PUBLIC
SAP Asset Manager
Document Version: 4.0 1911 – 2019-12-04

SAP Asset Manager Security Guide

THE BEST RUN SAP

Content

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/viewer/product/SAP_ASSET_MANAGER/p/en-US.

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

Document Version	Date	Description of Changes
1911	NOV 2019	Original release

1 Introduction

Provides an overview of the security-relevant information that apply to SAP Asset Manager.

About This Document

The Security Guide provides an overview of the security-relevant information that apply to the SAP Asset Manager solution, and can be used as a reference for security requirements of non-SAP on premise components.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the User Guide. Such guides are only relevant for a certain phase of the software lifecycle, whereas the Security Guide provides information that is relevant for all life cycle phases.

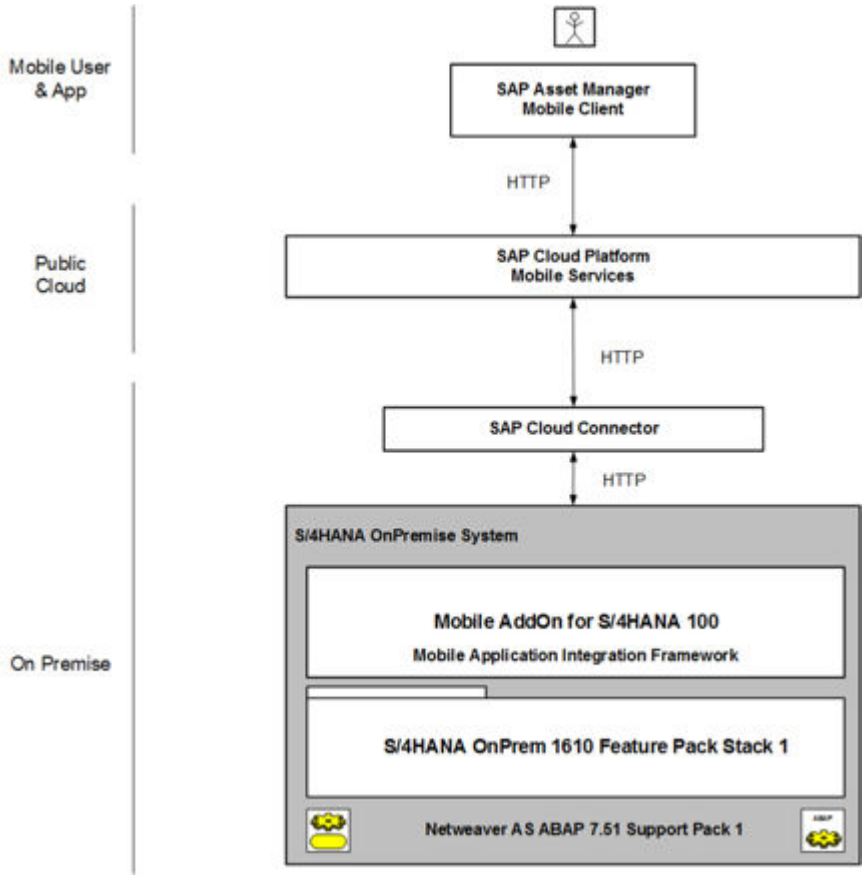
Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, ensure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Asset Manager. To assist you in securing SAP Asset Manager, we provide this Security Guide.

2 Technical System Landscape

SAP Asset Manager works with personal and transactional data.

The following diagram describes the technical landscape used by the current SAP Asset Manager version:



A brief explanation of the components:

- **SAP Asset Manager mobile client:** mobile application available both for SAP Asset Manager for iOS and SAP Asset Manager for Android
- **SAP Cloud Platform Mobile Services:** Provides service
- **Cloud Connector:** Connects the SAP Cloud Platform to the on-premise SAP S/4HANA system
- **SAP S/4HANA Enterprise Management on-premise 1610 Feature Pack Stack 1:** The SAP system of the customer running an enterprise business process, such as a plant maintenance module used by the SAP Asset Manager application

3 SAP Asset Manager Mobile Client Security

The SAP Asset Manager application uses the OAuth 2.0 protocol to authenticate users and to get authorization to access data on the SAP S/4HANA on-premise system.

The OAuth token that is obtained during the onboarding process is encrypted with 256-bit AES encryption using the passcode set up by the user. If the passcode is deactivated, a default key is used. User settings are persisted securely through the same 256-bit AES encryption.

For iOS devices, if passcode protection is activated, the screen blurs whenever the application goes to background to hide any sensitive data in the screenshot iOS takes and displays to show any recently used applications. SAP Asset Manager supports Face ID, Touch ID, and passcode protection to unlock the application on subsequent launches and idle timeouts. The Face ID, Touch ID, and/or passcode are saved on the mobile device using iOS Device Keychain.

For Android devices, if passcode protection is activated, the screen blurs whenever the application goes to background to hide any sensitive data in the screenshot Android takes and displays to show any recently used applications. SAP Asset Manager supports biometric authentication and passcode protection to unlock the application on subsequent launches and idle timeouts. The fingerprint authentication and/or passcode are saved on the mobile device using the device keychain.

Although it is not mandatory to use a passcode, we strongly recommend to set one for SAP Asset Manager.

Securing the Data Device Store

After users access the SAP Asset Manager application, they are redirected to the oAuth service and associated Identity Provider to retrieve an oAuth 2.0 token. The oAuth token is used to authenticate all traffic into the mobile services that provide data to the mobile client.

For iOS devices, after the token is retrieved, the token itself, along with any data, is secured in the offline data store of the mobile device. The offline data store is encrypted with a user defined password. Access to the offline data store to use the data or the oAuth token requires the iOS Keychain to unlock and decrypt the data store on the mobile device.

