

# Enhance the Digital Workplace Experience using SAP Work Zone - Setup and configure SAP Work Zone

Last Updated by Muralidaran Shanmugham

This blog series will cover some of the key concepts of SAP Work Zone and will also help you familiarize with the steps required to setup SAP Work Zone and integrate it with UI Cards and applications.

Enhance the Digital Workplace Experience using SAP Work Zone
<a href="#">Part 1 - Setup and configure SAP Work Zone</a>
<a href="#">Part 2 - SAP Work Zone Overview and Components</a>
<a href="#">Part 3 - Developing SAP UI Cards that render SAP business data within SAP Work Zone</a>
<a href="#">Part 4 - Developing SAP UI Cards that render data from 3rd party systems within SAP Work Zone</a>
<a href="#">Part 5 - Integrating Fiori Apps in SAP Work Zone</a>
<a href="#">Part 6 - Integrating SAP Conversational AI based chatbots with SAP Work Zone</a>

This blog post will guide you through the steps to setup your own SAP Work Zone tenant. Unlike other services on SAP Cloud Platform which can be enabled with a click of a button, Work Zone requires few steps to be performed - though majority of the steps have been automated using boosters (which I will explain below). Remember that Work Zone is a collection of different services like Launchpad/SAP Jam/Workflow etc and hence its absolutely required to have an Identity Authentication Service (IAS) and Identity Provisioning Service (IPS) to ensure all these services can work internally in a seamless fashion.

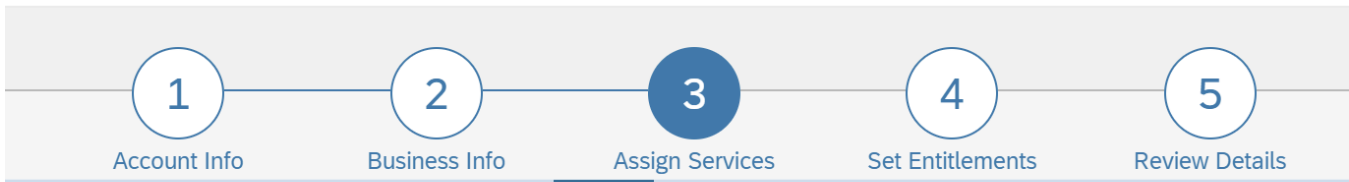
The steps which I am going to show assume that you are looking to setup a fresh SAP Work Zone tenant without the need to migrate an existing SAP Jam tenant. The [SAP Help documentation](#) clearly outlines the steps and [please refer to this documentation for updates](#) (as this blog post could be outdated and I wouldn't be necessarily updating it). The Help documentation has been updated to show the IPS source + target system transformation setups to be used which for instance take care of automatic assignment of administrator permissions.

## Pre-requisites:

- Access to SAP Cloud Platform Account:

Use [SAP Control Center](#) to provision SAP Cloud Platform with required entitlements.

## Edit Global Account | Live





☐ Services ☒ Applications ☐ Environments

☐ Show selected (27)

SAP Work Zone

### Extension Suite - Digital Experience

<input checked="" type="checkbox"/>	 SAP Work Zone	Cloud Foundry
<input type="checkbox"/>	 SAP Work Zone for HR	Cloud Foundry

- Access to Cloud Identity Services:

Cloud Identity Services provides access to IAS and IPS. Create a request for a tenant using the [SCI Tenant Registration app](#). Ensure you select Landscape as “QA” and Tenant Type as “Test”. At the time of writing this blog post, this was a requirement to enable IPS also in the same IAM tenant.

Once your IAS is provisioned, you will get an email to activate the account. Next, you need to raise an [Internal Incident](#) to enable IPS on this IAM tenant. (Component BC-IAM-IPS)

To access IAS, you would use the below URL:

URL pattern: [https://<tenant\\_id>.accounts400.ondemand.com/admin](https://<tenant_id>.accounts400.ondemand.com/admin)

To access IPS, you would use the below URL:

URL pattern: [https://<tenant\\_id>.accounts400.ondemand.com/ips](https://<tenant_id>.accounts400.ondemand.com/ips)

Within your IAS > Administrators menu, ensure your admin user has the below authorizations. This grants the IPS\_Admin role to the admin to make configurations in IPS.

More details on [SAP Help documentation](#).

