

**ABAP SDK**

**Implementation guide for Managed Identities**

<https://github.com/Microsoft/ABA>[P-SDK-for-Azure](https://github.com/Microsoft/ABAP-SDK-for-Azure)

***Author: Microsoft SAP Team Version: 1.0***

Contents

[What is a Managed Identity? 3](#_Toc90978357)

[Prerequisites 3](#_Toc90978358)

[Managed identity types 3](#_Toc90978359)

[System-assigned 3](#_Toc90978360)

[User-assigned 3](#_Toc90978361)

[How to create Managed Identities 3](#_Toc90978362)

[Create System-assigned Managed Identity(SAMI) 3](#_Toc90978363)

[Create User-assigned Managed Identity(UAMI) 3](#_Toc90978364)

[How to enable Managed identity on an existing VM 5](#_Toc90978365)

[Enable System-assigned Managed Identity 5](#_Toc90978366)

[Enable User-assigned managed identity 6](#_Toc90978367)

[How to assign Managed Identity to an Azure resource ? 6](#_Toc90978368)

[Steps to use Managed Identity from SAP using ABAP SDK for Azure 9](#_Toc90978369)

[Configuration 9](#_Toc90978370)

[ZREST\_CONFIG 9](#_Toc90978371)

[ZREST\_CONF\_MISC 9](#_Toc90978372)

[ZADF\_CONFIG 10](#_Toc90978373)

[ZADF\_MI\_CONFIG 10](#_Toc90978374)

[DEMO Program 11](#_Toc90978375)

[ABAP SDK Monitor 12](#_Toc90978376)

# What is a Managed Identity?

Managed identity is an identity that allows authentication with Azure AD without having to manage any credentials. It eliminates the need of credentials management by providing an identity for the Azure resource in Azure AD to fetch access tokens and thus securing communication between services. Refer to [Managed identities for Azure resources | Microsoft Docs](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview) for more insights.

It overcomes the below common challenges such as:

* Management of secrets and credentials.
* Forgetting to renew their credentials resulting in outages.
* Accidently leaking credentials leading to data leaks.

# Prerequisites

* Make sure you have installed ABAP SDK for Azure in your SAP system. Refer document ‘ABAP SDK for Azure – GitHub’ for more details, Visit <https://github.com/Microsoft/ABAP-SDK-for-Azure>

# Managed identity types

## System-assigned

It has a 1:1 relation with an Azure resource and shares the same life cycle i.e., when you delete the resource, we automatically clean up the identity.

### **User-assigned**

This managed identity is a standalone Azure resource with its own life cycle.

**As t**he lifecycle is not tied to an Azure resource, so once a resource is deleted, this Identity won’t be deleted. You can [enable a user-assigned managed identity](#_User-assigned_managed_identity) and assign it to one or more Azure resources.

# How to create Managed Identities

### Create System-assigned Managed Identity(SAMI)

A System-assigned Managed Identity can be assigned to a single Azure service. Please refer to [enable SAMI on Virtual machine](#_Enable_System-assigned_Managed) section to enable this identity on VM. As System-assigned Managed Identity is directly enabled on Virtual machine, you can [add this SAMI identity to Azure service](#_How_to_assign) by providing the Virtual machine name under Select Identity.

### Create User-assigned Managed Identity(UAMI)

Enabling azure service with a user-assigned identity would require you to create the identity first and then add its resource identifier to your azure service identity management.

1. Sign in to the [Azure portal](https://portal.azure.com/) to create the user-assigned managed identity.
2. In the search box, enter **Managed Identities**. Under **Services**, select **Managed Identities and then select Create**.

Graphical user interface, text, application

Description automatically generated

1. Enter values in the following boxes in the **Create User Assigned Managed Identity** pane:

Graphical user interface, application

Description automatically generated

* + - **Subscription**: Choose the subscription to create the user-assigned managed identity under.
    - **Resource group**: Choose a resource group to create the user-assigned managed identity.
    - **Name**: Enter the name for your user-assigned managed identity.

1. Select **Review + create** to create the Managed identity.
2. Note down the **Client Id of the UAMI** created. This would be required during UAMI entries configuration in SAP tables.

Graphical user interface, application

Description automatically generated

# How to enable Managed identity on an existing VM

### Enable System-assigned Managed Identity

To enable system-assigned managed identity on a VM that was originally provisioned without it, follow below steps:

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Navigate to the desired Virtual Machine and select **Identity**.
3. Under **System assigned**, select **Status as** **On** and then click **Save**:

Graphical user interface, text, application, email

Description automatically generated

### 

### Enable User-assigned managed identity

To enable user-assigned managed identity on a VM that was originally provisioned without it, follow below steps:

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Navigate to the desired VM and click **Identity in the left pane**. Select **User assigned** and then **+Add**

Graphical user interface, text, application, email

Description automatically generated

1. Click the user-assigned identity you want to add to the VM and then click **Add**.

# How to assign Managed Identity to an Azure resource ?

1. Sign in to the [Azure portal](https://portal.azure.com/) under which you have configured the managed identity.
2. Navigate to the desired resource on which you want to modify access control. For e.g., to give an Azure virtual machine access to a storage account, switch to the Storage container menu.
3. In the left pane, click on the **Access control (IAM).**

Graphical user interface, text, application, email

Description automatically generated

1. Go to the **Role Assignments** option and click **Add** to open the Add role assignment page.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

1. Goto your Storage account role assignment Page as shown below. Assign the necessary roles .e.g., storage Blob Data contributor for Azure Blob storage service.