For Android devices, after the token is retrieved, the token itself, along with any data, is secured in the offline data store of the mobile device. The offline data store is encrypted with a user defined password. Access to the offline data store to use the data or the oAuth token requires the device keychain to unlock and decrypt the data store on the mobile device.

If the user or an administrator uninstalls the SAP Asset Manager application, or the content of the device and the settings are reset, the user must set a new password to unlock, and decrypt the data store. Previous data from the data store is permanently lost.

4 SAP Cloud Platform Security

SAP Asset Manager requires the SAP Cloud Platform Mobile Service to provide user onboarding, user authentication, mobile application lifecycle management, and OData offline support.

> **i Note**
>
> Enable OAuth 2.0 based user authentication for SAP Cloud Platform as required by SAP Asset Manager.

For more information about SAP Cloud Platform security, see the Web site, SAP Cloud Platform Security: Trust Matters.

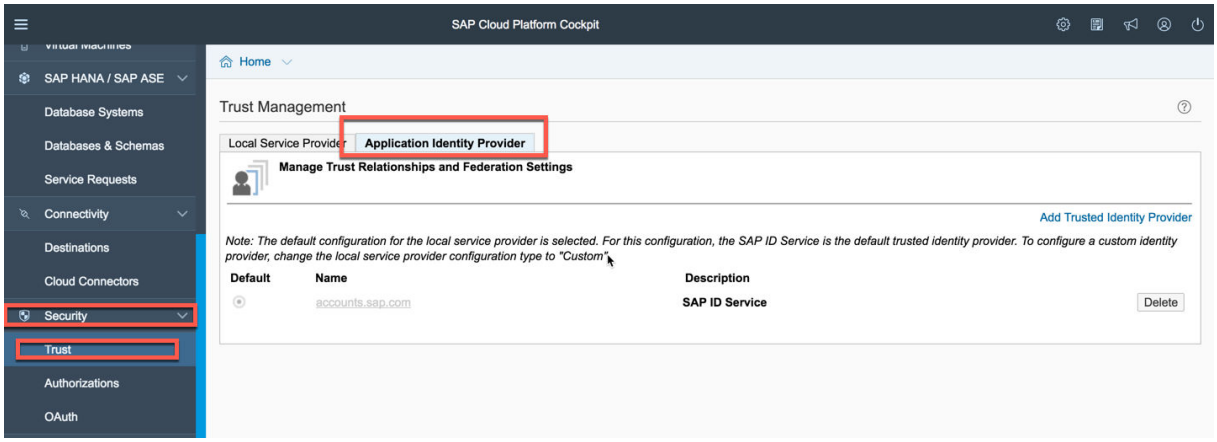
SAP Asset Manager requires user principle propagation when setting up a mobile destination in the SAP Cloud Platform Mobile Service. User principle propagation is necessary to properly perform data distribution calculation and authorization checks in the SAP back-end system.

For more information about the SAP Cloud Platform Mobile Service, see the SAP Cloud Platform Mobile Service for Development and Operations guide.

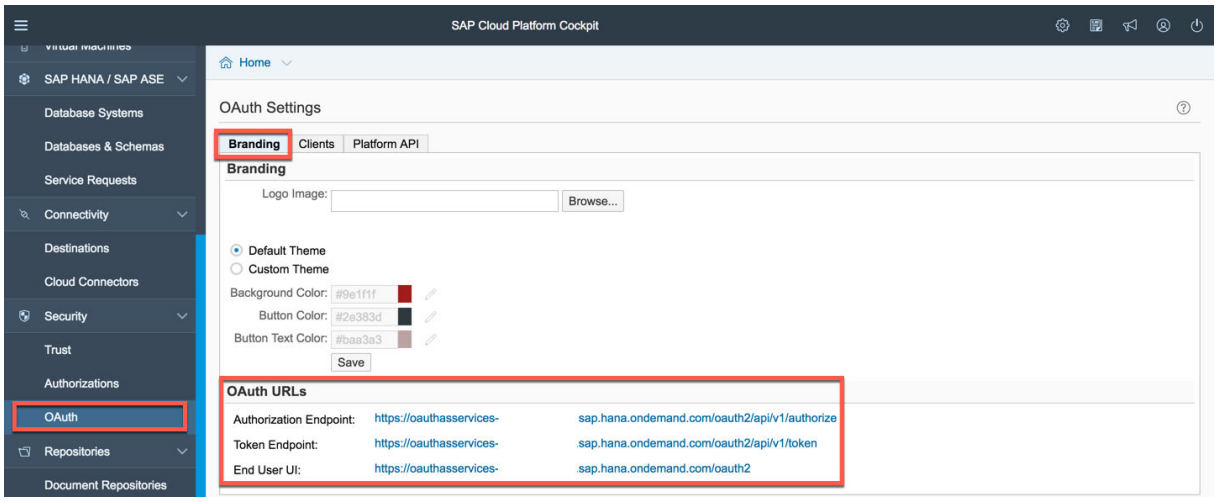
SAP Cloud Platform OAuth Authentication Service

SAP Cloud Platform offers an OAuth 2.0 user authentication service that communicates with an Identity Provider or local trust store to provide a secure method of passing valid credentials through HTTP calls.