The screenshot shows the SAP Identity Authentication Service (Europe) interface. The top header includes the SAP logo, the text "Identity Authentication Service [Europe]", and the user "agash3ej4". The left sidebar contains navigation icons and a list of administrators: Murali Shanmugham, SAP Cockpit, and WZ\_ADMIN. The main content area displays the profile of Murali Shanmugham, including User ID: P000000 and E-Mail: murali.shanmugham@sap.com. Below the profile, there is a section titled "Configure Authorizations" with several toggle switches: Manage Applications (ON), Manage Corporate Identity Providers (ON), Manage Users (ON), Read Users (OFF), Manage Groups (ON), Manage Tenant Configuration (ON), and Manage Identity Provisioning (ON, highlighted with a yellow box). The "Manage Identity Provisioning" toggle is currently turned ON, and its description is "Authorizations to configure identity provisioning".

Note: Ensure that all the Work Zone users which you have created in IAS are created of type "**employee**".

## Configure trust between SAP Cloud Platform and IAS

Using the Control Center, I was able to provision a SAP Cloud Platform account. As you can see below, it has the entitlements for SAP Work Zone and few other services like Business Application Studio etc.

The screenshot shows the SAP Cloud Platform Cockpit interface. The top header includes the SAP logo, the text "SAP Cloud Platform Cockpit", and the user "Murali". The left sidebar contains navigation icons and a list of services: Overview, Services, Subscriptions, Cloud Foundry, HTML5 Applications, Connectivity, Destinations, Cloud Connectors, Security, Administrators, Users, Role Collections, Roles, Trust Configuration, Entitlements, and Usage Analytics. The main content area displays the "Subaccount: Work Zone - Subscriptions" section, showing a list of 18 subscriptions. The subscriptions are organized into two categories: "Extension Suite - Development Efficiency" and "Extension Suite - Digital Experience". Each category contains several service tiles, each with a "Not Subscribed" status and a "Go to Application" link. The services include Audit Log Viewer, Extension Center, SAP Business Application Studio, Service Management, Transport Management, Document Management, Launchpad, Portal, SAP Work Zone, and Web Analytics. The "SAP Work Zone" tile is highlighted with a yellow box.

In the trust configuration, download the "SAML Metadata". This is required to setup the trust with IAS in the next step.

**SAP Cloud Platform Cockpit**

Home [Australia (Sydney)] / ANZ Team / Work Zone

Overview

Services

Subscriptions

Cloud Foundry

HTML5 Applications

Connectivity

Security

Administrators

Users

Role Collections

Roles

Trust Configuration

Entitlements

Usage Analytics

### Subaccount: Work Zone - Trust Configuration

All: 1

**Establish Trust** Manual Setup: **New Trust Configuration** **SAML Metadata**

Status	Name	Description
Default		
Active	SAP ID Service	Default identity provider

Learn more about how to [configure trust](#) at

Navigate your IAS > Applications and create a new application. I have used the name “WZ SCP Account”. In the Trust settings for this new applications, navigate toe “SAML 2.0 Configuration”

**SAP Identity Authentication Service [Europe]** agash3ej4 Murali Shanmugham

Home

Users & Authorizations

Applications & Resources

Applications

Tenant Settings

Terms of Use Documents

Privacy Policy Documents

E-Mail Template Sets

Password Policies

Custom CSS

Tenant Texts

Identity Providers

Monitoring & Reporting

Applications

Search

Custom Applications

WZ SCP Account

System Applications

Administration Console  
oac.accounts.sap.com

User Profile  
sp.accounts.sap.com

### WZ SCP Account

This application name appears on the login and registration pages.

[Home URL](#) Home URL not configured

Trust Authentication and Access Branding and Layout

Single Sign-On

Type  
Choose SAML 2.0 or OpenID Connect. SAML 2.0

**SAML 2.0 Configuration**  
Configure trust with a service provider by uploading metadata for web-based authentication. Not Configured

**Subject Name Identifier**  
Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 authentication requests to Identity Provider. User ID

**Default Name ID Format**  
Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider. Unspecified

Upload the metadata file which you had downloaded earlier from SAP Cloud Platform subaccount and save your changes.



## Define from Metadata

Configure trust with a service provider by uploading metadata for web-based authentication.

Metadata File:

[Browse...](#)

## Configure Manually

\*Name:

## Assertion Consumer Service Endpoint

The URLs of the service provider assertion consumer service endpoint that receives responses from Identity Authentication service.