Graphical user interface, text, application, email

Description automatically generated

1. Select **Managed identity** and click **Select members under Members Tab**.

Graphical user interface, text, application

Description automatically generated

1. Grant access to the Managed Identity to connect to Azure Blob storage as mentioned below:

Under select ‘**Managed identities’** choose subscription where MI belongs to, and Managed Identity as shown below.

You can select type as [user-assigned managed identity](#_User-assigned) or [system-assigned managed identity](#_System-assigned).

\*Note: In case of SAMI , choose system assigned Managed identity as MI type and select SAMI corresponding to the virtual machine.

Graphical user interface, application

Description automatically generated

# Steps to use Managed Identity from SAP using ABAP SDK for Azure

## Configuration

ABAP SDK has following main configuration tables which needs to be maintained.

* **ZREST\_CONFIG** : Master Table for Interface ID Maintenance. You must define a new Interface name and keep the destination as blank.
* **ZREST\_CONF\_MISC** : This table stores miscellaneous information for interfaces such as information on alerts and re- processing of failed messages automatically.
* **ZADF\_CONFIG** : This is an Interface extension table which stores data that is more specific to Azure Services like Interface type, SAS keys, base URI, call type and processing Method.
* **ZADF\_MI\_CONFIG** : This table stores the information relevant to establishment of connection with Azure service such as Managed Identity Client Id and the resource.

**Note :** 2 interface IDs need to be maintained in these tables, i.e., 1 interface ID for fetching Managed Identity token and another Interface ID(e.g., Azure Blob Interface Id) for accessing the Azure service using this token.

Maintaining these config tables for MI access token is as shown below:

### ZREST\_CONFIG

1. MI Token Configuration:

Create a new Interface ID such as ‘Z\_MI\_DEMO’ and keep the RFC destination as blank.

**Interface** : MI Interface ID **Destination** – Blank

Graphical user interface, application, Word

Description automatically generated

1. Blob Configuration is as follows:

Graphical user interface, application, Word

Description automatically generated

### 

### ZREST\_CONF\_MISC

1. MI Token Configuration:

Create an entry in table ‘ZREST\_CONF\_MISC’ for the interface Id ‘Z\_MI\_DEMO’ created.

Table configuration:

* METHOD – ‘GET’ to fetch the token
* MAX\_RETRY : Number of retry in case of service failure.
* EMAIL\_ID : Email id to which alerts would be send.
* MAIL\_BODY\_TXT : Text Id to be maintained for the mail content to be sent.
* RETRY\_METHOD : Blank.
* Change Interface ID

Graphical user interface, application, Word

Description automatically generated

1. Blob Configuration is as follows:

Graphical user interface, text, application

Description automatically generated

### ZADF\_CONFIG

1. MI Token Configuration:

Create an entry in table ‘ZADF\_CONFIG’ for the interface Id ‘Z\_MI\_DEMO’ created above.

Table configuration:

* INTERFACE\_TYPE - ‘**Azure Managed Identities**’.
* SAS\_KEY : Blank.
* URI - ‘**http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01**’ to get the token from the Instance Metadata Service.
* SERVICE\_TYPE - Synchronous(S).
* IS\_TRY : Keep reprocessing flag blank.

Note: This field can be utilized in our future release to control the reprocessing based on value of X. Presently it should be enabled as blank.

Graphical user interface, text, application, email

Description automatically generated

1. Blob Configuration is as follows:

### Graphical user interface, text, application, email Description automatically generated

### ZADF\_MI\_CONFIG

Create an entry in table ‘ZADF\_MI\_CONFIG’ for the above interface Id ‘Z\_MI\_DEMO’.

Table Configuration:

* **Interface** : MI Interface ID
* **Client ID :** Provide client Id of the user-assigned Managed Identity created in the VM. Refer section for the [client id](#_Create_User-assigned_Managed).
* **Resource Id** : Maintain resource url for which needs to be accessed e.g., https://storage.azure.com/ to connect to Azure storage service.
* **MI Name** : Provide service line specific name representing the UAMI configuration.

Graphical user interface, application

Description automatically generated

# DEMO Program

Please refer to DEMO program ‘**ZADF\_DEMO\_AZURE\_MI**’ in SMT system for fetching access token and establishing connection with Azure Blob service. Code level usage overview is as below:

* Call factory method of the ‘ZCL\_ADF\_SERVICE\_FATORY’ to create an instance of ZCL\_ADF\_SERVICE\_AAD.
* Now, leverage method ‘**GET\_AAD\_TOKEN\_MSI**’ of this ‘ZCL\_ADF\_SERVICE\_AAD’ instance to generate MI token for authentication.
* Usage of the method ‘ADD\_EXPIRY\_TIME’ of class ‘ZCL\_ADF\_SERVICE\_BLOB’ is no longer needed for Azure Blob service.
* Pass the header attribute as ‘**Authorization**’ with the above MI token to the call the Azure service.

Text

Description automatically generated

# ABAP SDK Monitor

You can leverage the Interface Monitor (Transaction ZREST\_UTIL) provided to monitor history of all the messages posted to Azure Services. You can view the statuses of the messages as well in this monitor in case of scheduled background jobs.

Go to transaction ZREST\_UTIL and provide your Interface ID in the selection screen and execute to view all the corresponding messages.

Application

Description automatically generated with medium confidence

In this monitor, you can view the status of the HTTPs message and its headers, response, payload and so on.