Using the SAP Cloud Platform Cockpit, set Identity Providers in the *Trust* section of the *Security* page, under the *Application Identity Providers* tab:



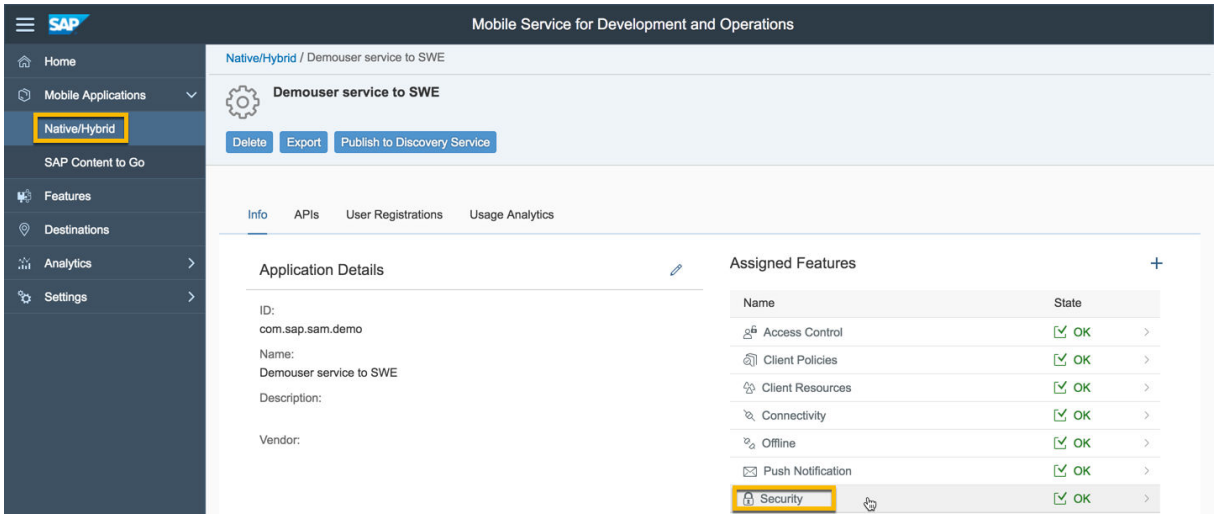
Once you set the Identity Provider, configure the OAuth service to generate tokens for requests accepted by the Identity Provider. Configure the requests using standard OAuth 2.0 token retrieval methods through the URLs on the bottom of the *Branding* tab:



Adding an OAuth Authentication Client to a Mobile Services Application

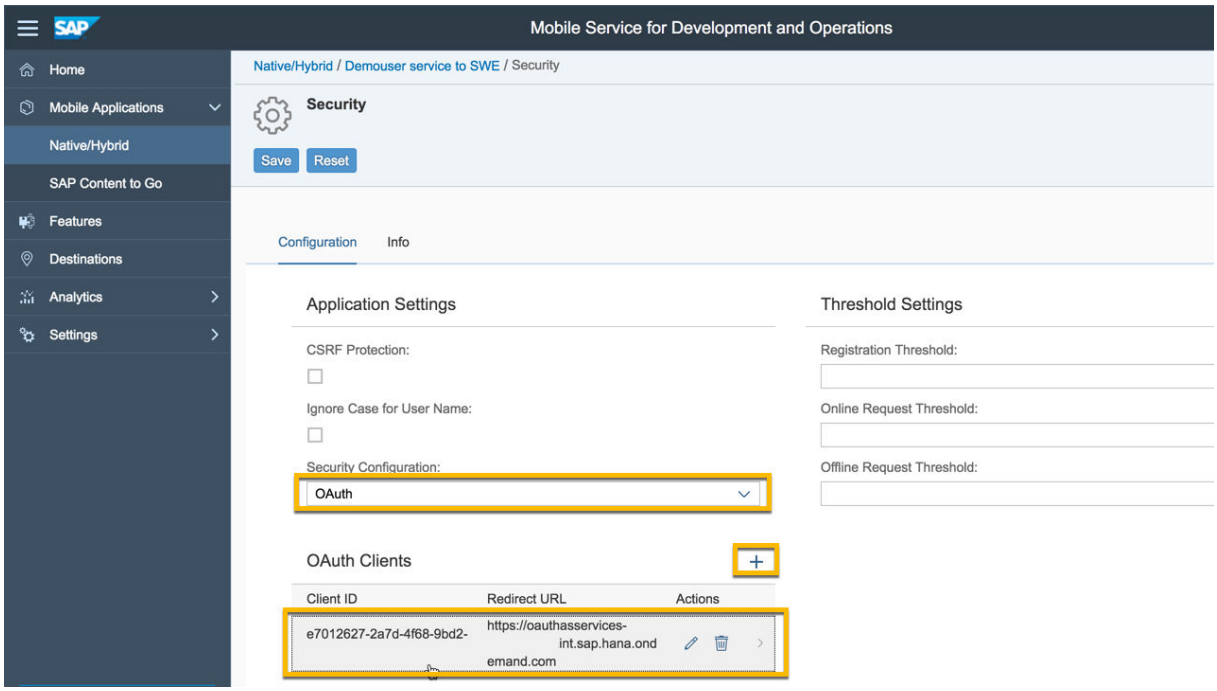
When you create a mobile services application to provide OData services to client applications, you can secure the application by using the SAP Cloud Platform as the authorization server through the oAuth service it provides. To secure the application, enable the *Security* feature of the mobile service application. Then, configure it to use the oAuth service of the SAP Cloud Platform that was previously set up. Finally, add the client to the security settings of the application.

Adding a client to the OAuth platform service of the SAP Cloud Platform is performed as a *Security* feature in the *Mobile Application* configuration on the Mobile Services Cockpit:



Inside of the security features of the application, set the *Security Configuration* to `<OAuth>` to use OAuth 2.0 tokens to authenticate to the application. Setting this field ensures that users can repeatedly authenticate into the application for the life of the OAuth token without having to contact the Identity Provider to enter their