[+ Add URL](#)

Default	URL	Index	
<input checked="" type="radio"/>	<input type="text" value="https://wz.authentication.ap10.hana.ondemand.com/saml/SSO/alias/wz.cf-ap10"/>	<input type="text" value="0"/>	

## Single Logout Endpoint

The URLs of the service provider single logout endpoints that receive logout messages.  
The SOAP Endpoint is called only when the user password is changed.

[Save](#)

[Cancel](#)

In the SAML Assertion attributes, add a new attribute called “Groups”. Ensure that it starts with an uppercase.



## Attributes

You can change the default names of the assertion attributes that the application uses to recognize the user attributes. You can use multiple assertion attributes for the same user attribute.

[+ Add](#)

User Attribute	Assertion Attribute	
Groups	<input type="text" value="Groups"/>	
First Name	<input type="text" value="first_name"/>	
Last Name	<input type="text" value="last_name"/>	
E-Mail	<input type="text" value="mail"/>	
User UUID	<input type="text" value="user_uuid"/>	

Similarly, in the Default attributes section, add the Group attribute with the value “Workzone\_User\_Type\_\${type}”.



## Attributes

Set the names and the fixed values of the default attributes included in the assertion.

[+ Add](#)

Attribute	Value	
<input type="text" value="Groups"/>	<input type="text" value="Workzone_User_Type_\${type}"/>	

This completes the setup of the new application in IAS. Navigate to the User Groups menu and add the below Work Zone groups. Users will be assigned to the respective groups to control the level of access within Work Zone.

Identity Authentication Service [Europe]

Home
Users & Authorizations

User Management

User Groups
Administrators
Import Users
Export Users
User Provisioning

Applications & Resources
Identity Providers
Monitoring & Reporting

Groups

Search

Workzone Admin  
Workzone\_Admin

Workzone Area Admin  
Workzone\_Area\_Admin

Workzone End User  
Workzone\_End\_User

Workzone Page Content Ad...  
Workzone\_Page\_Content\_Admin

Workzone Support Admin  
Workzone\_Support\_Admin

Workzone User Type public  
Workzone\_User\_Type\_public

Assign the Workzone\_Admin role to your user in the User Management.

The next task is to setup the trust on the SAP Cloud Platform side. To obtain the metadata file from IAS, navigate to Tenant Settings > SAML 2.0 configurations to download the metadata file.

Identity Authentication Service [Europe]
agash3ej4

Home
Users & Authorizations
Applications & Resources

Applications

Tenant Settings
Terms of Use Documents
Privacy Policy Documents
E-Mail Template Sets
Password Policies
Custom CSS
Tenant Texts

Identity Providers

Tenant Settings

Risk-Based Authentication

Corporate User Store

SPNEGO

SAML 2.0 Configuration
View and download tenant SAML 2.0 configuration.

OpenID Connect Configuration

Switch you your SAP Cloud Platform Trust Configuration. Notice that by default it has the SAP ID servie which will enable users to access the applications using S/P/I/C user IDs. Click on the “New Trust

Configuration" button.

Overview

Services

Subscriptions

Cloud Foundry

HTML5 Applications

Connectivity

Security

Trust Configuration

Entitlements

Usage Analytics

Home [Australia (Sydney)] / ANZ Team / Work Zone

Subaccount: Work Zone - Trust Configuration

All: 1

Establish Trust

Manual Setup:

New Trust Configuration

SAML Metadata

Status	Name	Description
Active	SAP ID Service	Default identity provider

Learn more about how to [configure](#)

Upload the metadata file which you downloaded earlier from IAS. Provide a meaningful name and description and save your changes.

#### New Trust Configuration

Metadata:\*

metadata (4).xml

Upload

<?xml version="1.0" encoding="utf-8"?><ns3:EntityDescriptor xmlns:ns3="urn:oasis:names:tc:SAML:2.0:metadata" xmlns="http://www.w3.org/2000/09/xmldsig#" xmlns:ns2="http://www.w3.org/2001/04/xmllenc#" xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion" ID="S7d92a2e8-4076-4695-804b-d4466efe9f77" entityID="https://agash3ej4.accounts400.ondemand.com"><Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference URI="#S7d92a2e8-4076-4695-804b-d4466efe9f77"><Transforms><Transform

Name:\*

IAS

Description:

IAS IdP

Origin Key:\*

httpsagash3ej4.accounts400.ondemand.

Status:

Active

Available for User Logon:

☒

Link Text for User Logon:

Create Shadow Users During Logon:

☒

Show Details

Parse

Save

Cancel

Its important to turn off the SAP ID service once you have configured trust with IAS and activated it. Use the Pencil icon to edit the settings.

