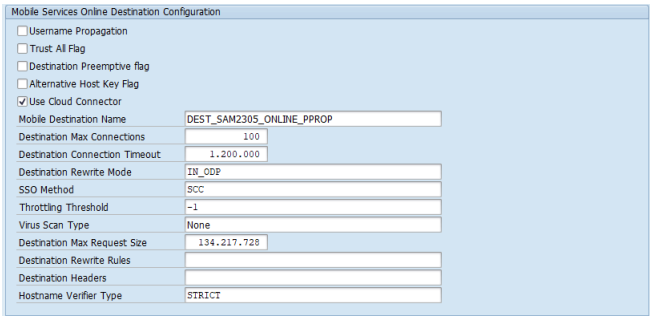
The primary operation of applications connecting to offline destinations in SAP BTP services is through the oDataOffline framework on the mobile device. Changes made to data on the local devices must be synced with the back end database on demand.

Mobile Services Offline Destination Configuration

Field Name	Description	Standard or Advanced View
Username Propagation	Enables the Username propagation flag on SAP Mobile Services Connectivity	Advanced
Trust All flag	Not used by MAIF applications	Advanced
Determination Preemptive flag	Not used by MAIF applications	Advanced
Alternative Host Key flag	Not used by MAIF applications	Advanced
Use Cloud Connector	Must be selected for on-premise back end servers	Advanced
Mobile Destination Name	Name of the mobile destination defined in the client metadata. The name in this field must match the name of the destination defined by the MDK metadata.	Advanced
Destination Max Connections	Maximum number of simultaneous users downloading data from the destination	Advanced
Destination Connection Timeout	The longest amount of time expected for each request to spend downloading from the destination	Advanced
Destination Rewrite Mode	Method used to rewrite mobile services URLs to back end service URLs. *IN_ODP* is the standard rewrite mode that is compatible with the cloud connector rewrite modes from the SCC's virtualhost definitions	Advanced
SSO Method	The single sign-on method used to identify mobile application users to the back end system. SCC is the standard cloud connector principal propagation mode.	Advanced
Throttling Threshold	Not used by MAIF applications The default of *-1* is held in this field	Advanced
Destination Max Request Size	The maximum size of a request for requests being sent to the mobile device	Advanced
Destination Rewrite Rules	If the Destination Rewrite mode is set to *custom*, the custom definitions for mobile services can be entered here	Advanced

Field Name	Description	Standard or Advanced View
Destination Header	Custom headers can be inserted here for the connection. If the SAP Gateway system being connected to the SAP BTP services instance does not have the default client set to the client hosting the data being requested, the client can be overwritten. See the following format for an example: Sample Code `{ "name": "sap-client", "value": "001", "overwrite": true }`	Advanced
Hostname Verifier Type	Not used by MAIF applications The default of *STRICT* is held in this field	Advanced

Mobile Services Online Destination Configuration



Mobile applications supported by MAIF have supported online destinations since October 2017. Online destinations are OData services provided by MAIF for on-demand download and data sync with the mobile applications. Online destinations are useful for a mobile application that frequently handles updating data that must be downloaded in real time and can only be accessed while the mobile device has an internet connection.

Mobile Services Offline Destination Configuration

Field Name	Description	Standard or Advanced View
Username Propagation	Enables the Username propagation flag on SAP Mobile Services Connectivity	Advanced
Trust All flag	Not used by MAIF applications	Advanced
Determination Preemptive flag	Not used by MAIF applications	Advanced

Field Name	Description	Standard or Advanced View
Alternative Host Key flag	Not used by MAIF applications	Advanced
Use Cloud Connector	Must be selected for on-premise back end servers	Advanced
Mobile Destination Name	Name of the mobile destination defined in the client metadata. The name in this field must match the name of the destination defined by the MDK metadata.	Advanced
Destination Max Connections	Maximum number of simultaneous users downloading data from the destination	Advanced
Destination Connection Timeout	The longest amount of time expected for each request to spend downloading from the destination	Advanced
Destination Rewrite Mode	Method used to rewrite mobile services URLs to back end service URLs. *IN_ODP* is the standard rewrite mode that is compatible with the cloud connector rewrite modes from the SCC's virtualhost definitions	Advanced
SSO Method	The single sign-on method used to identify mobile application users to the back end system. SCC is the standard cloud connector principal propagation mode.	Advanced
Throttling Threshold	Not used by MAIF applications The default of *-1* is held in this field	Advanced
Destination Max Request Size	The maximum size of a request for requests being sent to the mobile device	Advanced
Destination Rewrite Rules	If the Destination Rewrite mode is set to *custom*, the custom definitions for mobile services can be entered here	Advanced
Destination Header	Custom headers can be inserted here for the connection. If the SAP Gateway system being connected to the SAP BTP services instance does not have the default client set to the client hosting the data being requested, the client can be overwritten. See the following format for an example: Sample Code `{ "name": "sap-client", "value": "001", "overwrite": true }`	Advanced
Hostname Verifier Type	Not used by MAIF applications The default of *STRICT* is held in this field	Advanced

5 Installing the SAP Service and Asset Manager Client

When you first install and start the SAP Service and Asset Manager application, a demo version is loaded, complete with demo data. Use the demo version to acclimate yourself to the app before connecting to the SAP Business Technology Platform.