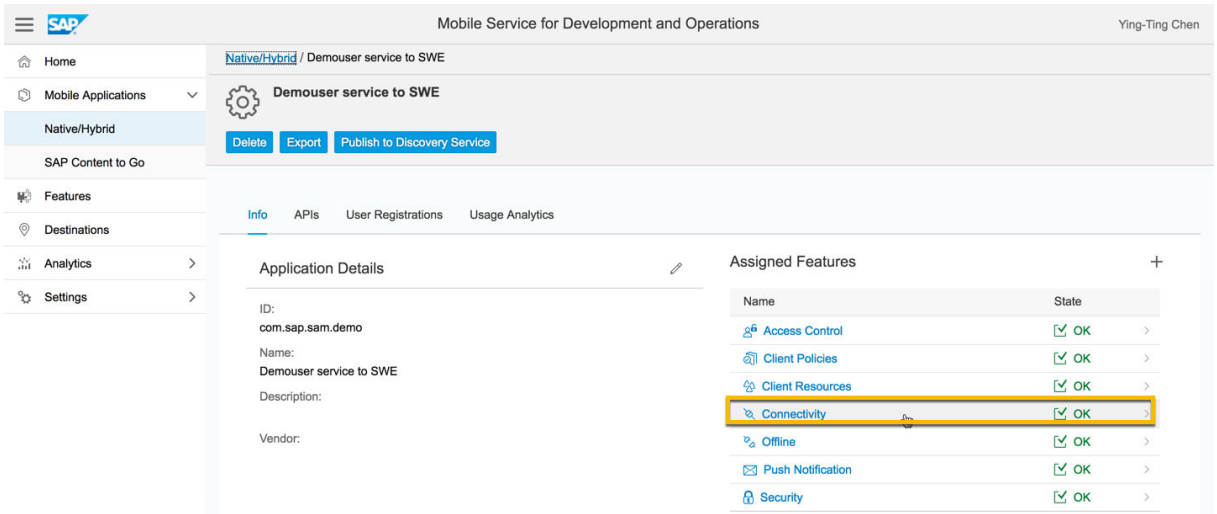
credentials again. The OAuth service tracks the identity of the token and uses the token to authenticate users into the application, as the token is passed in with the connection attempts. You can add individual clients to include individual redirect URLs or token expiration dates if necessary.



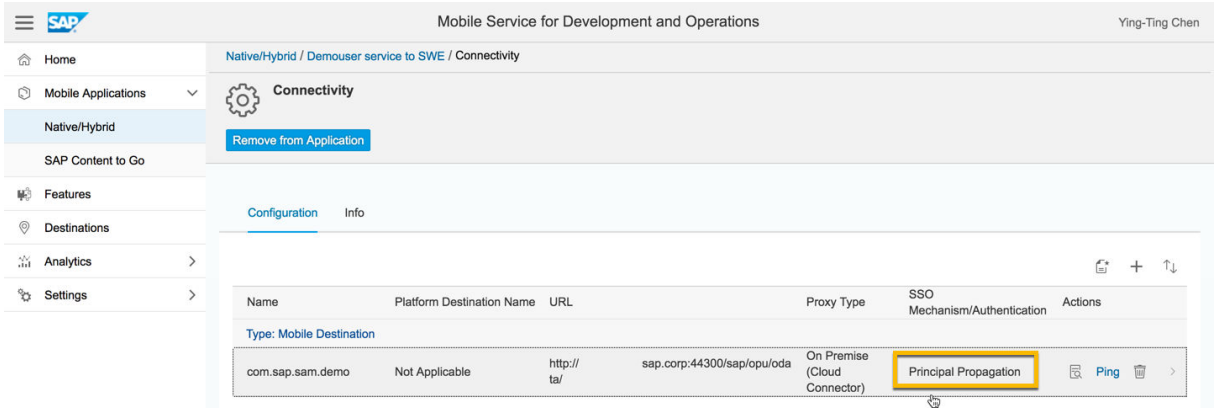
Configuration Principle Propagation to Backend Connections

Authentication to an individual component served by Mobile Services does not ensure authentication to a backend service. To propagate the authentication information of the application to the backend service, turn on principle propagation of the destination that is set as the backend connection of the application.

Check the setting in the *Connectivity* tab of the *Mobile Application*.

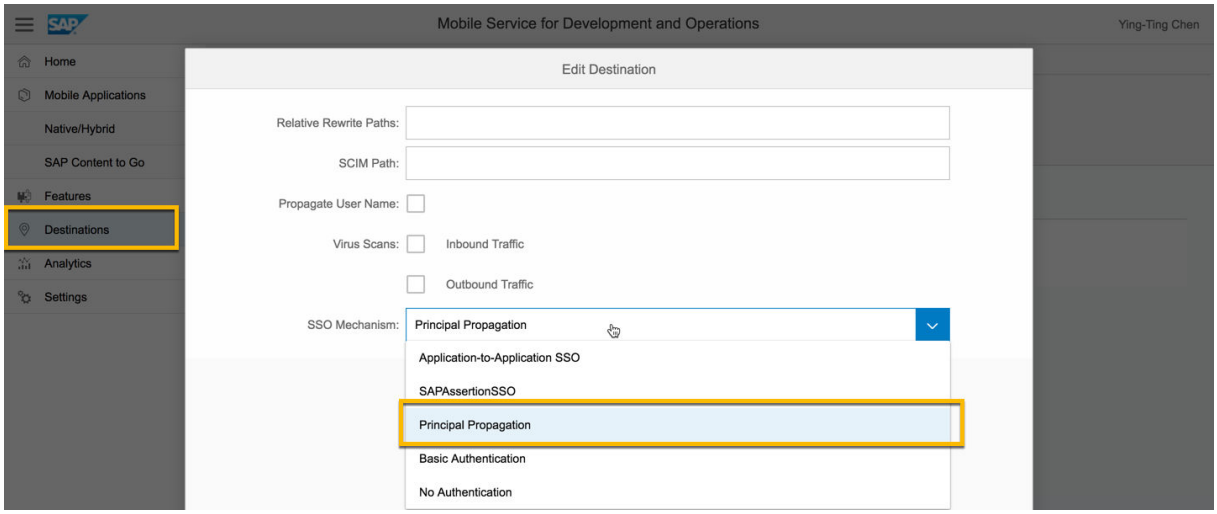


Configure the security method of the connection for *Principle Propagation*. If it is not configured for principle propagation, it will not provide the credentials from the application to the on-premise back-end system that is providing the data service for the SAP Mobile Add-On



To edit the connection to the backend, edit it in the *Destinations* tab of the Mobiles Services Cockpit.

To edit the connection, select the connection, click *Edit*, and navigate through the wizard to the *SSO Mechanism* page. Change the *SSO Mechanism* to `<Principal Propagation>`.



> ## Note
>
> If user authentication services are not required, use the *Basic Authentication* setting to allow connections to the back-end system to log in as a single, predefined, set of credentials for every user that accesses the connection.

5 SAP Cloud Connector Security

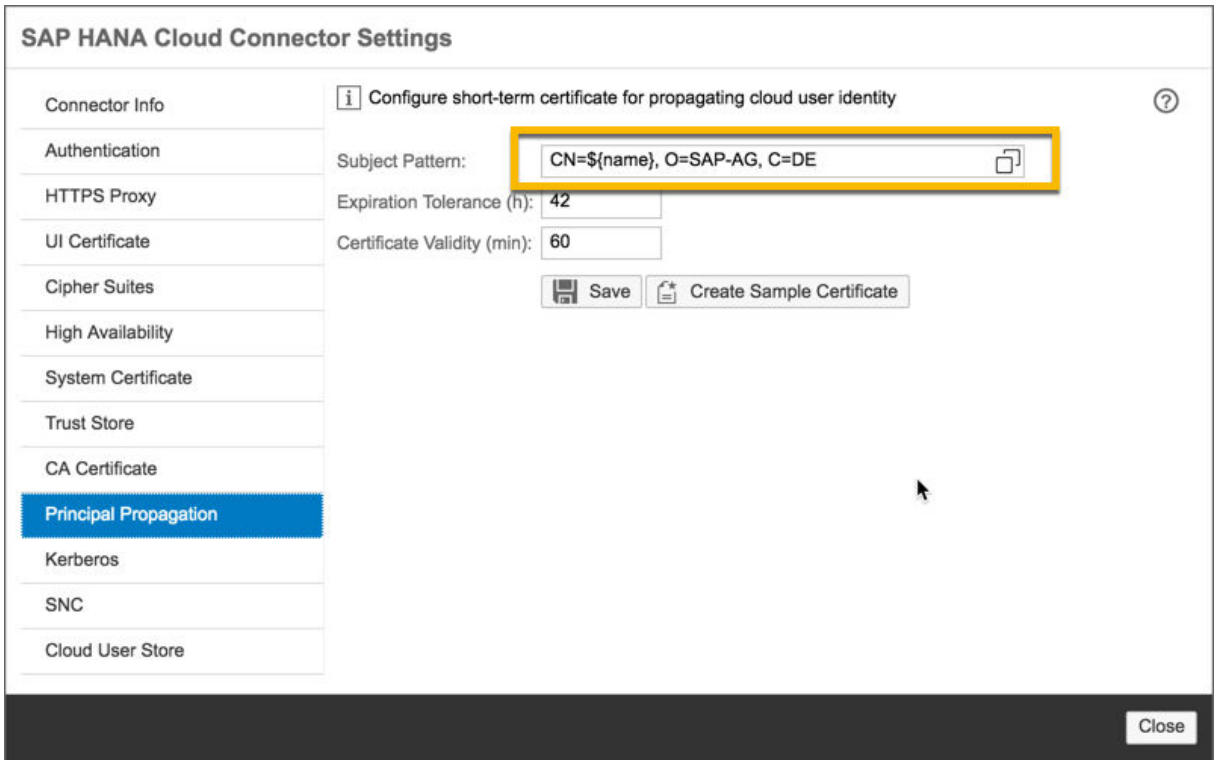
The SAP Cloud Connector allows the SAP Cloud Platform to connect to the SAP S/4HANA on-premise system of the customer.

Configure the principle propagation from the SAP Cloud Connector to the SAP S/4HANA on-premise ABAP system. For more information on SAP Cloud Connector security and how to configure principle propagation to an ABAP system, refer to SAP Cloud Platform Connectivy Service documentation.

Principle Propagation Compatibility

In the context of the SAP Mobile Add-On, the authorization expectation is for the SAP Cloud Connector to pass the cloud user identity through principle propagation in a subject pattern that is matched to a matched alias in the back-end system.

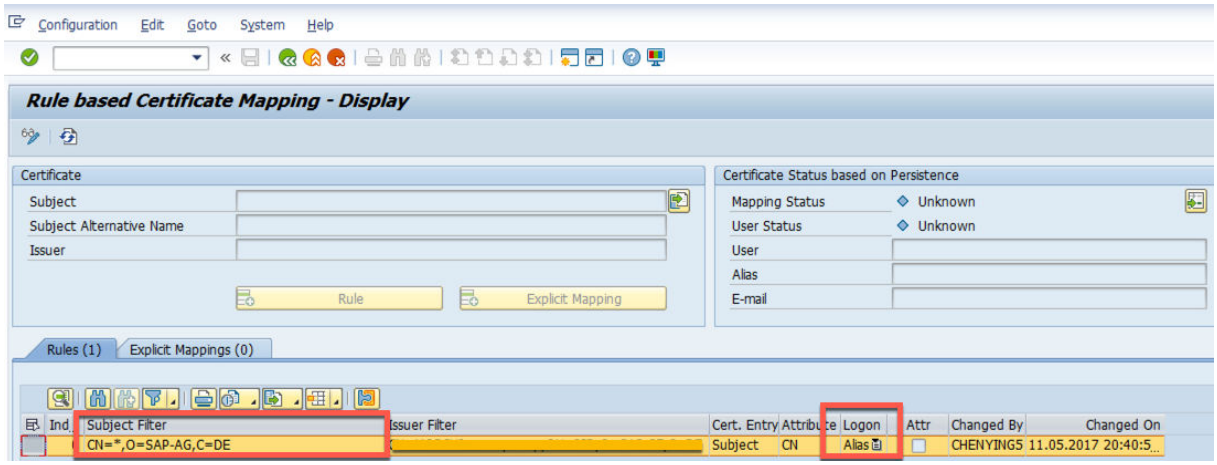
To achieve this expectation, in the *SAP HANA Cloud Connector Settings*, set the `<Subject Pattern>` so it is matched by the SAP S/4HANA on-premise authentication configuration. The matching on-premise configuration is either in a rule-based certificate mapping (through the *CertRule* transaction), or the assignment of external IDs to users (through the *EXTID_DN* transaction).

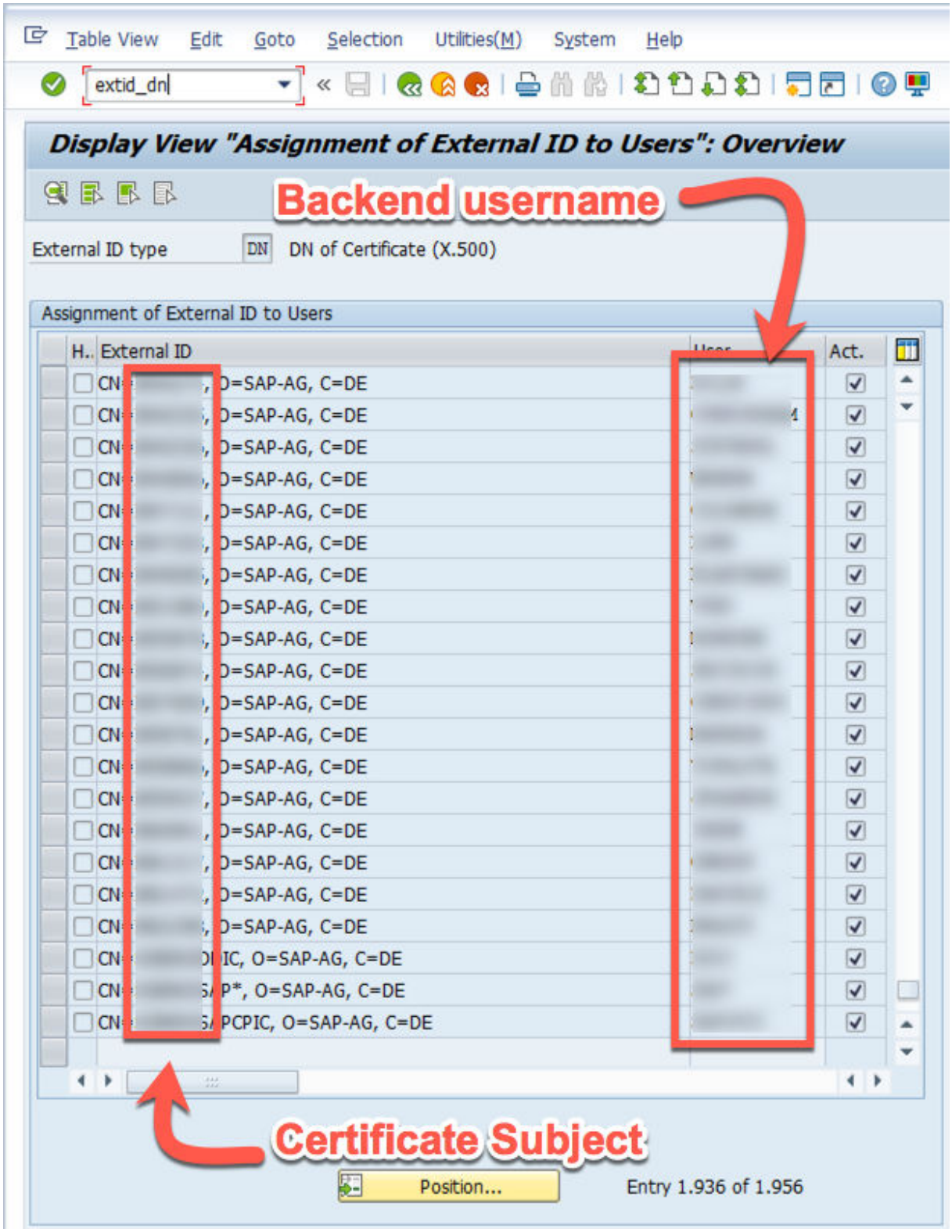


Use the SAP Cloud Connector settings to set a valid subject pattern. After you set the subject pattern, configure the rule based certificate mapping through the *CERTRULE* transaction or by assigning external IDs to

users through the *EXTID_DN* transaction. Configuring the rule based certificate maps the subject pattern that is passed from the SAP Cloud Connector.

Following is a corresponding example of an SAP S/4HANA on-premise that uses the rule based certificate mapping, with the subject filter set to match the pattern of the subject that is passed into the on-premise system from by the SAP Cloud Connector :





Configuring your system in this way allows the back end on-premise system to see requests authenticating through principle propagation to properly filter the subject as the alias for authentication.

> **i Note**
>
> If you set a rule based certificate mapping for a system through the *CERTRULE* transaction, you can no longer manually assign individual external IDs to users through the *EXTID_DN* transaction.

6 Identity and Access Management

For identity and access management, SAP Asset Manager uses functions provided by an identity provider that is either self-hosted or hosted by the SAP Cloud Platform.

User authentication is delegated through one of the following options, depending on your configuration:

- SAP Cloud Platform Identity Authentication
- A customer-chosen different identity provider, configured with the SAP S/4HANA on-premise system

To delegate an OAuth service with an identity provider, see the following topics in the *SAP Cloud Platform* documentation:

- Protecting Applications with OAuth 2.0
- Configuring OAuth Authentication

6.1 User Authentication

The SAP Asset Manager service uses the OAuth 2.0 based authentication and authorization model provided by the SAP Cloud Platform.

The SAP Cloud Platform supports the OAuth 2.0 protocol as a reliable way to protect application resources, whereas SAP Asset Manager uses it to authenticate users. For more information, see Protecting Applications with OAuth 2.0.

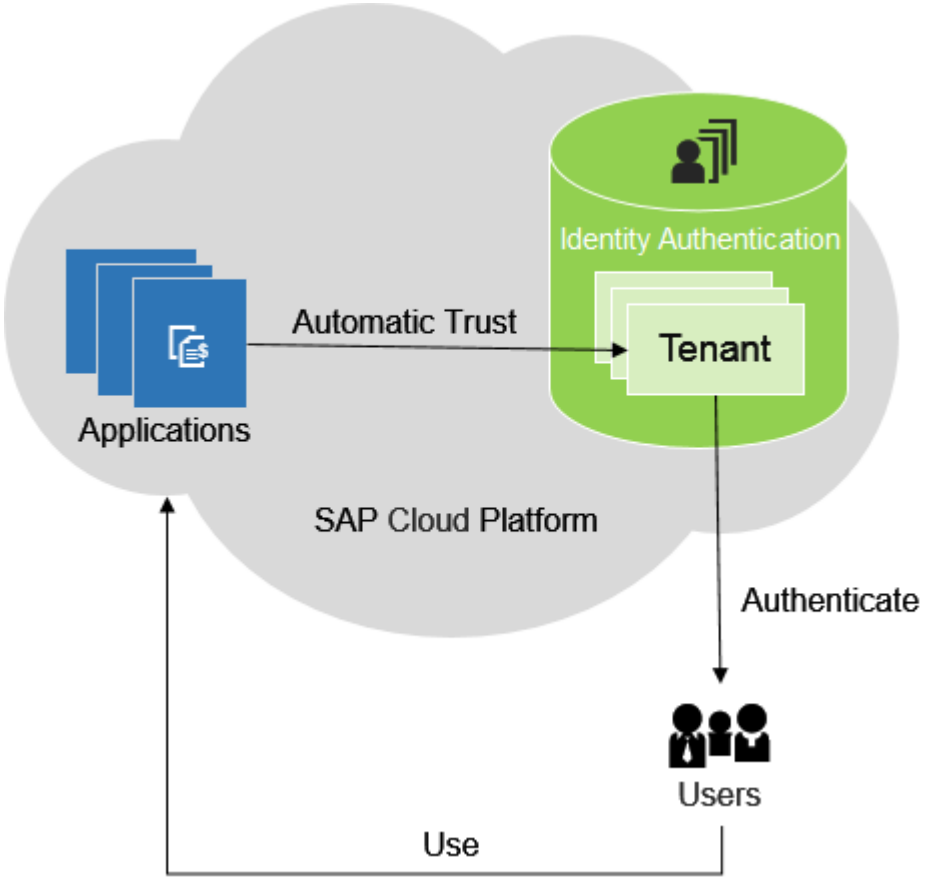
There is only one OAuth scope defined for the SAP Asset Manager service, which you see only on the Provider account. During the onboarding process, when users log in to the application for the first time, the mobile application sends an authorization request to the OAuth server that is running on your SAP Cloud Platform. TheSAP Cloud Platform delegates the call to your SAP Cloud Platform Identity Authentication tenant. Then, on the mobile device, users enter their credentials into a form generated by the SAP Cloud Platform Identity Authentication tenant.

Once the onboarding process is successfully completed, an access token is automatically granted for the users. When SAP Asset Manager accesses service resources, the token (called a bearer token) is used for authentication.

Before authorizing the application to use the service on the SAP Cloud Platform, register the OAuth clients for SAP Asset Manager.

Identity Federation

SAP Cloud Platform supports identity federation with an external identity provider. Use theSAP Cloud Platform Identity Authentication service as an identity provider for our solution, sinceSAP Cloud Platform provides solid integration with the SAP Cloud Platform Identity Authentication service.



Identity Federation with Identity Authentication Tenant

In SAP Asset Manager, user IDs are used to make sure that users can access only those objects they have authorization for. Therefore, the service must be able to identify the caller user ID for each request based on the bearer token. User principal propagation is enabled in the OAuth configuration so that the service can identify the user ID for each request. SAML assertion (including user IDs) is exchanged from SAP Cloud Platform Identity Authentication for an OAuth access token. Using the access token, SAP Asset Manager provides the requested information to the authenticated users.

For more information, see Identity and Access Management.

Granting Access Tokens

Once the onboarding process is successfully completed, an access token and a refresh token are automatically granted for the users by the OAuth server. The OAuth server is the SAP Cloud Platform. The OAuth token is used to request resources from the server. If the token expires, the refresh token is used to request a new OAuth token from the OAuth server. Set the token lifetime and the refresh token lifetime values according to your security policy. For more information, see Configuring OAuth 2.0.

The OAuth token obtained during the onboarding process is encrypted with 256-bit AES encryption using the passcode set up by the user, or a default key if the passcode is deactivated. Uninstalling the app removes the token stored on the mobile device.

Revoking Access Tokens

You can revoke the access token that was provided for a user using the SAP Cloud Cockpit. By revoking access tokens, you can immediately reject access rights the user was previously granted. Users of the applications can also access and revoke their tokens if required. For more information, see Configuring OAuth 2.0.

7 Required and Essential Authorizations

7.1 Mobile User Essential Authorizations

A mobile user running the SAP Asset Manager application, or any other OData based application, must have the essential authentications to call the OData service through the SAP Gateway.

The following table lists the authorization objects required to run the OData service:

Authorization Object	Authorization Attribute	Value
P_ORGIN	INFTY	0105
	SUBTY	0001
P_PERNR	INFTY	0001
	SUBTY	*
	INFTY	0002
	SUBTY	*
	INFTY	0006
	SUBTY	*
	INFTY	0105
	SUBTY	*

For an ERP system Gateway (GW) HUB installation scenario, the following authorization object is required when a user connects from a HUB system to an ERP system:

Authorization Object	Authorization Attribute	Value
S_RFCACL	ACTVT	16
	RFC_CLIENT	<CLIENT SPECIFIC>
	RFC_EQUSER	Y
	RFC_INFO	*
	RFC_SYSID	<SYSTEM SPECIFIC>

Authorization Object	Authorization Attribute	Value
	RFC_TCODE	*
	RC_USER	*

8 Data Protection and Privacy

Describes the specific features and functions that SAP provides to support compliance with data protection legal requirements and data privacy.

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company-, industry-, regional-, or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to additional features that would be required in a particular environment. Make decisions related to data protection on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

> **i** Note
>
> In most cases, compliance with data privacy laws is not a product feature. SAP software supports data privacy by providing security features and specific data protection-relevant functions such as functions for the simplified blocking and deletion of personal data. SAP does not provide legal advice in any form. The definitions and other terms used in this guide are not taken from any given legal source.

Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form justified reason for the processing of **personal data**. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary **business purpose** has ended.
Deletion	Deletion of **personal data** so that the data is no longer usable.
Retention period	The time period during which data must be available.

Term	Definition
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization.

> ⚠ Caution
>
> The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

GeoLocation Data

When the user starts SAP Asset Manager for the first time, and begins work on a maintenance order for an asset, they are asked interactively if they want to allow the application to use geolocation. The geolocation functionality does not collect, store, or use the geolocation data for any reason other than to show the route to the respective assets on the map.

User Consent

SAP Asset Manager does not provide separate consent management, as only work-related data, such as work orders, notifications and readings are created by the app users. This data collection is covered by the employment contract as it is directly related to the daily work of the employees. Before using any device capabilities, such as the camera or photo library, the user is asked for consent by using the mobile capabilities.

Sensitive Person-Related Data

SAP Asset Manager is not designed to store sensitive person-related data. Therefore, there is no logging of sensitive person-related data.

Displaying Person-Related Data

All person-related data for SAP Asset Manager is retrieved to the mobile device based on the user ID of the user. Personal data includes user ID, name, phone number, and e-mail address of the technician or technicians assigned to the work orders and operations. Business partner data such as name, address, phone number, and e-mail is also personal data if the entity is a single-member company.

Change Log for Person-Related Data

HR-based time data, through the use of the Time Sheets module, can be appended to the SAP Asset Manager application.

Person-related data created with SAP Asset Manager is logged and stored on the SAP S/4HANA on-premise system in the customer environment. See the CATS regular/Record Working Time (Web Dynpro) topic for more information.

8.1 Deletion of Person-Related Data

A user cannot delete individual, replicated, person-related, protected data that originates from SAP S/4HANA in SAP Asset Manager.

If the user deletes the SAP Asset Manager application from the mobile device, or performs a reset of the application, performing those actions delete all person-related protected data in their local data store.

SAP Asset Manager may process person-related data that is subject to data protection laws applicable in specific countries as described in SAP Note 1825544: Simplified Deletion and Blocking of Personal Data in SAP Business Suite.

End of Purpose (EoP) Check

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data must be retained for other reasons.
  If an object is deleted by a user or by the synchronization job, it is blocked but still available in the database. Blocking of data prevents the SAP Asset Manager users from displaying and using data that may include person-related data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change blocked data.
- **Create:** It is not possible to create objects connected to a blocked project or work package.
- **Search:** It is not possible to search for blocked data.

Deletion

Work orders, notifications and timesheets for the user are stored on the device. By default, work orders are removed from the device upon completion or re-assignment. Completion is determined by the assignment type configured in the SAP back-end by the customer.

By default, the most recent two weeks time sheet records are stored. Older time sheet records are removed automatically from the mobile client when the user performs a synchronization to the SAP back-end system.

Uninstalling the app follows the standard iOS or Android process, and requires no special handling. When the app is uninstalled, all locally stored data is deleted as well.

8.2 Data Protection Aspects

Provides an overview of data protection aspects involved within the SAP Asset Manager application.

Data Storage Encryption

Application data stored by SAP Asset Manager is encrypted with 256-bit AES encryption using the passcode set up by the user or a default key if the passcode is deactivated.

Data that is stored in the SAP Asset Manager database on the SAP Cloud Platform is also encrypted.

OAuth Token Lifetime

The SAP Asset Manager application uses the OAuth protocol 2.0 to authenticate users, and to get authorization to access data on the SAP Cloud Platform. The OAuth token is obtained during the onboarding process. Register an OAuth client as described in Configuring OAuth 2.0.

During client registration, you can set the lifetime of both the OAuth token and the refresh token. If you do not define the lifetime (leave the fields empty), lifetime tokens are infinite. We recommend to set the lifetime of the tokens according to your security requirements.

GIS Authentication

GIS authentication is proxy-based. Authenticated basemaps and feature layers are requested through a local proxy that manages the generation and use of tokens based on the clientID and client secret which are configured in the proxy. See additional documentation from Esri on configuring such a proxy.

Passcode Protection in the Mobile Application

Users of SAP Asset Manager set a passcode to increase the protection of the application. Although it is not mandatory, we recommend having users set a passcode to increase application security.

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

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

Logging out of the Client

To log completely out of the SAP Asset Manager client, reset the entire application. All user data is reset.

9 Additional Information

For more information about the security concepts of SAP Cloud Platform, see the following documentation:

- Identity Access Management
- Securing Java Applications

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 a 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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

THE BEST RUN SAP