Establish Trust

Manual Setup: 

New Trust Configuration

SAML Metadata

Search

Status	Name	Description	Origin Key	Available for User Logon	Actions
Default					
Inactive	SAP ID Service	Default identity provider	sap.default	<input checked="" type="checkbox"/>	<div><div></div><div></div></div>
Custom					
Active	IAS	IAS IdP	httpsagash3ej4.account.s400.ondemand.	<input checked="" type="checkbox"/>	<div><div></div><div></div></div>

## Setup of Work Zone using Boosters

Boosters are one of the cool features of SAP Cloud Platform which helps our customers to get started with different use cases like Workflows, Mobile Cards, AI Business services etc. Good to see a booster also available for Work Zone. Look for it in the Global Account level.

SAP Cloud Platform Cockpit

Overview

Subaccounts

Resource Providers

Boosters

System Landscape

Entitlements

Members


Home [Australia (Sydney)] / ANZ Team

Boosters

Follow our interactive guided boosters to **build** applications or use different platform services and features.

work  All

Extension Suite - Digital Experience (1)



Get Started with SAP Work Zone

Configure subaccount settings, subscribe to SAP Work Zone, and assign roles.

Start

Just follow up the prompts provided by the wizard. In this case, it asks the details of the subaccount which you have already prepared (using the above instructions)

Get Started with SAP Work Zone

1 Check Prerequisites

2 Configure Subaccount

3 Review

Configure Subaccount

Select a Cloud Foundry subaccount and space. You can also enter the space name to create a new one. [i](#)

Subaccount:\* Work Zone

Select the subaccount for this booster.

Org:\* academy

View the organization name.

Space:\* dev

Create a new space or select an existing space.

The booster will automatically create the relevant artefacts like destinations, role collections etc and save us from manually performing those configurations.



Progress	
Assigning Service Quotas	DONE
Creating Space	DONE
Creating Service Instances	DONE
Creating Destination	DONE
Subscribing to SaaS Applications	PROCESSING
Creating Role Collection	PENDING
Mapping User Group to Role Collection	PENDING

At the end, you will get a popup with a success message. From here, you can navigate directly to the Work Zone application.

Success

Booster executed successfully

Your subaccount is ready for SAP Work Zone.

[Navigate to Subaccount](#)

Start developing in SAP Work Zone.

[Go to the provisioning application](#)

Close

## SAP Work Zone Configurator:

The configurations are not done yet. We still have few more things to do before we could use start using Work Zone.

Work Zone leverages SAP Jam for the collaboration aspects. As most of you might know, it has its own user management. Hence, we need to setup trust with IAS again and also configure IPS to provision users (from IAS to Work Zone)

When you try to access the Work Zone application from the previous step, it would take you to the Work Zone Configurator. It has the below URL Pattern

[https://\[subaccount\\_specific\].dt.workzone.cfapps.sap.hana.ondemand.com/sites#Workzone-Config](https://[subaccount_specific].dt.workzone.cfapps.sap.hana.ondemand.com/sites#Workzone-Config)

There are few steps which have been automated here and many still need to be done manually. The SAP Help documentation was clear in most of the places.

Work Zone Manager - Work Zone Configurator

Work Zone Directory

Content Manager

Provider Manager

Work Zone Configurator

### Work Zone Configurator

The process of setting up SAP Cloud Platform Work Zone consists of these 3 steps: Prerequisites, a Booster, and the Configurator. For more information, see [Onboarding to SAP Cloud Platform Work Zone](#).

Before starting the configurator, please confirm that you have completed the following steps:

- ☒ Prerequisites (configure IAS and trust)
- ☒ Work Zone Booster (run the booster in SAP Cloud Platform cockpit to automatically configure settings).

Now select the configuration option that is applicable to you:

☒ I want to create a new Work Zone.

☐ I want to create a Work Zone based on my existing SAP Jam tenant.

Next

Trigger the wizard by selecting the relevant options. In the “Set Up Environment”, you will need to copy paste the IdP trust token as shown below.

Work Zone Manager - Work Zone Configurator

### Create a New Work Zone

1 Set Up Environment — 2 Configure IAS and IPS — 3 Launch

#### 1. Set Up Environment

In this step, a series of configuration steps takes place in your subaccount to allow connectivity and authentication of different components in SAP Cloud Platform Work Zone.

Download the IDP trust from the SAP Cloud Platform Destinations screen and paste it here.

```
Mi00YWFmLWI4MTMTNjhhYzU1MGQ0MDk4MQwwCgYDVQKQDANTQVAXJTAjBgNVBAsM
HENQIERlc3RpbmF0aW9uIENvbmZpZ3VyYXRpb24wHhcNMjAxMjE0MTkzMzQxWhcN
MjIxMjE0MTkzMzQxWjCBgjlMEkGA1UEAwxCY2ZhcHBzLmFwMTAuaGFuYS5vbmRI
bWFuZC5jb20vNmY1YjVhZjgtMTBkMi00YWFmLWI4MTMTNjhhYzU1MGQ0MDk4MQww
CgYDVQKQDANTQVAXJTAiBgNVBAsMHENQIERlc3RpbmF0aW9uIENvbmZpZ3VyYXRb
```

This can be obtained from the destination menu within the subaccount. Click on “Download Trust”. While copying the token, ignore the header and footer.

**SAP Cloud Platform Cockpit**

Home [Australia (Sydney)] / ANZ Team / Work Zone

Overview Services Subscriptions Cloud Foundry HTML5 Applications Connectivity **Destinations** Cloud Connectors Security Administrators

Subaccount: Work Zone - Destinations  
All: 1

New Destination Import Destination Certificates **Download Trust** Renew Trust

Type	Name	Basic Properties
HTTP	workflow_dest	Authentication ProxyType URL

The next steps is to configure trust with IAS and setup IPS for provisioning users. Download the metadata which is provided here. Make a note of the SAP Jam URL and OAuth Client Key/Secrets.

**Work Zone Manager - Work Zone Configurator**

Create a New Work Zone

1 Set Up Environment 2 **Configure IAS and IPS** 3 Launch

### 2. Configure IAS and IPS

In this step, you'll need to manually configure IAS and IPS to enable user authentication and user provisioning. Follow the instructions for each step in the documentation. When you're done, check the boxes. For more information, see [Onboarding to SAP Cloud Platform Work Zone](#).

- ☒ Create an app in IAS using the metadata that you download here.
 

Download Metadata
- ☒ Set IAS as a source system.
- ☒ Set SAP Jam as a target system using the following parameters.
 

Note that SAP Jam is the collaborative component of SAP Cloud Platform Work Zone.

OAuth Client Key: [081A43F9F8F85B6E](#)

OAuth Client Secret: [tHEW5T5NCHf4F0HMEUGT5XKJBBWVQdPP4p](#)

SAP Jam URL: <https://tbivkqia0dw2pajwtgzh05.core10.workzone.ondemand.com>

Token Service URL: <https://tbivkqia0dw2pajwtgzh05.core10.workzone.ondemand.com/api/v1/auth/token>
- ☒ Configure and run the provisioning job.

Switch back to IAS > Applications and create a new application. I have given the name “SAP Jam”. Similar to the previous application configuration, navigate to the SAML 2.0 configuration in the Trust settings and import the metadata file which you downloaded in the previous step.

**SAP Identity Authentication Service [Europe]** agash3ej4 Murali Shanmugham

Home Users & Authorizations Applications & Resources **Applications** Tenant Settings Terms of Use Documents Privacy Policy Documents E-Mail Template Sets Password Policies Custom CSS Tenant Texts Identity Providers Monitoring & Reporting

Search

Custom Applications

**SAP JAM**

WZ SCP Account <https://wz.authentication.ap10.hana.on...>

System Applications

Administration Console <oac.accounts.sap.com>

User Profile <sp.accounts.sap.com>

### SAP JAM

This application name appears on the logon and registration pages.

[Home URL](#) Home URL not configured

Trust Authentication and Access Branding and Layout

Single Sign-On

Type Choose SAML 2.0 or OpenID Connect. SAML 2.0

**SAML 2.0 Configuration** Configure trust with a service provider by uploading metadata for web-based authentication. Not Configured

Subject Name Identifier Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 User ID

Set the Subject Name Identifier to User UUID as shown below.

Applications

Search

Custom Applications

SAP JAM  
https://tbivkqia0dw2pajwtgzho5.core10....

WZ SCP Account  
https://wz.authentication.ap10.hana.on...

Subject Name Identifier

User UUID, User ID, and Login Name are unique for the tenant.

Basic Configuration

Set a basic attribute from the list below.  
When Identity Authentication acts as proxy IdP, and the users have no profile in Identity Authentication, choose the advanced configuration option.