Prerequisites

- A connection to the internet is required so you can download the SAP Service and Asset Manager application.
- **iOS**:
  - Your iOS mobile device version must be 15.x or 16.x.
  - We recommend iOS devices that have been released in the past two years.
- **Android**:
  - Your Android mobile device version must be 11.x, 12.x, or 13.x.
  - We recommend Android devices with the following specifications:
    - At least 4 GB RAM.
    - Quad-core or Octa-core processor.
    - At least 64 GB storage.
- See 3342977: *Software Release Note - SAP Service and Asset Manager 2305*, for a complete list of back end and device requirements for the SAP Service and Asset Manager 2305 mobile application.

Context

Download the SAP Service and Asset Manager application to your mobile device from the App Store (iOS) or SAP Software Download Center (Android). A demo version is initially loaded. When you are ready to begin working with the true application, exit the demo, log in, and begin working.

Procedure

1. In the App Store Search box, type **`SAP Asset Manager`** and tap *Search*.

   The application description opens.
2. Tap *Free* and then tap *Install*.

   The SAP Service and Asset Manager client application is downloaded from the store. After the download, an SAP Service and Asset Manager application icon appears on the mobile device.

3. Tap the icon to open the application.

Results

The SAP Service and Asset Manager client is installed on your mobile device. See the Initial Log In to the SAP Service and Asset Manager Application [page 50] procedure for information on how to access the application and begin work.

> **Note**
>
> To check the version of the client software, tap the *Information* icon on the *Module* screen of the mobile device.

Next Steps

Dark mode is available for the SAP Service and Asset Manager client application. Access the *Settings* menu for your iOS or Android device. Find the dark mode setting in the *Display* menu.

5.1 Obtain SAP Service and Asset Manager Onboarding URL or QR Code

Context

Use the following procedure to generate an onboarding QR code for the SAP Service and Asset Manager. The parameters needed for the procedure are as follows:

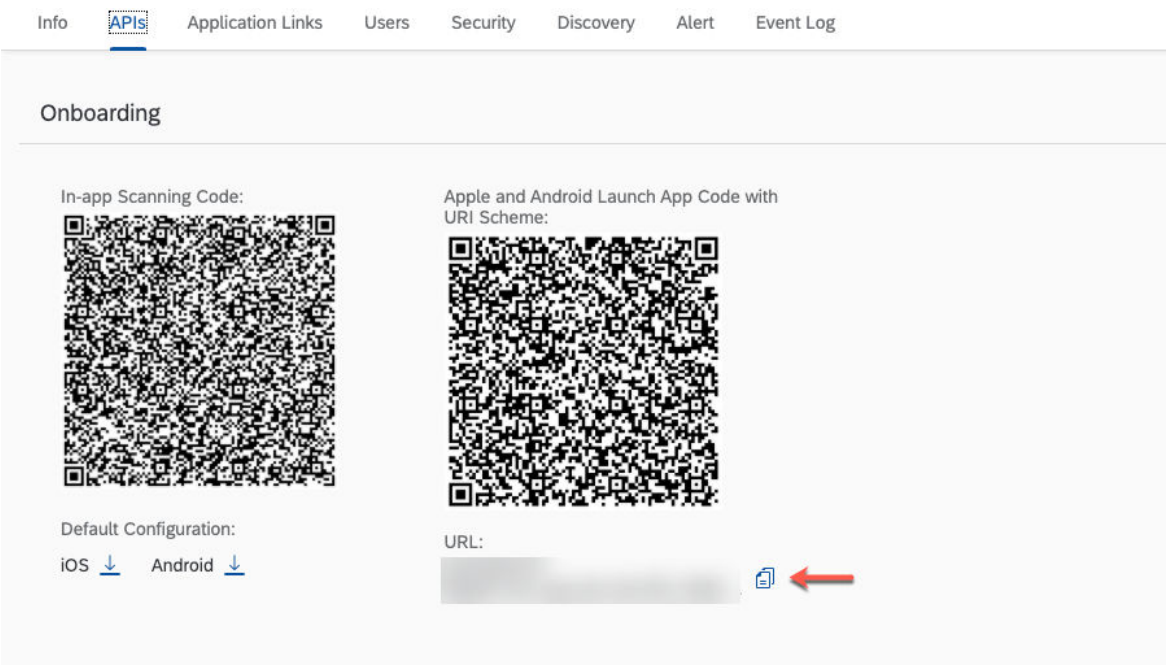
Attribute Name	Value
Apple Device Application URI Scheme	samclient
Android Device Application URI Scheme	samclient
Mobile Device Application Type	Mobile Development Kit

Procedure

1. Using the SAP Business Technology Platform Mobile Services Cockpit, navigate to the *sap.sam<XXXX>* application, where *<XXXX>* is the release version.