Select a basic attribute: User UUID

Add the user attribute “Groups”

Applications

Search

Custom Applications

SAP JAM  
https://tbivkqia0dw2pajwtgzho5.core10....

WZ SCP Account  
https://wz.authentication.ap10.hana.on...

System Applications

Administration Console  
oac.accounts.sap.com

User Profile  
sp.accounts.sap.com

SAML Assertion Attributes

Attributes

You can change the default names of the assertion attributes that the application uses to recognize the user attributes for the same user attribute.

+ Add

User Attribute	Assertion Attribute
Groups	Groups
First Name	first_name
Last Name	last_name
E-Mail	mail
User UUID	user_uuid

Set the default attribute Groups with the value Workzone\_User\_Type\_\${type}

Applications

Search

Custom Applications

SAP JAM  
https://tbivkqia0dw2pajwtgzho5.core10....

WZ SCP Account  
https://wz.authentication.ap10.hana.on...

Default Attributes

Attributes

Set the names and the fixed values of the default attributes included in the assertion.

+ Add

Attribute	Value
Groups	Workzone_User_Type_\${type}

We need to create a technical user to communicate between IAS and IPS. Navigate to IAS > Administrators and create a user of type “System”. Provide a BASIC Authentication and make a note of the User ID and password.

The screenshot shows the 'System Details' page for 'WZ\_ADMIN' in the SAP Identity Provisioning System. The left sidebar lists administrators: Murali Shanmugham, SAP Cockpit, and WZ\_ADMIN (highlighted). The main content area shows configuration options for 'WZ\_ADMIN':

- Configure System Authentication:**
  - Certificate:** Not Configured (link to configure).
  - Set Password:** Set password for system authentication. (Value: 2c21c8c9-2ec5-4081-a2f5-864756f01404)
- Configure Authorizations:**
  - Manage Applications:** ON (Authorizations to configure applications)
  - Manage Corporate Identity Providers:** ON (Authorizations to configure corporate identity providers)
  - Manage Users:** ON (Authorizations to manage, export, and import users)
  - Read Users:** ON (Authorizations to read and export users)

Launch the IPS service to configure the Source and Target systems.

Remember the URL pattern to launch IPS: [https://<tenant\\_id>.accounts400.ondemand.com/ips](https://<tenant_id>.accounts400.ondemand.com/ips)

In the Source Systems, create an entry for Identity Authentication. Populate the properties as provided in this [Help page](#). I didn't bother using any of the optional properties. When adding the properties for passwords – use the credential option.

The screenshot shows the 'Source Systems' page in the SAP Identity Provisioning System. The left sidebar lists navigation options: Home, Source Systems (highlighted), Target Systems, Proxy Systems, Job Logs, and Authorizations. The main content area shows the details for the source system 'agash3ej4' (IAS Tenant for WZ, Enabled):

- Type:** Identity Authentication
- System Name:** agash3ej4
- Destination Name:** (empty)
- Description:** IAS Tenant for WZ

In the Target Systems, create an entry for **"SAP Work Zone"**. Maintain the properties for this target system as per this onboarding [Help page](#). After saving your Source and Target systems, its time up update the transformations within each of them. Refer to the same onboarding Help page to copy the snippets to source and target systems. Please note that the below screenshot is outdated and you need to select SAP Work Zone as the target system

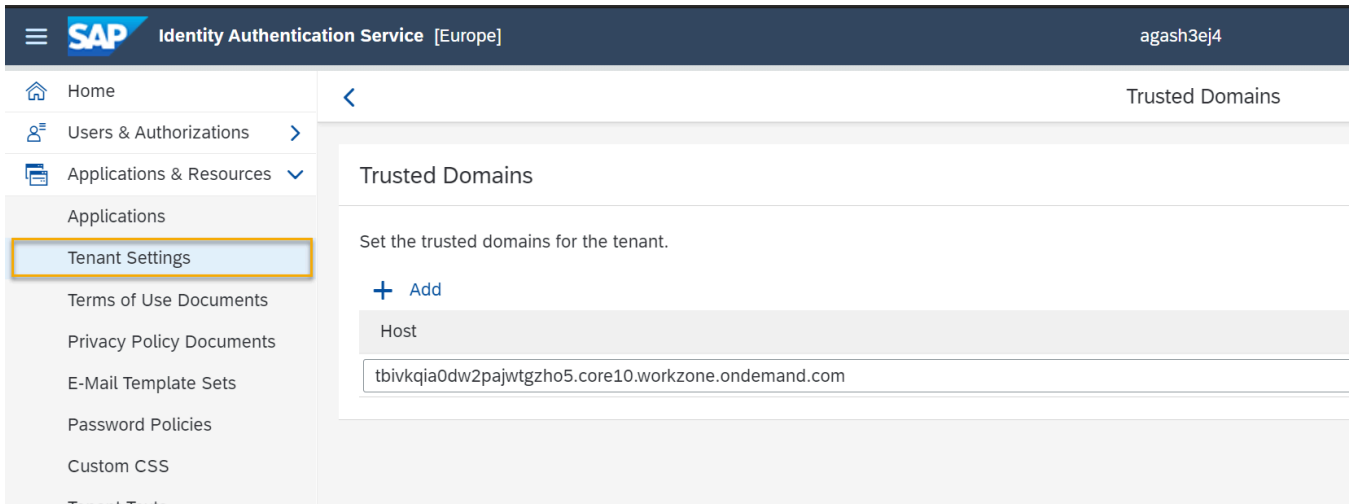
The screenshot shows the SAP Identity Provisioning console. On the left is a navigation menu with options: Home, Source Systems, Target Systems (highlighted with an orange box), Proxy Systems, Job Logs, and Authorizations. The main area is titled 'Target Systems' and lists a system named 'JAM\_FOR\_WZ' with the description 'SAP Jam Tenant for Work Zone' and a status 'Enabl...'. To the right, the 'Target System Details' panel shows 'JAM\_FOR\_WZ' with the type 'SAP Jam Collaboration'. Below this are three tabs: 'Details' (selected), 'Transformati...', and 'Properties'. The 'Details' tab contains a form with the following fields: Type (SAP Jam Collaboration), System Name (JAM\_FOR\_WZ), Destination Name (empty), Description (SAP Jam Tenant for Work Zone), and Source Systems (agash3ej4). This entire details panel is highlighted with an orange rounded rectangle.

This completes the setup of IPS. To trigger replication of users into Work Zone with their respective role assignments, trigger the job from the source system. Click on “Run Now” form the Read Job. You should be able to see in the job logs the users and groups read and written to Work Zone.

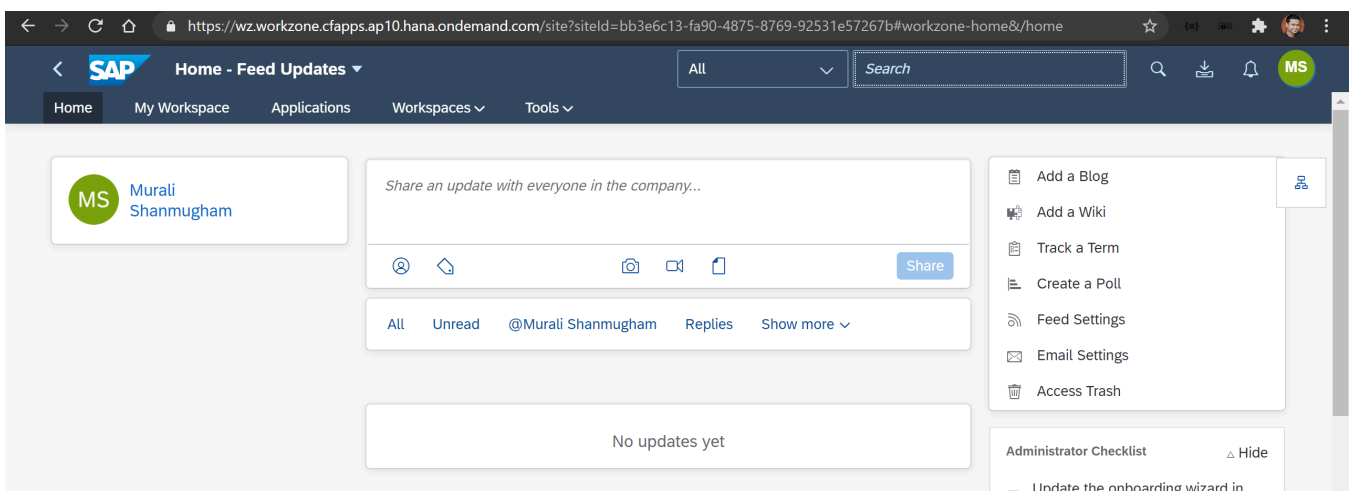
The screenshot shows the SAP Identity Provisioning console with the 'Source Systems' tab selected in the left navigation menu. The main area displays 'Source System Details' for 'agash3ej4', which is an 'Identity Authentication' system. Below the system name are four tabs: 'Details', 'Transformati...', 'Properties', and 'Jobs' (highlighted with an orange circle). The 'Jobs' tab shows a table with two rows of job types and their corresponding actions. The first row is 'Read Job' with actions 'Run Now', 'Schedule', and 'Resume'. The second row is 'Resync Job' with the action 'Run Now'. This table area is highlighted with an orange rounded rectangle.

Job Type	Actions
Read Job	Run Now Schedule Resume
Resync Job	Run Now

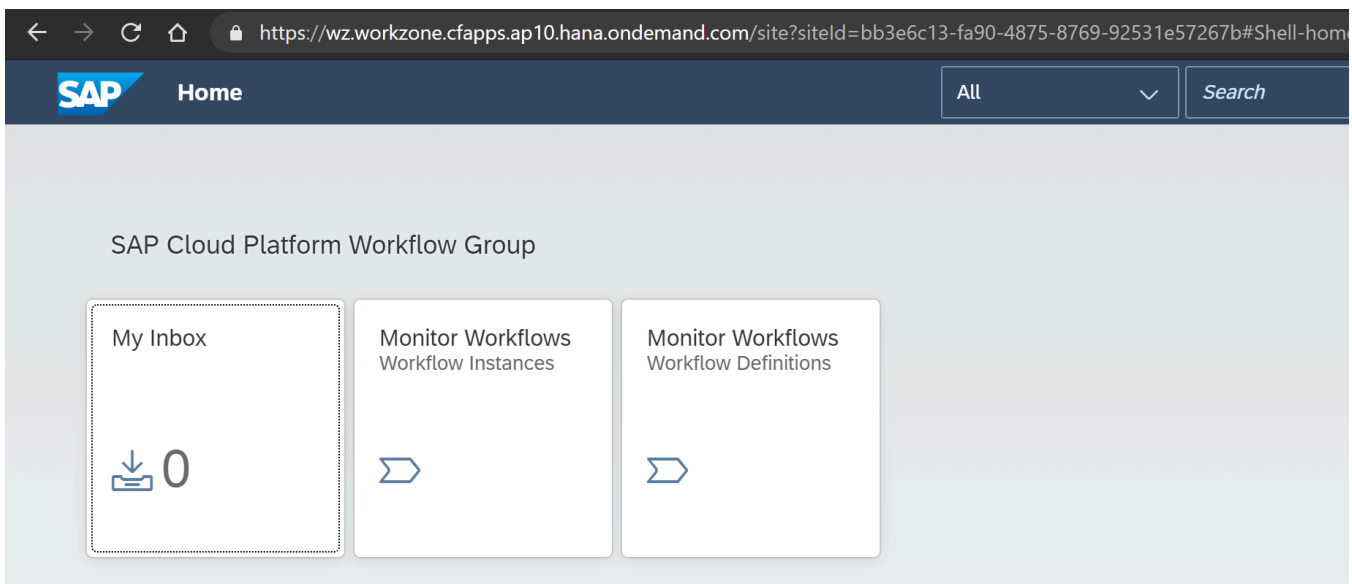
Before testing your access in Work Zone, ensure you add the SAP JAM URL in the trusted domain of IAS. This is enable Work Zone to embed SAP Jam contents (within iFrames/overlays)



You should be now able to login to Work Zone using the IAS credentials and explore the capabilities.



The Fiori Launchpad will also be available in the Applications menu.



The users created in IAS will be replicated and visible within Work Zone (Administration Console) as shown below. Since I have assigned myself to Work Zone Admin role in IAS, it maps to the Company Administrator role within Work Zone.

<

SAP

Members

HomeMy WorkspaceApplicationsWorkspacesTools

AllSearch

MS

Administration Console

Change Admin Area:

Company

Overview

General Settings

Users

Members

Member Lists

Members

csv export of all users in the system can be obtained using the [User Detail](#) Admin report.

[Manage users using external IDM](#)

People Search

Search Users

Show: 

Active

Email	First name	Last name	Status	Admin Type	
murali.shanmugham@sap.com	Murali	Shanmugham	Active	Company Administrator	Action

Stay tuned for more blog posts on how to configure SAP Work Zone with UI Cards and Workflow applications.

PS: To demonstrate SAP Work Zone to customers/partners, please use the demo [16520](#).

### Other related blog posts:

[SAP Work Zone Overview and Components](#)