2. Select the *Application Links* tab. Find the *Device Application URI Scheme* section and click *Edit*.
3. Enter the parameters as shown in the table in this procedure.
4. Open the `<Device Application>` drop-down list and select *Mobile Development Kit*. Then click *OK*.
5. Click *OK* in the Confirm Save dialog window to confirm the save.
6. Navigate to the *APIs* tab.

   The launch app QR codes are now available in the *Onboarding* section.



Next Steps

Continue to the Download the SAP Service and Asset Manager Mobile Application [page 48] procedure. When prompted, scan the QR code using your mobile device, or copy and paste the URL to your device browser.

5.2 Download the SAP Service and Asset Manager Mobile Application

Prerequisites

A connection to the internet is required so you can download the SAP Service and Asset Manager application.

Context

Download the SAP Service and Asset ManagerSAP Service and Asset Manager application to your mobile device from the App Store (iOS) or SAP Software Download Center (Android). A demo version is initially loaded. When you're ready to begin working with the true application, exit the demo, log in, and begin working.

Procedure

1. **Download the mobile application:**
   a. In the App Store Search box, type **SAP Service and Asset Manager** and tap *Search*.
   b. Tap *Free* and then tap *Install*.

      The SAP Service and Asset Manager client application is downloaded from the store. After the download, an SAP Service and Asset Manager application icon appears on the mobile device.
   c. Tap the icon to open the application.

      The SAP Service and Asset Manager client is installed on your mobile device. Continue to the next step to access the application and begin work.

      > ⓘ Note
      >
      > To check the version of the client software, tap the *Information* icon on the *Module* screen of the mobile device.

2. **Verify that app deployment is successful:**
   a. Tap on the SAP Service and Asset Manager icon.

      The SAP Service and Asset Manager splash screen appears.
   b. Click the *Profile* icon on the top right of the screen. Reset the client by clicking *RESET*.
3. **Onboard your device:**
   a. On the initial screen of the SAP Service and Asset Manager application, click *Start*. When the *Activation* screen appears, choose *QR CODE SCAN*.
   b. Choose *Allow* to permit the application to take pictures.
   c. Scan the QR code (generated in the Obtain SAP Service and Asset Manager Onboarding URL or QR Code [page 47] task) located on the *APIs* tab of the SAP Business Technology Platform Mobile Services.
   d. Log in using your SAP Business Technology Platform email address and password credentials.
   e. Read the End-User License Agreement and click *Agree* to accept.
   f. Choose your device passcode. Reconfirm the passcode when prompted. If available on your device, you can choose to use either your passcode or a biometric login for subsequent logins.
4. Log in to the SAP Service and Asset Manager application.

   The SAP Service and Asset Manager application performs an initial transmit to bring down all of your jobs, notifications, assets, equipment, and other objects. Depending on the size of your application, the transmit could take several minutes. When finished, the main *Overview* screen is shown and you're ready to explore the application.

5.3 Initial Log In to the SAP Service and Asset Manager Application

During the initial logon process, set a numerical passcode to unlock the application without having to enter your user name and password each time the application or the mobile device is locked.

Context

To work with your application, first log in with a corporate user name and password. Then, set a secondary personal passcode known only to you to easily unlock the application when it is locked on your device. You do not need to enter your user name and password after the initial log on, only the passcode.

Touch ID is supported on iOS and Android models with the capability and with users who choose to implement the Touch ID feature.

Procedure

1. Tap on the app icon to open the application.

   The application splash screen appears.

   > ⓘ Note
   >
   > You can try out the app in demo mode before using it productively with your business data. To launch the app in demo mode, tap on *Try the Demo*, and ignore the remaining steps.

2. On the initial screen of the application, read the End-User License Agreement and click *Agree* to accept.
3. Scan the QR code provided to you by your administrator.

   > ⓘ Note
   >
   > **For Administrators:** You can generate an application QR code through the *APIs* tab in the SAP BTP cockpit.

4. Log in using your SAP BTP email address and password credentials.
5. Choose your device passcode. Reconfirm the passcode when prompted.

Results

The application performs an initial transmit to bring down all of your assigned objects, such as work orders, notifications, or equipment. Depending on the size of your application, the transmit could take several minutes. When finished, the main *Overview* screen is shown and you are ready to begin to work with the application.

> **Note**
>
> If your customer site has enabled digital registration, a pop-up wizard appears. See the Registering Digital Signature procedure for information on how to register.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP