WorkZone Cloud Edition 2025.0

Installation and Operations Guide

KMD WorkZone

Contents

Installation and Operations Guide for WorkZone Cloud Edition

This guide provides information and guidance about operating WorkZone - Cloud Edition, including setup, installation, and upgrade instructions.

Get started

- Register WorkZone apps in Azure
- Enroll WorkZone - Cloud Edition in Azure and set up SCIM provisioning
- Creating Organizational units for WorkZone Cloud Edition
- Add guest users

What's new

Updated guidelines for configuring automatic provisioning for the enterprise WorkZone application

For instructions on how to provision the group description from Entra ID to WorkZone, see 4. Configure automatic provisioning for the enterprise application.

2024.5

Updated guidelines for configuring automatic provisioning for the enterprise WorkZone application

For instructions on how to provision the group description from Entra ID to WorkZone, see 4. Configure automatic provisioning for the enterprise application.

New WorkZone for Office registry key for handling redirection templates

A new `HideRedirectionTemplate` registry key is available for WorkZone for Office Windows Registry. It defines how WorkZone for Office will handle the redirection templates when new documents are created from WorkZone Client.

See Registry keys.

ServerScan Directory Watcher Service

The new KMDServerScan Directory Watcher Service is a Windows service that uploads scanned documents and their metadata to cases in WorkZone.

See Install and configure ServerScan Directory Watcher Service.

New behavior of guest user naming

When you create a guest user based on an e- mail address that is not of your organization's primary domain, the generated user name of the guest user will be suffixed with a running number. This behavior is introduced to ensure that all users have unique user names. It is generally recommended that you name your internal users uniquely, also across subdomains. Read more and see an example in Add guest users.

2024.5

Updated configuration guidelines for registering the WorkZone app in Azure

For instructions on how to register WorkZone app in Azure, see Register WorkZone apps in Azure and Create a WorkZone Enterprise application.

If you plan to use WorkZone 365 with Exchange Online, you will need to add API permissions to your WorkZone app registration. See Register WorkZone apps in Azure.

New WorkZone for Office registry key for handling redirection templates

A new `HideRedirectionTemplate` registry key is available for WorkZone for Office Windows Registry. It defines how WorkZone for Office will handle the redirection templates when new documents are created from WorkZone Client.

See Registry keys.

ServerScan Directory Watcher Service

The new KMD ServerScan Directory Watcher Service is a Windows service that uploads scanned documents and their metadata to cases in WorkZone.

See Install and configure ServerScan Directory Watcher Service.

New behavior of guest user naming

When you create a guest user based on an e-mail address that is not of your organization's primary domain, the generated user name of the guest user will be suffixed with a running number. This behavior is introduced to ensure that all users have unique user names. It is generally recommended that you name your internal users uniquely, also across subdomains. Read more and see an example in Add guest users.

2024.4

Updated configuration guidelines for WorkZone 365 add-ins

If your organization will use WorkZone 365 with shared mailboxes on the Microsoft Exchange Server 2019, you must set custom account to your WorkZone 365 application pool in the Internet Information Services (IIS). See Set custom account in WorkZone 365 application pool.

2024.3

Updated configuration guidelines for WorkZone 365 add-ins

- To use WorkZone 365 add- ins, you will need to download and adjust relevant manifest files. See Deploy and configure WorkZone 365.
- For instructions on how to install and update WorkZone 365 add- ins, see Deploy and configure WorkZone 365 and Update existing WorkZone 365 add- ins.
- If your organization will use WorkZone 365 with shared mailboxes on the Microsoft Exchange Server 2019, you must add an impersonation permission to your Exchange server first. See Using WorkZone 365 with shared mailboxes on Exchange Server 2019.

2024.2

SmartPost: Important if you upgrade from 2024.1 to 2024.2

If you upgrade from 2024.1to 2024.2 and use SmartPost, you must cancel running SmartPost processes and restart them using the **Send SmartPost** dialog (not from the Processes Overview). This is to ensure that SmartPost uses the upgraded NgDP dispatcher.

Mass Dispatch: Important if you upgrade from 2024.1 to 2024.2

If you upgrade from 2024.1to 2024.2 and use WorkZone Mass Dispatch, you must complete all mass dispatch processes before you upgrade. Any active mass dispatch processes will not continue to run after the upgrade.

2024.1

No changes in this release.

2024.0

Add process packages

You can now add customized process packages using in WorkZone Configurator.

Note that existing command line Package Loader tool is not supported in a cloud installation.

See Activate and load process packages.

2023.3

This is the first version of this guide.

Configure

Follow the procedures below to configure specific WorkZone modules.

Deploy and configure WorkZone 365

WorkZone 365 extends Microsoft 365 (formerly Office) applications with add-ins for document management and collaboration.

There are two types of WorkZone 365 add-ins which require different deployment approaches:

- Outlook add-ins (for email and meeting integration)
- Office add-ins (for Word, Excel, and PowerPoint integration)

Prepare the WorkZone 365 add-ins manifest files

Before you start the deployment, you must download and, in some cases, adjust the manifest files for all relevant WorkZone 365 add-ins.

A manifest file is an XML document that tells Microsoft Office how to load and display the WorkZone 365 add-in. Each type of WorkZone 365 add-ins (Office, Outlook mail, Outlook meeting) has its own manifest file.

If you need multiple WorkZone installations to coexist in the same Office environment, you must customize the manifest files by using unique GUIDs (to prevent conflicts) and different add-in display names (to help users identify which WorkZone 365 version they are using).

Customize the manifest files

To customize the manifest file, you will need to:

Download the manifest file from the WorkZone server

1. Download the manifest files from your WorkZone server using the following links (copy and paste the URLs provided below into your browser's address bar, replacing the `[hostname]` with your proper host name):
    - WorkZone 365 add-in for Outlook: `https://[hostname]/app/office/webaddins/outlook/mail/MailManifest.xml`

- WorkZone Meeting add-in: `https://[host-name]/app/office/webaddins/outlook/meeting/MeetingManifest.xml`
- WorkZone 365 add-in for Word, Excel, and PowerPoint: `https://[hostname]/app/office/webaddins/office/OfficeManifest.xml`

2. Replace the *[hostname]* with your preferred WorkZone instance. For example: *https://workzone.dk/app/office/webaddins/office/OfficeManifest.xml*.
3. Press **Enter**. The manifest file will be downloaded to your computer's default download location.

If needed, update the WorkZone ID (GUID)

If you use multiple instances of WorkZone 365, for example, Outlook on the same Exchange server, or different versions of WorkZone 365 for Outlook on the same Exchange server, you must change the WorkZone 365 ID (GUID) in the `MailManifest.xml` under the `<Id>` tag. For example:

```
    <Id>7f0f121e-7dba-428b-b37f-6035270e48b4</Id>
```

An example of a unique ID (GUID) for production and test instances in the manifest files could look as follows:

- Manifest file for Outlook Test add-in: `<Id>7f0f121e-7dba-428b-b37f-6035270e48b4</Id>`
- Manifest file for Outlook PROD add-in: `<Id>d9be36b1-6aea-425c-87bc-ce614ce8053d</Id>`

You can use a GUID generation tool, for example, GUID Generator to get the unique IDs.

If needed, update the add-in display name and localized label values

By default, the WorkZone 365 add-in label is "*WorkZone*", but you can adjust it in the relevant manifest file. If you use multiple instances of WorkZone 365, you will need to update the label values and DisplayName in the manifest file to identify your environment in the Office UI. For example, you can replace "WorkZone" with your environment name, such as "*WorkZone Prod*" or "*WorkZone Test*". Additionally, you can add a localized label for different languages (replace the "*New_name*" in the examples below

with your preferred name for each language).

Examples for each type of manifest files:

- OfficeManifest.xml file (WorkZone 365 add- in for Word, Excel, and PowerPoint):

  Example:

```
<DisplayName DefaultValue="WorkZone">
     <Override Locale="da-DK" Value="New_name"/>
     <Override Locale="de-DE" Value="New_Name"/>
</DisplayName>
...
<Resources>
...
<bt:ShortStrings>
    <bt:String id="XXXX.Label" <DefaultValue="WorkZone">
          <bt:Override Locale="da-DK" Value="New_name" />
          <bt:Override Locale="de-DE" Value="New_name" />
    </bt:String>
    </bt:String id="YYYY.Label" DefaultValue="WorkZone">
          <bt:Override Locale="da-DK" Value="New_name" />
          <bt:Override Locale="de-DE" Value="New_name" />
    </bt:String id="YYYY.Label" DefaultValue="WorkZone">
<bt:ShortStrings>
```

- MailManifest.xml file (WorkZone 365 add- in for Outlook):

  Example:

```
<DisplayName DefaultValue="WorkZone">
     <Override Locale="da-DK" Value="New_name"/>
     <Override Locale="de-DE" Value="New_name"/>
</DisplayName>
```

```
<Description DefaultValue="WorkZone 365 - Mail">
</Description>
...
<Resources>
...
<bt:ShortStrings>
   <bt:String id="XXXX.Label" <DefaultValue="WorkZone">
         <bt:Override Locale="da-DK" Value="New_name" />
         <bt:Override Locale="de-DE" Value="New_name" />
   </bt:String>
<bt:ShortStrings>
```

- MeetingManifest.xml file (WorkZone Meeting add-in for Outlook):

  Example:

```
      <Override Locale="da-DK" Value="New_name"/>
      <Override Locale="de-DE" Value="New_name"/>
</DisplayName>
<Description DefaultValue="WorkZone 365 - Meeting">
</Description>
</DisplayName>
```

> **Important:** Make sure to update all "WorkZone" instances in the XML file.

Save the customized manifest file

Save a copy of each manifest file locally or on a shared drive under a proper file name. This will help you monitor all your instances and versions of WorkZone 365, especially if you have updated the displayed name or made any feature changes to the manifest file.

When you upload the new manifest file, remember to insert the manifest name, description, and GUID for the add-in that you want to update.

After you have adjusted the manifest file(s), you are ready to deploy the WorkZone 365 add-ins.

Deploy the WorkZone 365 add-ins

The deployment approach depends on your environment.

- For Cloud environments: Microsoft 365 Admin Center deployment
- For on-premises environments:
  - Outlook add-ins: Exchange Admin Center deployment
  - Office add-ins: Group Policy deployment

Cloud Deployment

1. Open the Microsoft 365 Admin Center.
2. Navigate to **Integrated apps** > **Upload custom apps**.
3. Upload your customized manifest files.

For the detailed steps, see Microsoft article Deploy an Office add-in using the admin center.

On-Premises Deployment

Outlook add-ins

1. Open the Exchange admin center: https://[exchange-server]/ecp.
2. Upload your customized manifest files (`MailManifest.xml` and/or `MeetingManifest.xml`).
3. Install the WorkZone 365 Outlook add-ins. See Microsoft article Add-ins for Outlook in Exchange Online for the detailed steps.

Office add-ins

Office add-ins (for Word, Excel, and PowerPoint) cannot be deployed via Exchange admin center. Instead, the centralized deployment must be done using the group policies.

1. Download and install Microsoft Office Administrative Templates.
2. On your drive, create a folder named **Manifest** and add there your `OfficeManifest.xml` file.
3. Create a network share for the **Manifest** folder, and add network share to trusted locations. See Microsoft article Sideload Office Add-ins for testing from a network share for the detailed steps.
4. Configure the Group policy for WorkZone 365 add-ins.

Post-deployment verification

After you have deployed the WorkZone 365 add-ins:

- Check that the add-in appears with the Office label specified in the manifest file
- Verify that add-in loads in all required applications
- Confirm that WorkZone functionality works as expected

Troubleshooting

If WorkZone 365 add-ins do not appear:

- Verify that relevant manifest file is available and has correct formatting
- Clear the Office cache. See the Clear cache Microsoft article for the detailed steps.
- Users might need to relaunch the Office app for the WorkZone 365 add-in to appear.

Note: It may take up to 24 hours for a new add-in to appear for all users. It may take up to 72 hours for add-in updates or settings changes to reflect to the users. For more information about centralized deployment of web add-ins, see official Microsoft guide.

Update existing WorkZone 365 add-ins

When you upgrade to a newer version of WorkZone, the WorkZone 365 add-ins will automatically update to the latest release. However, some releases include updates to the manifest files to enable new Microsoft features, which means that if you made any customizations to your manifest files (such as GUIDs, add-in displayed name, localized labels), you will need to preserve them.

- Any changes to the manifest files will be documented in the release notes.

1. Download the new manifest files from the WorkZone server.
2. Preserve your customizations for the manifest files, if any (GUIDs, displayed name, localized labels).
3. Upload the customized manifest files using your deployment method:
    - For Cloud environments: **Microsoft 365 Admin Center** > **Settings** > **Integrated apps**.
    - For on-premises environments: Update all manifest files in your network share (for Outlook add-ins) and in the Exchange admin center (for Office add-ins).

> **Tip:** Sometimes, users may not immediately see the add-in after an update. Users can try right-clicking the panel to manually refresh it after the new add-in update. You can verify whether the add-in has been updated by checking if it has a higher build number than before.

Using WorkZone 365 with shared mailboxes on Exchange Server 2019

If your organization wants to use WorkZone 365 with shared mailboxes on Microsoft Exchange Server 2019, you must complete the following steps first:

- Add your Exchange server URL in WorkZone Configurator
- Add impersonation permission to your Exchange Server 2019
- Set custom account in WorkZone 365 application pool

Important: For shared mailboxes, WorkZone 365 functionality is only supported with Microsoft Exchange Server 2019 and Microsoft Exchange Server Online. If you use Exchange Server Online, no additional configuration is needed.

Add your Exchange server URL in WorkZone Configurator

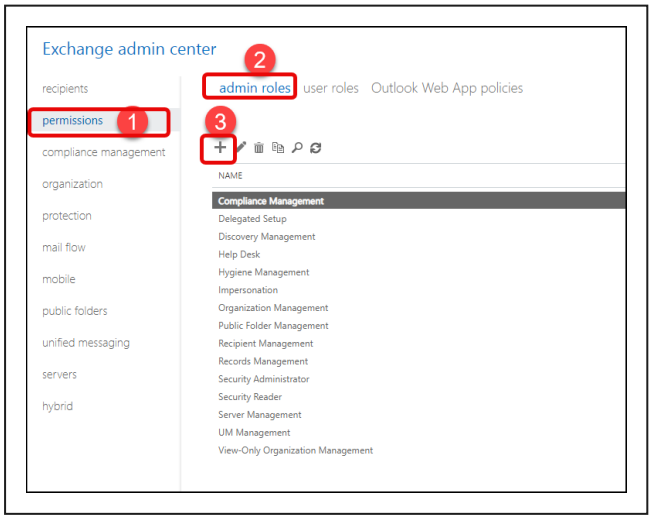
Prerequisite: You must have the CONFIGADM access code to edit the external services in WorkZone Configurator.

See Add a new external service.

Add impersonation permission to your Exchange Server 2019

Prerequisite: You must have an administrator account for the Exchange admin center.

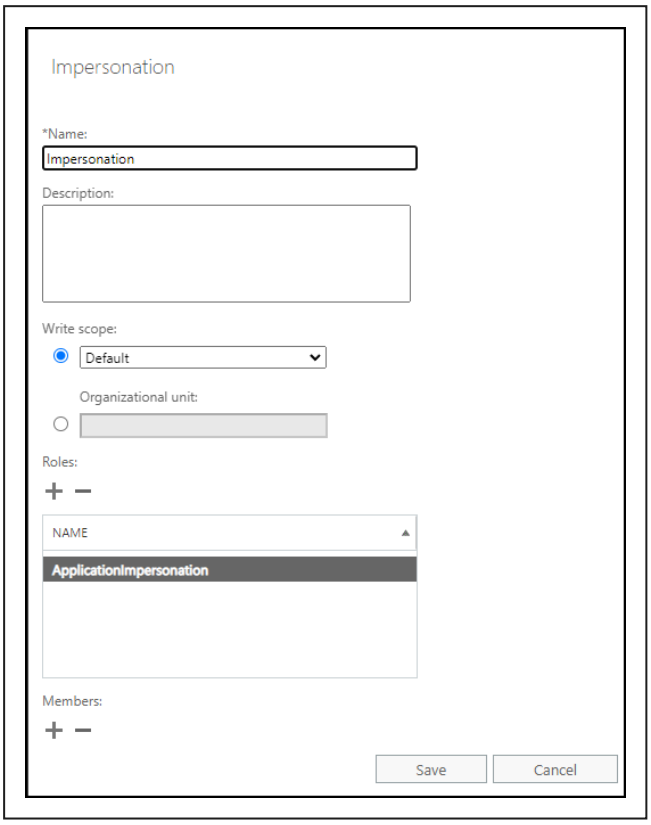
1. Log in to your Exchange admin center: `https://[your_exchange_server-]/ecp/`, replacing the *[your_exchange_server]* with your Exchange server. For example, https://workzone/ecp/.
2. On the **permissions** tab, select **admin roles** and click **+**.



3. In the new **Impersonation** dialog:

    a. Enter the permission name. For example, *Impersonation*.

    b. Add role: **ApplicationImpersonation**.



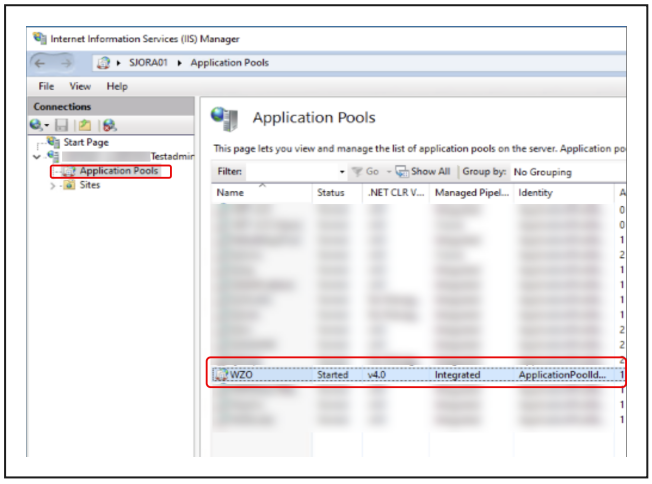
    c. In the **Members** section, click **+** and add your user.

> **Prerequisite:** This user must also:
>
> - Have access to OData.
> - Exist in WorkZone and (only for cloud environments) in the Entra ID directory (under the **SystemAccountUsers** catalog in the WorkZone 365 server properties).
> - Be a member of the security group that has security code **1** or higher (for example, `ScanJourCaptia_1`). See Entra ID provision and Apply security groups.

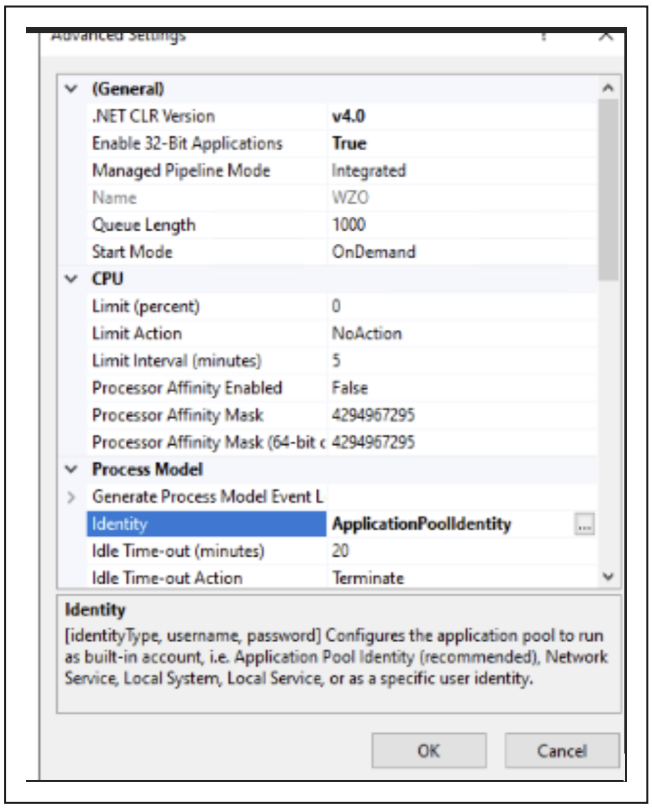
4. Click **Save**.

Set custom account in WorkZone 365 application pool

1. From web server, open the **IIS Manager**.
2. On the left panel, expand your server and select **Application Pools**.



3. Right-click the **WZO** application pool and select **Advanced settings**.
4. Under **Process Model**, click **...** next to the **Identity**.



5. Click **Custom account** > **Set**.
6. Enter the user name and password for your service account in Exchange Server, and click **OK**.
7. Verify that your new account is created in WorkZone.

Install and configure WorkZone for Office

Prerequisites for WorkZone for Office

- Visual Studio 2010 Tools for Office Runtime (Download from the Microsoft website).
- During the WorkZone installation, you must select the **Office Services** feature.

Required data and default values

For WorkZone for Office to work correctly, you must verify that the following default values are present on the server.

- Document types:
  - **I** (Incoming)
  - **U** (Outgoing)
- Roles for document types:
  - **Afsender** (Sender)
  - **Modtager** (Recipient)
  - **Kopimodt.** (Copy Recipient)
  - **Sagspart** (Case Party)
- Roles for document references:
  - **Besvarer** (Reply To)
- Organizational contact types:
  - **A** (Unit)
  - **F** (Companies (without CVR))

- **I** (Institutions)
- **U** (Groups)
- **K** (Municipalities)

Correct these values manually (if needed) by overriding appropriate elements in the `settings.xml` file and uploading those to the database. See Configure WorkZone for Office server .

Cached Exchange Mode for WorkZone for Outlook

To increase performance for WorkZone for Outlook, it is required that you set up the user accounts in Microsoft Outlook to use **Cached Exchange Mode**. **Cached Exchange Mode** provides users with a better experience when connecting to Microsoft Exchange, because a full copy of the mailbox is stored on the local computer and is asynchronously updated.

In contrast, users might experience slight performance degradation when running in **Online** mode (that is, with **Cached Exchange Mode** turned off).

WorkZone for Office uses the cached mail store to resolve the email threads that an email is part of. This information is used to create a document reference when saving an email from the **Sent** items folder in Microsoft Outlook that has been sent in reply to another saved email. In this special case, there is a slight difference in behavior, since this reference can only be detected when **Cached Exchange Mode** is turned on.

Turn on/off cached exchange mode

1. Open Outlook.
2. On the **File** tab, click **Account Settings**.
3. On the **E- mail** tab, select the **Exchange Server** account, and then click **Change**.
4. Under **Server settings**, select the **Use Cached Exchange Mode** check box to turn cached **Exchanged Mode** on.

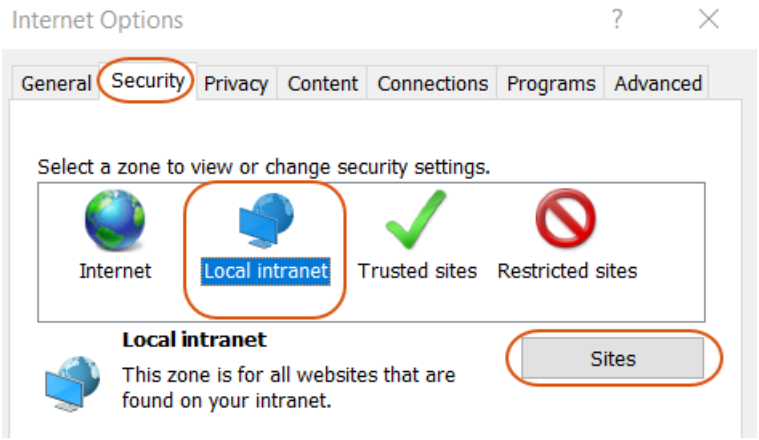
Add your website to the local intranet zone

1. In **the Control Panel**, select **Internet Options**.

   - Or-

Run the `inetcpl.cp` command in the command line.

2. On the **Security** tab, select **Local intranet** and click **Sites**.



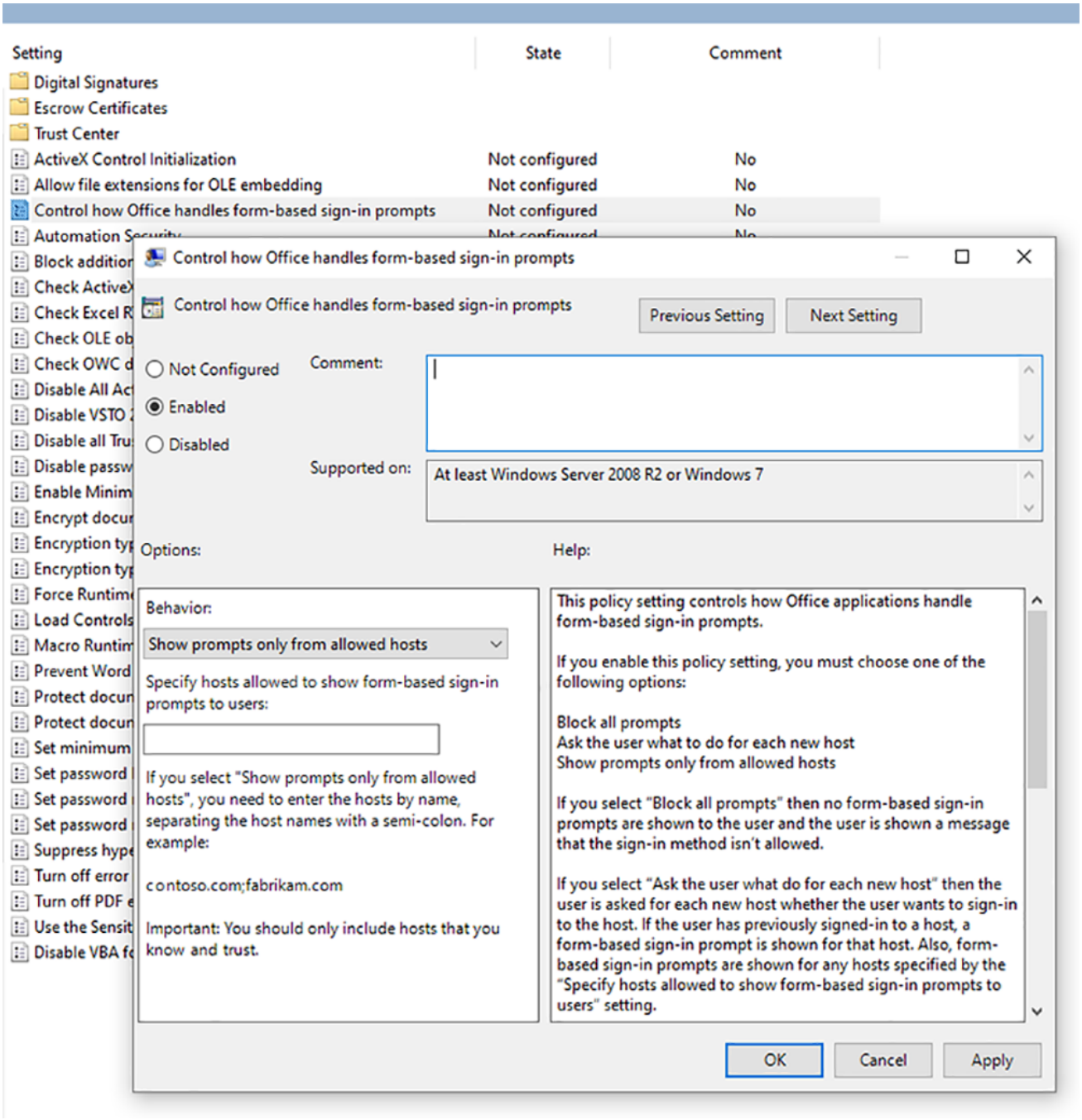
3. Click **Advanced**.
4. In the **Add this website to the zone** field, enter your website domain, and click **Add**.

Enable form-based authentication in Microsoft Office 365 apps

If your organization uses OAuth2 for user authentication, you must enable form-based authentication in Microsoft Office 365 apps.

To help provide additional security coverage, Microsoft manages how the form-based authentication in Office applications is handled. Form-based authentication is a legacy authentication method for Office resources that are not protected by Azure Active Directory or a Microsoft account. Because Office does not know the location of the form-based authentication, Office will block such sign-in dialogs and will notify the end-user that the sign-in has been blocked.

An administrator can enable the form-based authentication by adding a list of trusted locations by using a group policy. In this case, your users will be able to open documents from these locations without the warning.



End users can unblock themselves by changing a security setting in the Office Trust Center. They can do so proactively by going to **File** > **Options** > **Trust Center** > **Trust Center Settings** > **Form- based sign- in**, or they can wait until they have been prompted to open Trust Center via a warning dialog.

In the **Trust Center** > **Form- based Sign- in** panel, the end users should change **Block all sign- in prompts** to **Ask me what to do for each host** and save the changes. The list of safe hosts will be auto- populated based on future end- user actions.

After a user has made this change in the Trust Center, Office will not block future sign- in prompts. Instead, it will display a dialog asking if the user wants to continue signing in. If yes, Office will show the sign- in prompt immediately. In the future, Office will provide sign- in prompts for this allowed host, which will be added to the list of **Hosts allowed to show sign- in prompts** in the **Trust Center** > **Form- based Sign- in**.

Required registry settings

It is recommended, that you add the following registry settings on all PCs running WorkZone for Office, to avoid WorkZone add- in being occasionally turned off in Microsoft Office applications (Word, Excel, PowerPoint, Outlook).

- General Microsoft Office keys (apply to all Office versions, must be added once)

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer-
\Main\FeatureControl\FEATURE_BROWSER_EMULATION]
"OUTLOOK. EXE"=dword:00001b58
[HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\Outlook\Addins\Scanjour.Office.OutlookAddIn]
"LoadBehavior"=dword:00000003
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Office\Outlook\Addins\Scanjour.MeetingModule.OutlookAddIn]
"LoadBehavior"=dword:00000003
[HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\Word\Addins\Scanjour.Office.WordAddIn]
"LoadBehavior"=dword:00000003
[HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\Excel\Addins\Scanjour.Office.ExcelAddIn]
"LoadBehavior"=dword:00000003
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Office\PowerPoint\Addins\Scanjour.Office.PowerPointAddIn]
"LoadBehavior"=dword:00000003
```

- Microsoft Office 2016, 2019, and Microsoft 365 keys (must be added once):
  - Outlook

```
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Of-
fice\16.0\Outlook\Resiliency\DoNotDisableAddinList]
```

```
"Scanjour.Office.OutlookAddIn"=dword:00000001
```

```
"Scanjour.MeetingModule.OutlookAddIn"=dword:00000001
```

    The following setting is only required, if you want to view **Cases & Document** lists as a folder in Outlook:

```
[HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\16.0\Outlook\Security]
```

```
"EnableRoamingFolderHomepages"=dword:00000001
```

    See WorkZone for Office user guide for more information.

  - Word

```
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Of-
fice\16.0\Word\Resiliency\DoNotDisableAddinList]
```

```
"Scanjour.Office.WordAddIn"=dword:00000001
```

  - Excel

```
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Of-
fice\16.0\Excel\Resiliency\DoNotDisableAddinList]
```

```
"Scanjour.Office.ExcelAddIn"=dword:00000001
```

  - PowerPoint

```
[HKEY_CURRENT_USER\Soft-
ware\Mi-
```

```
crosoft\Of-
fice\16.0\PowerPoint\Resiliency\DoNotDisableAddinList]
```

```
"Scanjour.Office.PowerPointAddIn"=dword:00000001
```

- Deleting keys (must be rolled out on a daily basis or whenever WorkZone users log in to their machines):
  - Deleting keys to clear blacklists of add-ins that caused Microsoft Office apps to crash:

```
[-HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Office\16.0\Outlook\Resiliency\CrashingAddinList]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Office\16.0\Word\Resiliency\CrashingAddinList]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Office\16.0\Excel\Resiliency\CrashingAddinList]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Of-
fice\16.0\PowerPoint\Resiliency\CrashingAddinList]
```

  - Deleting keys to clear the list of already disabled Microsoft Office add-ins:

```
[-HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\16.0\Outlook\Resiliency\DisabledItems]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\16.0\Word\Resiliency\DisabledItems]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\16.0\Excel\Resiliency\DisabledItems]
```

```
[-HKEY_CURRENT_USER\Soft-
ware\Microsoft\Office\16.0\PowerPoint\Resiliency\DisabledItems]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer-
\ProtocolExecute\wzfo]
```

```
"WarnOnOpen"=dword:00000000
```

Configure WorkZone for Office server

You can configure the behavior and appearance of WorkZone for Office by changing the server settings. For example, you can change the default values by overriding the values in the server configuration.

Configurable elements

Note: You can also configure many of these elements in WorkZone Configurator. See Outlook configuration.

Element	Default value	Description
RecordTypes - Incoming	I	Defines the value used for the record_type field on saved emails. The value of Incoming is the record_type field that is used when saving a received email. Valid values of Incoming and Outgoing are values from the domain on the record_type field (custom_domain with the domain parameter 'AT').
RecordTypes - Outgoing	U	Defines the values used for the record_type field on saved emails. The value of Outgoing is the record_type field that is used when saving an email which is sent or going to be sent. Also, this value is automatically set

Element	Default value	Description
		for reply documents. In a standard configuration, the **Document Type** for reply documents is `U, Outgoing`. Valid values of `Incoming` and `Outgoing` are values from the domain on the `record_type` field (`custom_domain` with domain parameter 'AT').
`PartyRoleKeys - Sender`	`Afsender`	Defines the values used for the sender, recipient, and Cc recipient roles on archived emails. Valid values of the `Sender`, `Recipient`, and `CcRecipient` roles are values from the domain on the `party:custom_label` field in the record register (`custom_label` with domain parameter 'AP').
`PartyRoleKeys - Recipient`	`Modtager`	Defines the values used for the sender, recipient, and Cc recipient roles on archived emails. Valid values of the `Sender`, `Recipient`, and `CcRecipient` roles are values from the domain on the `party:custom_label` field in the record register (`custom_label` with domain parameter 'AP').
`PartyRoleKeys - CcRecipient`	`Kopimodt`	Defines the values used for the sender, recipient, and Cc recipient roles on archived emails. Valid values of the `Sender`,

Element	Default value	Description
		`Recipient`, and `CcRecipient`roles are values from the domain on the `party:custom_label` field in the record register (`custom_label` with domain parameter 'AP').
`PartyRoleKeys - CaseParty`	`Sagspart`	Defines the values used for the sender, recipient, and Cc recipient roles on archived emails. Valid values of the `Sender`, `Recipient`, and `CcRecipient`roles are values from the domain on the `party:custom_label` field in the record register (`custom_label` with domain parameter 'AP').
`DocumentRefRoleKeys - Reply`	`Besvarer`	Defines the value used for the role of document references that is created when replying to an archived email. Valid value of `Reply`is the value from the domain on the `appendix:role` field in the record register (`custom_label` with domain parameter 'AA').
`ContactTypes - Company`	`A;F;I;U;K`	Defines the list of contact types which should be considered as organizational units during an automatic mapping of personal senders to organizational units.

Element	Default value	Description
AutoCreateMissingContact	True	Defines whether the system should create contacts from the email sender, recipient, and Copy fields if the contacts do not exist.
SuggestAnyContactWhenSavingEmail	True	Automatically adds or suggests matching organizational contacts from the contact register when you save an email from Outlook. When this setting is disabled, matching organizational contacts are not added automatically or suggested to be added.
GlobalSuggestionsBlacklist	gmail.com; gmail.dk; hotmail.com; hotmail.dk; facebook.com; yahoo.com; yahoo.dk; mail.tele.dk; mail.tdc.dk	Domain names in this list are excluded from searches for organizational contacts.
PredefinedFilters	my_open_cases; my_personal_d rafts	Defines the lists of cases or documents to be automatically added to the navigation pane in Microsoft Outlook when the user opens Outlook for the first time after installing WorkZone for Outlook. For example, the following configuration will add the **Cases & Documents** folder to the nav-

Element	Default value	Description
		igation pane, including two sub-folders: • **Open Cases** (filter name `my_open_cases`) • **Drafts** (filter name `my_personal_drafts`) Find the full list of search filters in the Standard lists table.
`RegisterSelfWhenSaveEmail`	`False`	Defines whether the user who is about to save an Outlook item appears as a contact in the **OutlookItemRegistrationDialog** dialog box. The default value is `False` which means that the e-mail address of the user who saves an Outlook item does not appear in the dialog box as a sender or a recipient. Change the value to `True` to make the email address of the user who saves the Outlook item appear as a contact, including sender or recipient information.
`CheckAllUnresolvedContacts`	`False`	By default, only contacts from the **To**, **From**, and **Cc** fields which are registered in the contact register are selected in the **OutlookItemRegistrationDialog** dialog box. When enabled, all contacts are automatically selected.

Element	Default value	Description
UseCurrentUserAsCaseHandler	False	Defines who should be assigned as a case handler to an Outlook item which is about to be saved on a case. This value is used for **OutlookItemRegistrationDialog** only. • `False` – The case handler is inherited from the case on which the Outlook item is saved. • `True` – The case handler that is assigned to the Outlook item is the current user.
MassRegistration - EnableEditCommonMetadata	False	Defines if common metadata values of the multiple saved Outlook items can be edited. This value is used for **MultipleSavingCommonMetadataDialog** only. • `False` – The common metadata values for the multiple saved Outlook items cannot be edited, and the **Save Multiple Outlook Items** dialog box is not displayed. • `True` – The **Save Mul-**

Element	Default value	Description
		tiple Outlook Items dialog box is displayed, and the common metadata values for the multiple saved Outlook items can be edited.
`DisplayDateFormat`	`SystemDefault`	Defines the date format for the date picker content control. The configuration of a short or long date format will apply to all users, but the exact format such as dd-mm-yy or MM-dd-yy will be defined locally by the user's regional settings. If the value is `SystemDefault`, the system date format is used. If the value is `Short` or `Long`, the short or long date format is used respectively.
`SuggestAnyContactWhenCreatingCase`	`True`	Automatically adds or suggests matching organizational contacts from the contact register when you create a case from Outlook. When this setting is disabled, matching organizational contacts are not suggested or added automatically.
`SearchFilters - Register Name="Case" BlackList`	`my_reading_list_cases; my_meetings;`	Simplifies the search process. By specifying search filters to be excluded from the search dialog box you can limit the

Element	Default value	Description
	my_organized_meetings; my_temporary_cases; my_recent_cases; my_changed_cases	number of search options for case and meeting. Find the full list of search filters in the Available case and meeting lists table.
SearchFilters - Register Name="Record" BlackList	my_reading_list_records; my_changed_records; my_recent_records; thrashed_records	Simplifies the search process. By specifying search filters to be excluded from the search dialog box you can limit the number of search options for documents. Find the full list of search filters in the Available document lists table.
Check-ResolvedContactsBlackList	<empty>	If you do not want the contacts from a specific company to be saved as parties, specify the company's email domain in the @domain format. When a user creates a new case or saves an email to a case in Outlook, contacts that belong to the specified email domain are not pre- selected for saving. The user can select them manually, if needed.
DocumentTemplatesPath	<empty>	A path to a folder that contains Word, Excel and Power Point templates. When a user creates a new document in WorkZone Client, this folder opens in the Windows **Open file** dialog box. There are three ways to define

Element	Default value	Description
		the path: • Absolute path • Relative path • UNC format If the path is not defined, the Office **Template selection** dialog box opens.
<AccessCodesAffectRequiredFields>	<empty>	Users assigned access codes listed here must assign at least one access code when they create a new case, document, or contact.

Default server settings

Standard value set in WorkZone Office server installer

Below is the standard value set installed using `KMD WorkZone Office Server.msi`:

```
<Scanjour>
    <Settings>
        <OfficeClients>
            <RecordTypes>
                <Incoming>I</Incoming>
                <Outgoing>U</Outgoing>
            </RecordTypes>
            <PartyRoleKeys>
                <Sender>Afsender</Sender>
                <Recipient>Modtager</Recipient>
                <CcRecipient>Kopimodt.</CcRecipient>
```

```
                    <CaseParty>Sagspart</CaseParty>
                </PartyRoleKeys>
                <DocumentRefRoleKeys>
                    <Reply>Besvarer</Reply>
                    </DocumentRefRoleKeys>
                <ContactTypes>
                    <Company>A;F;I;U;K</Company>
                </ContactTypes>
                <DefaultCountryCode>DK</DefaultCountryCode>
                <AutoCreateMiss-
ingContact>True</AutoCreateMissingContact>
                <SuggestAnyContactWhenSav-
ingEmail>True</SuggestAnyContactWhenSavingEmail>
                <GlobalSuggestionsBlacklist> gmail.-
com;g-
mail.dk;hot-
mail.-
com;hot-
mail.dk;facebook.com;yahoo.com;yahoo.dk;mail.tele.dk;mail.tdc.dk
                </GlobalSuggestionsBlacklist>
                <PredefinedFilters>my_open_cases;my_personal_draft-
s</PredefinedFilters>
                <Register-
SelfWhenSaveEmail>False</RegisterSelfWhenSaveEmail>
                <Check-
AllUnresolvedContacts>False</CheckAllUnresolvedContacts>
                <UseCur-
rentUserAsCaseHandler>False</UseCurrentUserAsCaseHandler>
                <MassRegistration>
                    <EnableEditCom-
monMetadata>false</EnableEditCommonMetadata>
```

```
                </MassRegistration>
                <DisplayDateFormat>SystemDefault</DisplayDateFormat>
                <SearchFilters>
                <Register Name="Case" BlackList="my_reading_list_case-
s;my_meetings;my_organized_meetings;my_temporary_cases;my_recent_
cases;my_changed_cases">
                <Filter Name="ClosedCases">
                <Description xml:lang="en-GB">Closed case-
s</Description>
                <Description xml:lang="da-DK">Afsluttede sager-
</Description>
                <Description xml:lang="ja-JP">保存済ケース</De-
scription>
                <Column Name="closed" Value="&lt;&gt;&quot;&quot;" />
                </Filter>
                </Register>
                <Register Name="Record" BlackList="my_reading_list_
records;my_changed_records;my_recent_records;thrashed_records"/>
                </SearchFilters>
                <Check-
ResolvedContactsBlackList></CheckResolvedContactsBlackList>
                <DocumentTemplatesPath></DocumentTemplatesPath>
                <AccessCodesAf-
fectRequiredFields></AccessCodesAffectRequiredFields>
            </OfficeClients>
        </Settings>
</Scanjour>
```

How to configure server settings:

1. Locate the configuration file

```
%Program Files(x86)\KMD\WorkZone\Modules\Office\Configuration\settings.xml
```

2. Edit the `setting.xml` file and save your changes.
3. Reload the configuration by running the following in the command prompt:

```
%Program Files(x86)\KMD\WorkZone\Modules\Office\configurationloader.exe
```

Use these parameters:

`/dbdsn=<dsn>` – The name of the database to be updated.

`/dbuser=<user>` – The name of the database user.

`/dbpassword=<password>` – The password of the database user.

`/serveruri=<protocol>://<hostname>` – The protocol and hostname for the oData service.

`/serveruser=<username@domain>` – The name of a user with access to WorkZone.

`/serverpassword=<password>` – The password of a user with access to WorkZone.

Registry keys

You can use new registry keys to fine-tune a standard behavior of WorkZone for Office according to your needs. Below, you can find the right registry path for your configuration:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\ScanJour\Clients\Options - Windows 32 bit; Outlook 32 bit or >Windows 64 bit; Outlook 64 bitComputer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ScanJour\Clients\Options - Windows 64 bit; Outlook 32 bitComputer\HKEY_CURRENT_USER\SOFTWARE\ScanJour\Clients\Options - To apply changes only to the current user's machine
```

Define a delay to start processing emails in the Sent folder (the 'Save on Send' functionality)

1. Add the `SentFolderItemsProcessingDelay` key to the registry.
2. Specify the delay in ms.

Skip checking unsaved emails when a user starts WorkZone for Office

1. Add the `IgnoreUnsavedEmailsInSentFolder` key to the registry.
2. Specify a value:
    - **1** – skip checking unsaved emails
    - **0** – check the unsaved emails (this is the default value)

Define how WorkZone for Office will handle the redirection templates when new documents are created from WorkZone Client

1. Add the `HideRedirectionTemplate` key to the registry.
2. Specify a value:
    - **1** – upon detecting a redirection template, WorkZone for Office will close the document and create a new one from the template selected by the user.
    - **0** – upon detecting a redirection template, WorkZone for Office will make it invisible instead of closing.

Define a timeout for a SmartTask to be shown in offline mode

The `SmartTaskOfflineTimeOut` key defines the time when WorkZone for Office tries to connect to WorkZone Process. If connection fails during the defined time, smarttask is shown in the offline mode. When the connection is established again, a user must click the smarttask to see the updated information.

1. Add the `SmartTaskOfflineTimeOut` key to the registry.
2. Specify the timeout in ms.

Define a timeout to disable the **Process** button

The `StartProcessButtonTimeOut` key defines the time when WorkZone for Office tries to connect to WorkZone Process. If the timeout has run out and connection wasn't established, the **Process** button stays active and the next attempt to connect will be applied. If connection fails due to another reason than timeout, the **Process** button is disabled. Users see the hint that WorkZone Process is either not installed, or connection has failed.

1. Add the `StartProcessButtonTimeOut` key to the registry.
2. Specify the timeout in ms.

Define source to pull the TLS settings

If you have connection issues related to TLS (Transport Layer Security), it may be caused by the WorkZone for Office custom settings. To disable them and pull the TLS settings from the.NET framework, create the DWORD key called `SkipCustomTlsSettings` in registry and set its value to 1.

Search filters

WorkZone for Office requests search lists from WorkZone. If any of the lists are not needed on a particular form, WorkZone for Office excludes it by using a specific command in the request.

Available case and meeting lists (search filters)

User interface name	Name in code	Description
Open cases	`my_open_cases`	Your current cases.
Cases with reminders	`my_case_reminders`	Those of your cases that have reminders.
Unit’s open cases	`units_open_cases`	Current cases that belong to your unit.
Unit’s cases with no case handler	`units_cases_without_owner`	Cases that belong to your unit and which are not yet assigned to a case handler.
Cases with no case handler and unit	`cases_without_owner_and_unit`	Cases that belong to a temporary unit and

User interface name	Name in code	Description
		which are not yet assigned to a case handler.
Favorite cases	`my_favorite_cases`	Cases that you have added as favorites.
Followed cases	`my_followed_cases`	Cases where you have subscribed to follow updates.
Reading list cases	`my_reading_list_cases`	New cases that have been assigned to you.
Meetings	`my_meetings`	All your meetings.
Meetings organized by me	`my_organized_meetings`	Meetings that you have organized.
Recent cases	`my_recent_cases`	The cases that you have viewed or edited most recently. The list displays up to 1000 cases.
Unclassified cases	`my_temporary_cases`	Cases that belong to a temporary group. You can assign the cases to a relevant group at anytime.
Changed cases	`my_changed_cases`	Cases that you follow which have been updated recently.

Available document lists (search filters)

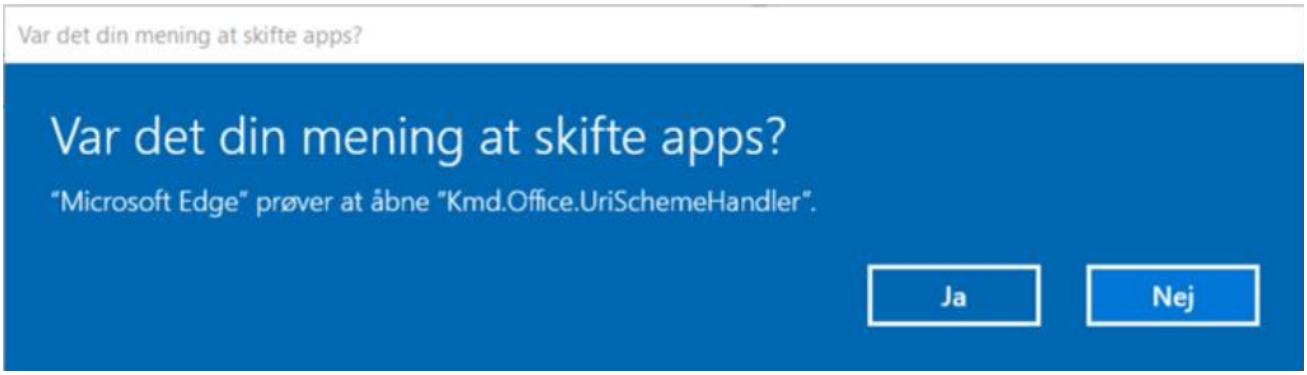
User interface name	Name in code	Description
Drafts	`my_personal_drafts`	Those of your documents that have the `draft` or `personal`

User interface name	Name in code	Description
		`draft` state.
Today	`my_documents_today`	The documents that you have created today.
Documents	`active_documents`	All your current documents. This list does not include any closed or archived documents.
Favorite documents	`my_favorite_records`	Documents that you have added as favorites.
Unit's documents with no case handler	`units_documents_without_owner`	Documents that belong to your unit and which are not yet assigned to a case handler.
Documents with no case handler and unit	`documents_without_owner_and_unit`	Documents that belong to a temporary unit and which are not yet assigned to a case handler.
Followed documents	`my_followed_records`	Documents where you have subscribed to follow updates.
Scanned today	`scanned_today`	Documents that you have scanned today.
Reading list documents	`my_reading_list_records`	New documents that have been assigned to you.
Recent documents	`my_recent_records`	The documents that you have viewed or edited most recently. The list displays up to 1000 documents.
Unanswered documents	`my_unanswered_records`	Those of your documents that have not been answered by the reply date.
Changed documents	`my_changed_records`	Documents that you follow which have been updated recently.

User interface name	Name in code	Description
Documents with reminders	`documents_with_reminders`	Documents that you must reply to within 7 calendar days.

Troubleshooting

In Edge, while using the WorkZone for Office functionality integrated in WorkZone Client, you may see the message " Did you mean to switch apps?" .



For example, it can appear when users share documents. The message appears because Edge encounters an unknown WorkZone handler. To avoid the message, you must add the following registry settings:

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer-
\ProtocolExecute\wzfo]
```

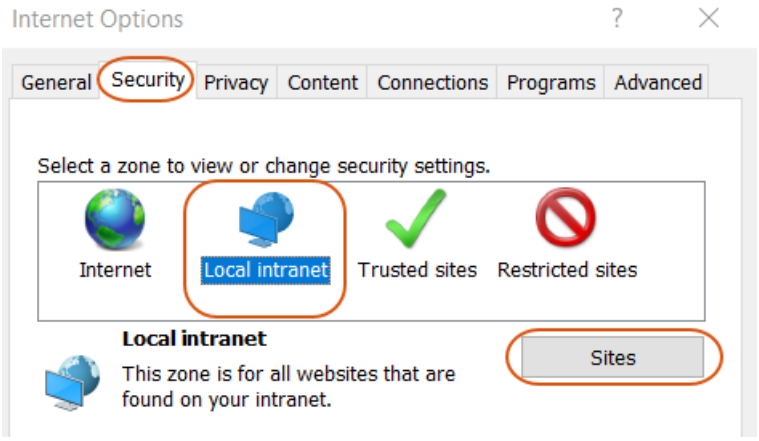
```
"WarnOnOpen"=dword:00000000
```

While using WorkZone 365 in Internet Explorer, Microsoft Edge, or desktop version, you click **Help**, but user guide is not opened.

Workaround: Open the user guide in Chrome.

Solution: Add `https://docs.workzone.kmd.net` to the local intranet zone:

1. Click **Tools** in Internet Explorer and select **Internet options**.
2. On the **Security** tab, click **Local intranet** and then **Sites**.

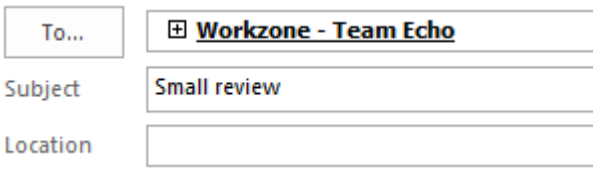


3. Click **Advanced**.
4. Type in `https://docs.workzone.kmd.net`, and click **Add**.

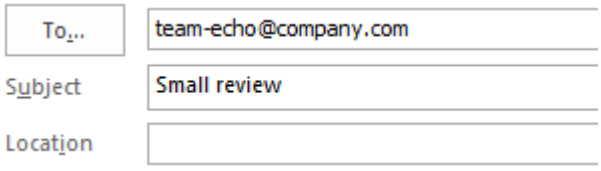
A meeting was sent to a group, but its contacts are not saved as parties on case.

Sometimes Outlook doesn't parse a group email as a group. In this case, the meeting is sent, but contacts cannot be extracted by WorkZone. To solve this issue, ensure that the group email is converted to the group before sending the meeting. See examples:

Group email converted to the group:



Group email not converted to the group:



When you save the Process view list, you see the following notice:

To fix this, you must add the following registry settings:

Microsoft Office 2016:

```
[HKEY_CURRENT_USER\Soft-
ware\Policies\Microsoft\Office\16.0\Common\Security\Trusted Pro-
tocols\All Applications\wzfo:]
```

Note: Value is not mandatory for this key.

In Excel 2016 subscription 365, if you click **Cancel** for the second time, the Excel document is closed without the confirmation message.

This is a specific behavior of Microsoft Office 2016, subscription 365.

You see a COMException when the FQDN (fully qualified domain name) host is used

- If you open a previous version of a Microsoft Office document in the **File > Cases & Documents > Manage versions** section
  - or -
- If you open a non- Microsoft Office document in Outlook overview and the https protocol is used.

The COMException is caused by a known issue in WebDAV. WebDAV is used for opening documents. To fix the exception, proceed with the instructions described in the WorkZone

Explorer User guide (see Automatic Authentication of users fails when accessing WorkZone Explorer through an FQDN host).

You may experience a situation when a WorkZone for Office functionality does not work for no clear reason. Then the reason might be short default timeouts that expire due to slow network connection.

List of issues that may be caused by short timeouts:

- Smart tasks are in the offline state.
- The **Start Process** button is dimmed.
- API methods (for example, opening document, creating a new email and others) do not work.
- The WorkZone for Office add- in is not ready to process the requests.

To fix these issues, you need to increase the default timeouts:

1. Run `regedit.exe`.
2. Go to:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\ScanJour\Clients\Options
   ```

3. Set new values for the relevant registry keys.

Registry key	Default value (ms)	Definition
SmartTaskOfflineTimeOut	3000	When a user opens a smart task, the WorkZone for Office client should connect to the WorkZone Process server during the time specified here. If the time limitation runs out, a notification with an issue description appears.
StartProcessButtonTimeOut	3000	WorkZone for Office should connect to the WorkZone Process

		server during the time specified here. If the time limit runs out, the **Start Process** button is dimmed, and a user sees a tool tip that notifies about the issue.
LocalServiceConnectionTimeout	30 000	When ActiveX sends a request to WorkZone for Office, the WCF service client should connect to the WCF service server during the time specified here.
LocalServiceOperationTimeout	600 000	When ActiveX sends a request to , the WorkZone for Office add-in and the WCF service should execute the request during the time specified here.
OpenApplicationTimeout	30 000	When a user launches the WorkZone add-in, the add-in should get ready during the time specified here.

Issues in Microsoft Outlook 2016 appeared after installing the October 2017 Microsoft Outlook security update (patches KB 4011178 and KB 4011162 respectively).

The security update affects WorkZone for Office case, document and process overview in Microsoft Outlook. To fix this, you must add the following registry settings:

Microsoft Outlook 2016:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security]
"EnableRoamingFolderHomepages"=dword:00000001
```

Find more information here.

Save on Case does not work for appointments and meetings created out of WorkZone for Office.

Save on case crashes if the `DisableCrossAccountCopy` registry setting exists in the registry list. Find more information here and delete the registry setting if it is worthwhile for your WorkZone installation.

Install and configure WorkZone SharePoint

Prerequisite:

- WorkZone SharePoint is supported from WorkZone Cloud Edition only.
- Your organization must use Entra ID.
- The WorkZone SharePoint app must be registered in Entra (see Register WorkZone SharePoint app in Azure).
- WorkZone SharePoint requires WorkZone version 2022.1 or later.

WorkZone SharePoint Connector is designed and tested to work on Cloud- based (Azure) setup with Microsoft Office Online. It is independent from any other WorkZone service, although it connects to WorkZone (OData and OAuth2) and Office Online – SharePoint.

The WorkZone SharePoint architecture consists of 3 parts:

1. WorkZone SharePoint Backend (SpConnector) - is responsible for communication between customer's SharePoint and WorkZone.
2. WorkZone SharePoint Frontend – provides UI for WorkZone components displayed in SharePoint.
3. WorkZone SharePoint package – a SharePoint app to deploy to your SharePoint site. See Microsoft documentation for detailed guidelines.

WorkZone SharePoint Backend (SpConnector)

Backend can be installed on any server.

Prerequisite:

- Network connection must be opened for WorkZone OData, WorkZone OAuth2 and SharePoint Online
- IIS website named WorkZone has to be created
- ASP.NET Core Runtime Hosting Bundle in a version .NET 8.0 or later (delivered with the WorkZone SharePoint Connector) must be installed on the same server as the WorkZone SharePoint Connector

1. Run the SpConnector.Setup.msi file.

- Default installation path:

```
C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\WZSP
```

- Configuration file:

```
C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\WZSP\appsettings.json
```

Parameterless installation leaves configuration values empty, although some settings are required to run the application.

Msi installer accepts the following parameters (case insensitive)

- `USE_HTTP` - default value is false. Enforces HTTPS communication, if true HTTP is allowed.
- `WZ_CLIENT_ID` - ClientID, registered on local WorkZone OAuth2. Required value.
- `WZ_CLIENT_SECRET` - Client secret registered on local WorkZone OAuth2. Required value.
- `WZ_ALLOWED_URLS` - WorkZone server URL (OData).
- `SP_Client_ID` - application that is hosting SharePoint in Azure. Required value.
- `SP_Client_Secret` - secret that allows connection to SharePoint. Required value.
- `SP_Tenant_ID` - Azure tenant where SharePoint is hosted.
- `CORS_Policy` - SharePoint instance URL.

Example:

```
msiexec /i "SpConnector.Setup.msi" WZ_CLIENT_ID=WZSP_Con-
figClient_ID WZ_CLIENT_SECRET=secret WZ_ALLOWED_URLS-
S=https://db01.lmdom.local SP_Client_Id=11b258ae-e076-4fcf-a5cf-
2d6b00134e1b SP_Client_Secret=secret SP_Tenant_Id=a11f8617-45a3-
48a0-a860-2e890e171ea0 CORS_Policy=https://kmddk.sharepoint.com/
```

Additionally, after installing the WorkZone SharePoint, add it to the allowed Cross Origin Resource Sharing (CORS) origins in OData by editing the

```
C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\OData\web.config
```

file on the server with WorkZone. Add the SharePoint instance URL to the existing values under:

```
<add key="allowCorsOrigin" value="[SharePoint instance URL]" />
```

(where "[SharePoint instance URL]" is the actual URL). See **AllowedCorsOrigins** parameter in the Command line configuration for more information about allowing specific origins of the web client to be accessed.

WorkZone SharePoint Frontend

Frontend does not require any specific hosting. It can be hosted anywhere, but must be accessible for SharePoint. Frontend contains only static files that have to be put on the web server. For this reason, there is no installer provided by KMD.

WorkZone SharePoint package

Package is a SharePoint app that you will need to deploy to your SharePoint Online site, as described in the Microsoft guidelines.

The `workzone.sppkg` extention is provided by KMD to each customer/environment separately, as it contains the URL to WorkZone services (WorkZone domain, WorkZone SharePoint Backend and WorkZone SharePoint Frontend).

Upgrade WorkZone SharePoint

If you are upgrading from earlier versions, uninstall the old version of WorkZone SharePoint before installing the new version.

Install and configure WorkZone Teams

Prerequisite:

- WorkZone Teams app is currently supported with WorkZone Cloud Edition only.
- Your organization must use Entra ID.

The installation process consists of three parts:

1. Installing WorkZone Teams on the server.
2. Installing WorkZone Teams on the client.
3. Updating the Cross Origin Resource Sharing (CORS) in OData

Installing WorkZone Teams on the server

WorkZone Teams server- side application is hosted in cloud and deployed by the KMD technicians.

Installing WorkZone Teams on the client

Prerequisite: You must have the `appPackage.zip` app manifest (provided by the KMD technicians).

1. Start Microsoft Teams (either the web version or the desktop version).
2. Upload the WorkZone Teams app. See Upload your custom app in Microsoft Teams article from Microsoft.
3. Publish the WorkZone Teams app to your organization. See Publish your app to your org article from Microsoft.

Updating the Cross Origin Resource Sharing (CORS) in OData

After installing the WorkZone Teams, add it to the allowed Cross Origin Resource Sharing (CORS) origins in OData by editing the

```
C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\OData\web.config
```

file on the server with WorkZone. Add the WorkZone Teams URL to the existing values under:

```
<add key="allowCorsOrigin" value="[WorkZone Teams_URL]" />
```

(where "[WorkZone Teams_ URL]" is the actual URL). See **AllowedCorsOrigins** parameter in the Command line configuration for more information about allowing specific origins of the web client to be accessed.

Upgrade WorkZone Teams

If you are upgrading from earlier versions, uninstall the old version of WorkZone Teams before installing the new version.

Configure WorkZone Explorer

WorkZone Explorer uses WebDAV (Web Document Authoring and Versioning), which is a standard document protocol over HTTP. WebDAV can run over https as well. With WorkZone Explorer, you can manage cases and documents from Windows File Explorer. You can perform common operations on cases and documents such as creating and renaming cases and documents as well as opening, editing, and saving documents directly into WorkZone from a document editor that supports the WebDAV protocol, for example, Microsoft Office or Notepad.

> **Note:** WorkZone Explorer is part of the WorkZone installation. Note that it is not required to install a client, such as WorkZone Client.

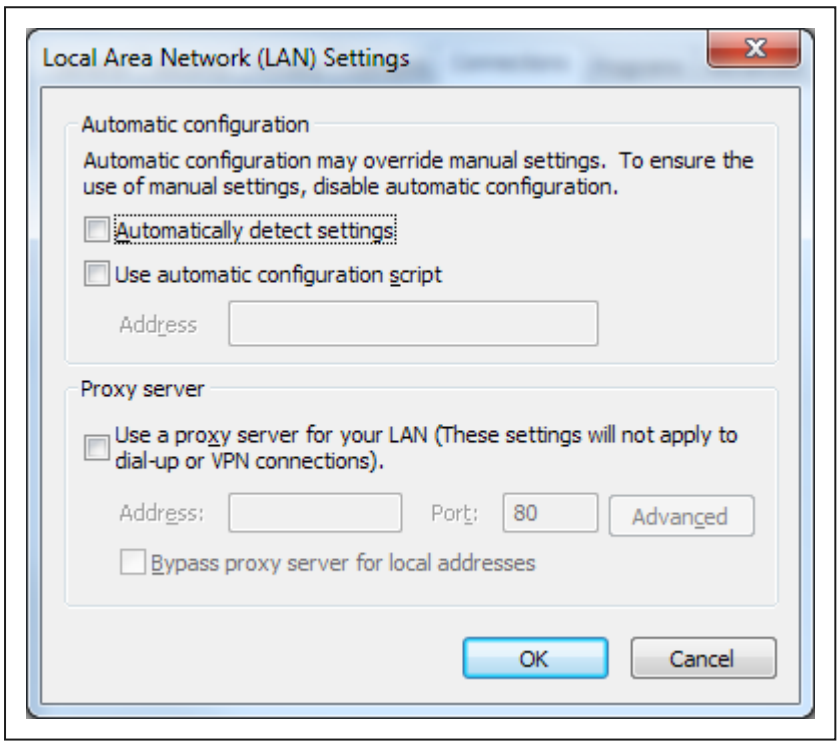
Optimizing performance and user experience

To ensure optimal performance and user experience of WorkZone Explorer, you can apply specific configurations to clients and/or to the network/domain.

LAN Automatically detect settings

If navigating the WorkZone Explorer folders is slow, make sure that the **Automatically detect settings** check box in the **Local Area Network (LAN) Settings** dialog box is cleared on the client.

To open the **Network (KAN) Settings** dialog box in Internet Explorer, click **Tools** > **Internet options** > **Connections** tab > **LAN Settings**.



Internet security zones

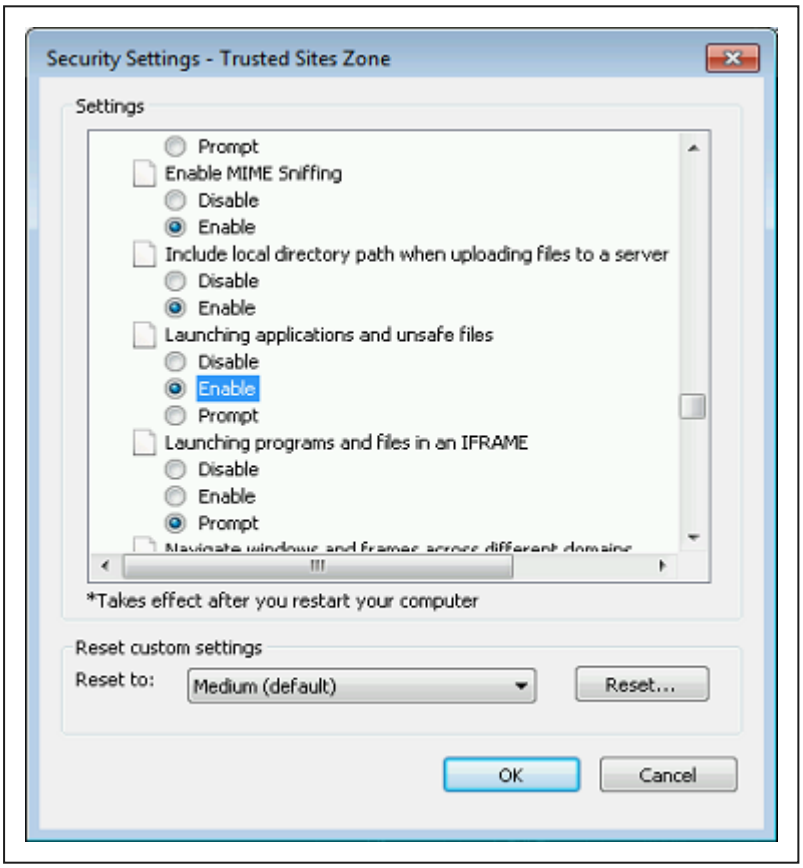
The WebDAV protocol is based on http, can run over https, and Internet Security zones therefore apply to WorkZone Explorer. To ensure the best user experience and optimal performance, the WorkZone Explorer host name must be configured correctly in the Internet Security Zones.

1. In Internet Explorer, click **Tools** > **Internet options** > **Security** tab.
2. Add `https://webdavhost` to either the **Trusted sites** zone or the **Local intranet** zone.

The **Local intranet** zone must be selected in order to have automatic integrated user authentication performed by Windows without **Log on** dialog boxes.

3. Add `file://webdavhost` to the **Trusted sites** zone.

   If the file protocol is added to the **Local intranet** zone, poor search performance or display of search results may result when using the search connectors for searches. In some cases, you might receive a security warning when opening a document folder location from a search result or when moving documents from the **Recycle Bin** to the **Restore** folder. If you want to avoid these security prompts, enable **Launching applications and unsafe files** for **Trusted Sites** zone.



Windows 11 File Explorer integration to WorkZone Cloud

If you use Windows 11 and WorkZone Cloud Edition, follow the steps below to enable the Windows File Explorer integration.

1. Make sure that you have set Internet Security Zones correctly. See Optimizing performance and user experience.
2. In Microsoft Edge, go to **Settings** > **Default browser** and set:
    - The **Let Internet Explorer open sites in Microsoft Edge** option to **Incompatible sites only (Recommended)**,
    - The **Allow sites to be reloaded in Internet Explorer mode (IE mode)** option to **Allow**.
    - Under **Internet Explorer mode pages**, click **Add** to add the URL of the WorkZone Explorer page. For example, `https://k-md.workzone.cloud/explorer` and `https://k-md.workzone.cloud/explorer/`.

    You can use a group policy to roll out the Edge setup in an organization.

Advanced features

Permanent links

It is possible to make permanent links to any document or case in the archive. These links are available through a hidden folder called " .archive" . All you need to know is the DNS, the ID, and the file extension, and then you can open any document using following address:

```
https://[WorkZoneHost]/.a/WhateverYouWant (D[RecordKey]).[Extension]
```

This mechanism can also be used to generate permanent links to documents.

You can also show cases through the.archive folder by using:
`https://[WorkZoneHost]/.a/WhatEverYouWant (C[FileKey])`

View error messages

Sometimes WorkZone Explorer does not show user friendly and descriptive error messages from the WebDAV server in case of errors or illegal operations. See FAQ.

If you want to see the real error from the system, you can use Fiddler on the client and, in this way, see the actual response and error from the server.

Run WorkZone Explorer on a Windows Server

It is not possible to access clients or services directly from the web server.

> **Tip:** For information on how to enable access from the web server, search for "kb 896861" on **Microsoft Docs.**

If you want to run WorkZone Explorer from Windows File Explorer on a Windows Server operating system, you must also enable the Windows feature called **Desktop Experience**.

Troubleshooting

Click an issue below to see the solution or workaround.

Automatic Authentication of users fails when accessing WorkZone Explorer through an FQDN host

If you access WorkZone Explorer through an FQDN host name, automatic Windows user authentication will not work. An error message will occur or the Windows **Logon** window will be displayed repeatedly.

To make the logon happen automatically, add the https address for the WorkZone Explorer host to the Windows registry named **AuthForwardServerList**. For example: `https://db01.lmdom.local`. After you have modified the registry, you have to restart the WebClient service.

You can find information on how to make this change in the registry in the Microsoft article Prompt for credentials when you access WebDav- based FQDN sites in Windows. Follow the instructions listed under **Registry information** in the **Resolution** section.

> **Note:**

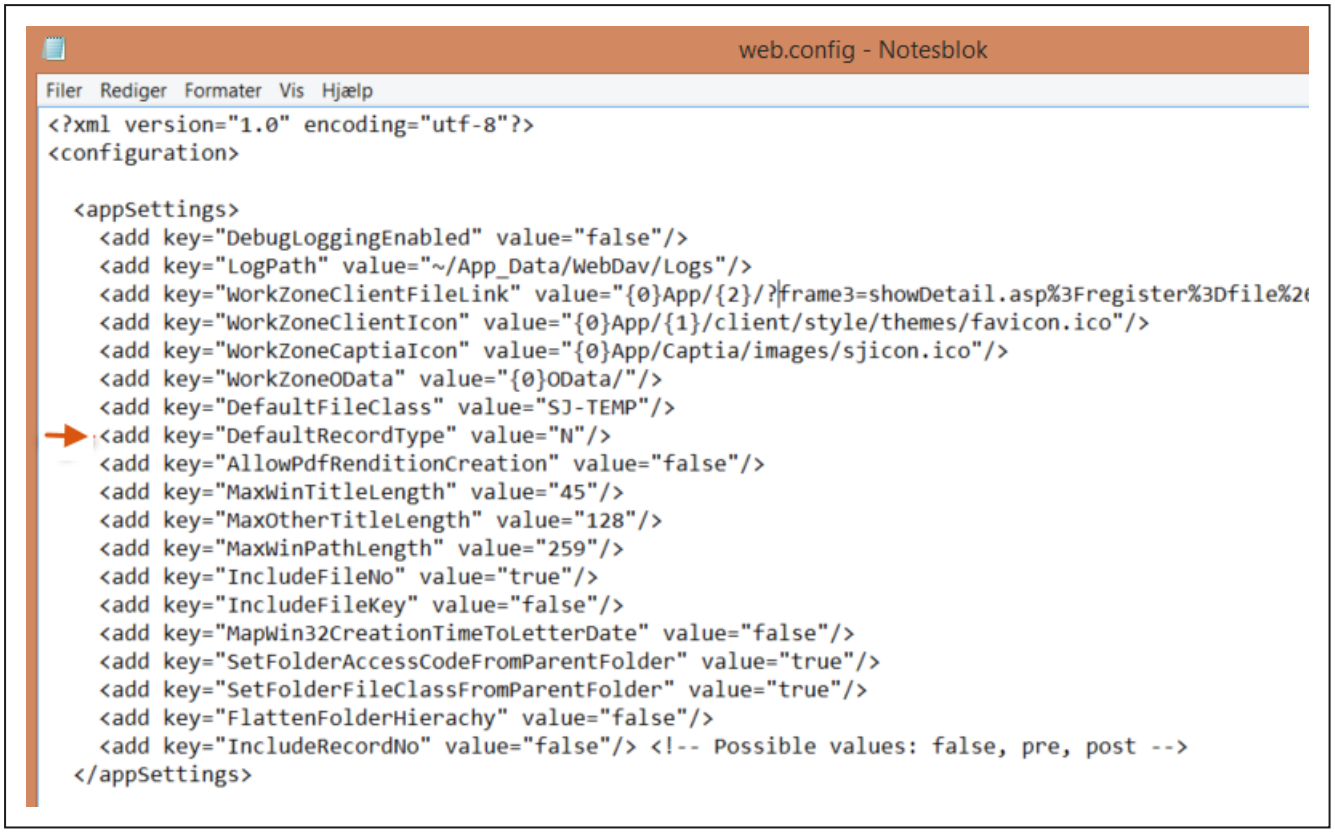
- You do not need to install the hotfix mentioned in the Microsoft article.
- The hotfix mentioned in the Microsoft article is included in Windows 8, although Windows 8 is not listed in the **Properties** section.

Users get an error message when they try to create documents in WorkZone Explorer

If users get an error message when they try to create documents in WorkZone Explorer, it is probably because the document type **N** (Internal) does not exist. WorkZone Explorer requires that the document type **N** is created and that the `DefaultRecordType` parameter is set to **N** in the web.config file. Check if this document type has been created in WorkZone Configurator and in the WorkZone web.config file.

1. In WorkZone Configurator, go to **Document** > **Properties** > **Document types**. If the document type **N** does not exist, create it. See Create a property.
2. Check if the parameter `DefaultRecordType` is set to **N** under `<appsettings>` in the WorkZone `web.config` file, which is located in `C:\Program Files (x86)\KMD\Workzone\IIS\Workzone\Explorer`. If this is not set to **N**, spe-

cify it as shown below.



Cannot download more than 50 megabyte or upload large files

WorkZone Explorer is based on Microsoft WebDav to open and edit files (documents) and is restricted by any default values defined for the WebDav extension. You can edit the default values to improve performance when working with large files.

See customize the web client in the registry (external link to Microsoft support) The information is relevant for the Windows 7 and Windows 10 operating systems.

Configure Citizen Access

WorkZone Citizen Access allows citizens to access their own cases and documents that are saved in WorkZone. Citizens identify themselves with a digital ID in an external client, portal, or form and will then get access to specific cases and documents.

About Citizen Access

Note: This is the first release of WorkZone Citizen Access. The release contains a basic set of features.

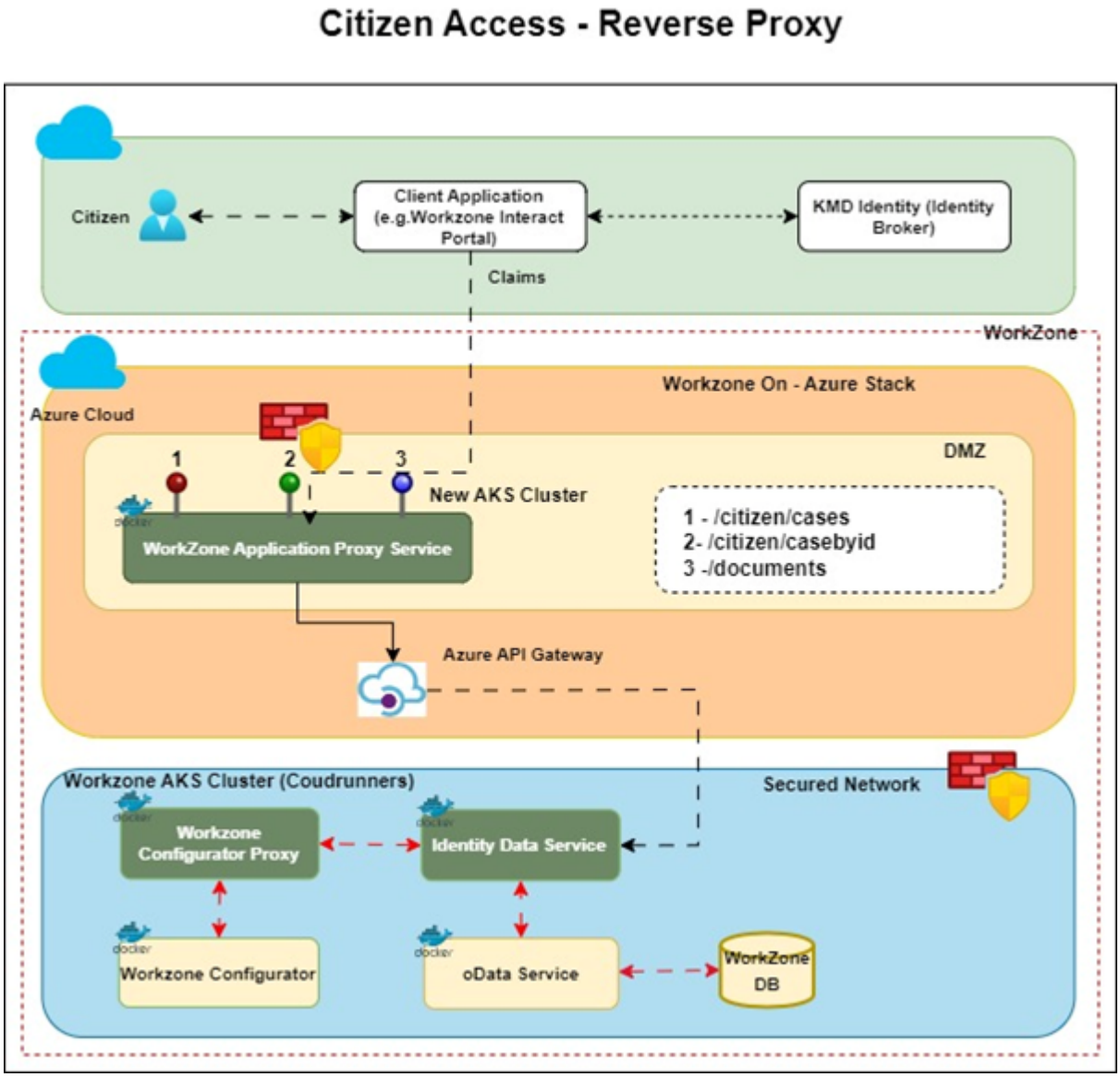
With WorkZone Citizen Access citizens can view the meta data of specific cases and documents that are saved in WorkZone even if the citizens are not registered as WorkZone users. Citizens must log in with a digital ID in a client, a portal, or a form and will then get access to view the meta data of specific cases and documents that they have been granted access to. In this release, it is not possible to view or download documents.

- **Portal integration** – You can build specific applets or forms as marked cases and documents that allow non WorkZone users to access "My cases" or "My documents".
- **WorkZone Interact integration** – You can create an Interact form that selects cases and documents that are relevant to a citizen's inquiry, for example, a selection of documents.

As an example, a Danish citizen can access WorkZone data by logging into an Interact form with MitID (the Danish digital ID). When a citizen logs in with MitID credentials, a request is redirected to the KMD Identity for authentication and post authentication. The Interact form gets the user claims from the KMD Identity and then passes the claims to the WorkZone Application Proxy Service to communicate with Identity Data Service to retrieve the meta data of cases and documents.

Architecture

The diagram below shows the architecture of the Citizen Access module.



Authentication

MitID authentication

Cititizens in Denmark will log in to a client/form/portal for authentication using MitID credentials.

Azure authentication

Azure authentication is used to authenticate the request coming to the OData Service by using Azure App Client ID and Secret.

Components

WorkZone Application Proxy Service

WorkZone Application Proxy Service is an endpoint for customers to consume WorkZone data using WorkZone Identity Service (IDS). This Service exposes the endpoints for other applications such as Workzone Client Application (UI for authentication), WorkZone Interact , or any other third- party provider who wants to consume this service to access WorkZone data.

This service is a containerized service that is deployed in Azure AKS using DevOps pipelines. Post authentication of citizens, this service is called by providing the end user claims details with the required payload/input parameters. Also, WorkZone Application Proxy Service sends a request to Azure API Gateway.

The endpoints can provide the information that belongs to the citizen such as listing the cases, case details, and documents associated with the case.

WorkZone Identity Data Service (IDS)

This is the proxy service for OData Service (Containerized). This service is called by Azure API Gateway to interact with the OData Service by providing the required input parameters such as Authentication token, external ID (MitID), and the query parameters to the OData Service to retrieve the data and will send the response back to WorkZone Application Proxy Service.

The WorkZone Identity Service provides:

- Restricted access to WorkZone data for external contacts.
- Standard integration to MitID with a later option for other providers.
- Secure access to data via reverse proxy.
- Only access to cases with marked access for contacts.
- Logging of data access via the WorkZone use log.

You can use WorkZone Identity Service in different integrations.

Demilitarized Zone (DMZ):

A DMZ or demilitarized zone is a perimeter network that protects and adds an extra layer of security to an organization’s internal local- area network from untrusted traffic.

The main benefit of a DMZ is to provide an internal network with an advanced security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization's private network.

WorkZone Application Proxy Service will be deployed in the DMZ with two firewalls. A firewall while accessing the WorkZone Application Proxy Service and a second firewall while accessing IDS.

Configure Citizen Access

This topic describes how to configure the applications that are required to run WorkZone Citizen Access.

> **Prerequisite:** To run WorkZone Citizen Access, you must first enable the **WorkZone Citizen Access IDS enabled** feature in WorkZone Configurator. Go to **Global** > **Feature settings** > **WorkZone Citizen Access**.

To run WorkZone Citizen Access, you need the following applications:

Application	Deployment	Comments
Test client	Locally	An app that you can use to access the Citizen Access module. You must configure the app locally.
WorkZone Application Proxy	AKS	Deploy to AKS as a container.
API Management	Azure	Configure in Azure.
WorkZone Identity Data Service (IDS)	AKS	Deploy to AKS as a container.

See also the Architecture diagram.

> **Prerequisite:**
>
> Before you can configure Citizen Access the following prerequisites must be fulfilled:

- The test client application URL must be registered with KMD Identity.
- Valid security details to authenticate from KMD Identity.
- Required access to configure the Azure API Management service.
- Required access to Azure Key Vault to read and update the keys.
- Access to run the PowerShell.
- Access to Citizen Access repo.
- Access to Citizen Access Client Application build artifact.
- WorkZone products must be deployed and able to access OData.
- Docker Desktop must be installed locally and must be able to build Linux images.

Configure the test client

The test client is an app that can be used for testing that citizens can log in with their digital ID. It's a web application that can be hosted in any Windows-based environment.

Prerequisite:

- .NET 8.0 Runtime installed on the host operating system.
- ASP.NET Core Runtime 8.0 installed on the host operating system.
- Development certificate installed on the host operating system. See the Microsoft article Generate self-signed certificates with the .NET CLI.
- Unused port number 44375 on localhost (or different one configured with KMD Identity).

Fetching the artifacts

1. Get the latest build files from the pipeline [Citizen Access Client App] (https://dev.azure.com/workzone- kmddk/WorkZone/_ build?definitionId=3147).

   Artifact name: `ClientBuild`

   File name: `Source.zip`

2. Extract files from `Source.zip`

3. Remove the `appsettings.Development.json`, and `appsettings.Production.json`` files.

Setting up the app

Replace the `appsettings.json` content with following snippet. The configuration gets data from WorkZone Citizen Access that is hosted on Dev- AKS.

```
              insert{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*",
  "Urls": "https://localhost:44375", // url on which application is running, must be configured with KMD Identity
  "Security": {
    "IdPMetadataUrl": "https://identity.kmd.dk/adfs/.well-known/openid-configuration",
    "ClientId": "", // ClientId for KMD Identity
    "ClientSecret": "", //Client Secret for KMD Identity
    "ApiScope": "allatclaims user_impersonation",
    "RequestDetailsApiUrl": https://<domain>/appproxyservice/api // Application Proxy API URL
  }
```

```
}
```

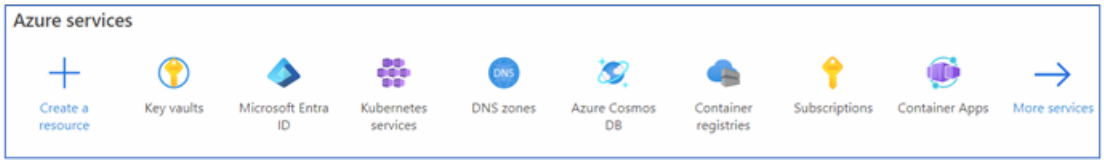
Running the test client

Open shell in folder containing sources and run `KMD.Workzone.CA.IdentityClient.exe`.

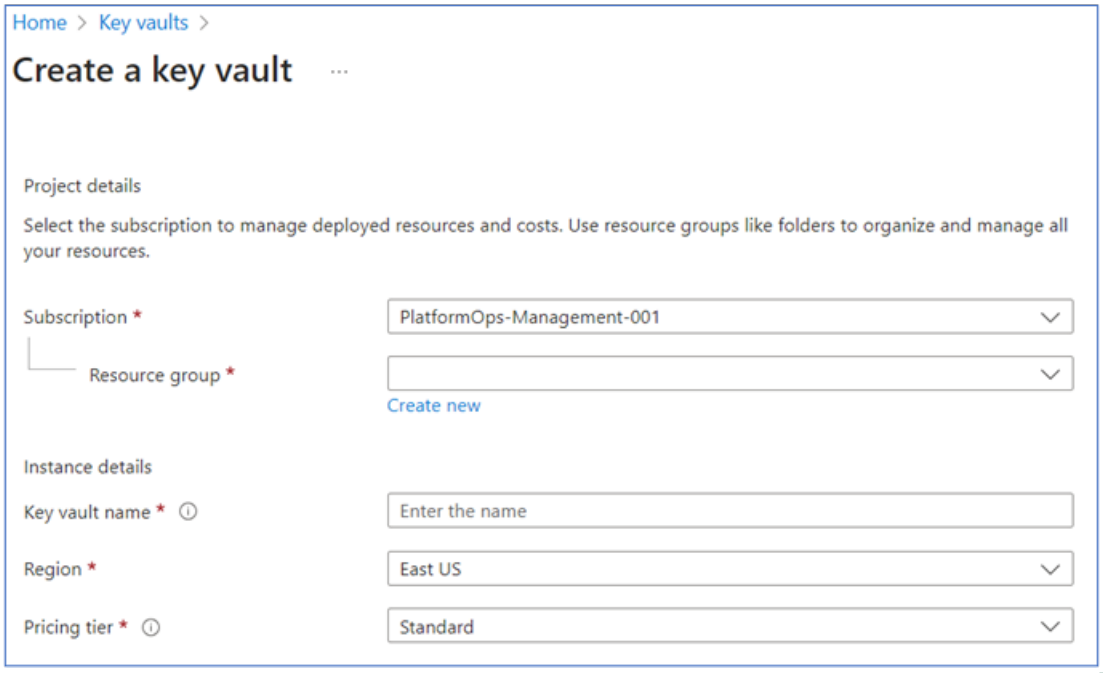
Configure Azure Key Vault

The key value configuration is required to store the keys so that the key will be sent as a header and validated in IDS.

1. In the Azure portal, select **Key vaults**.

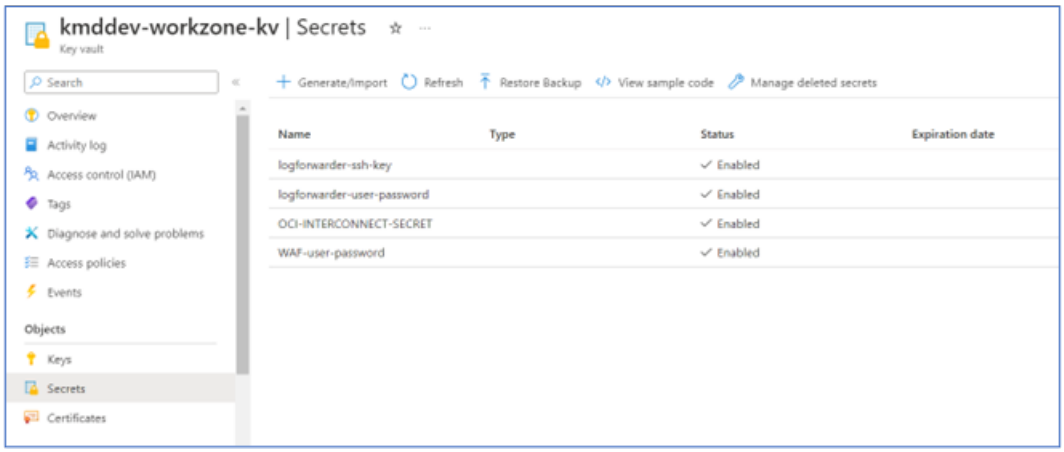


2. Create a new key vault by choosing a resource group, and fill in information in the **Instance details** section.

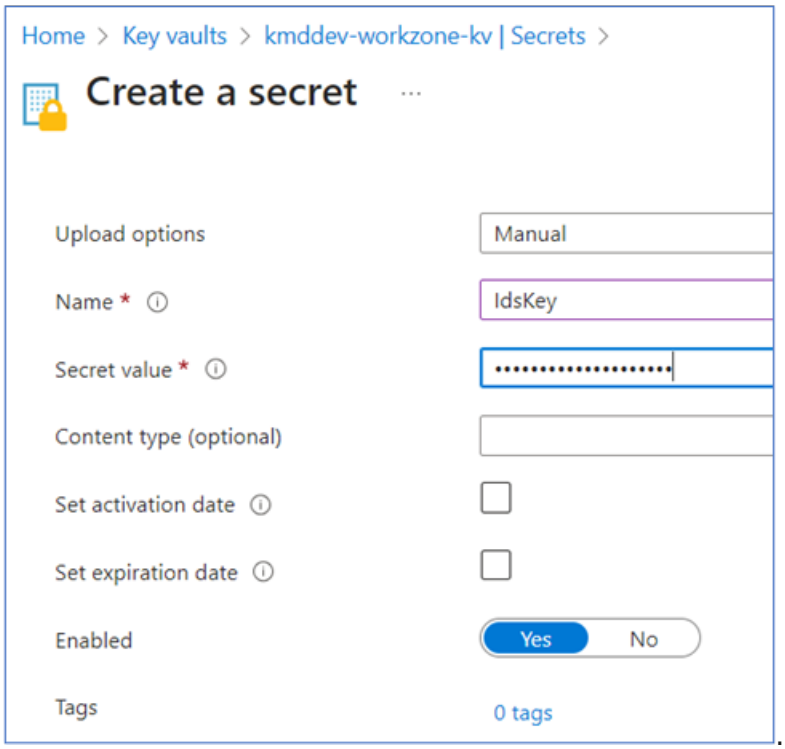


3. Click **Review + create**.

4. Select the key vault that you just created to create secrets.



5. Select **Generate/Import** to create a new secret. In this example, create a secret named *IdsKey* and enter a secret value, and then click **Create**.



Create an Azure AKS instance

1. In the Azure portal menu, select **Create a resource**.
2. In the **Search** box, enter **Kubernetes Services**, and then select **Kubernetes Services**.
3. On the **Basics** tab, fill in the following fields on :

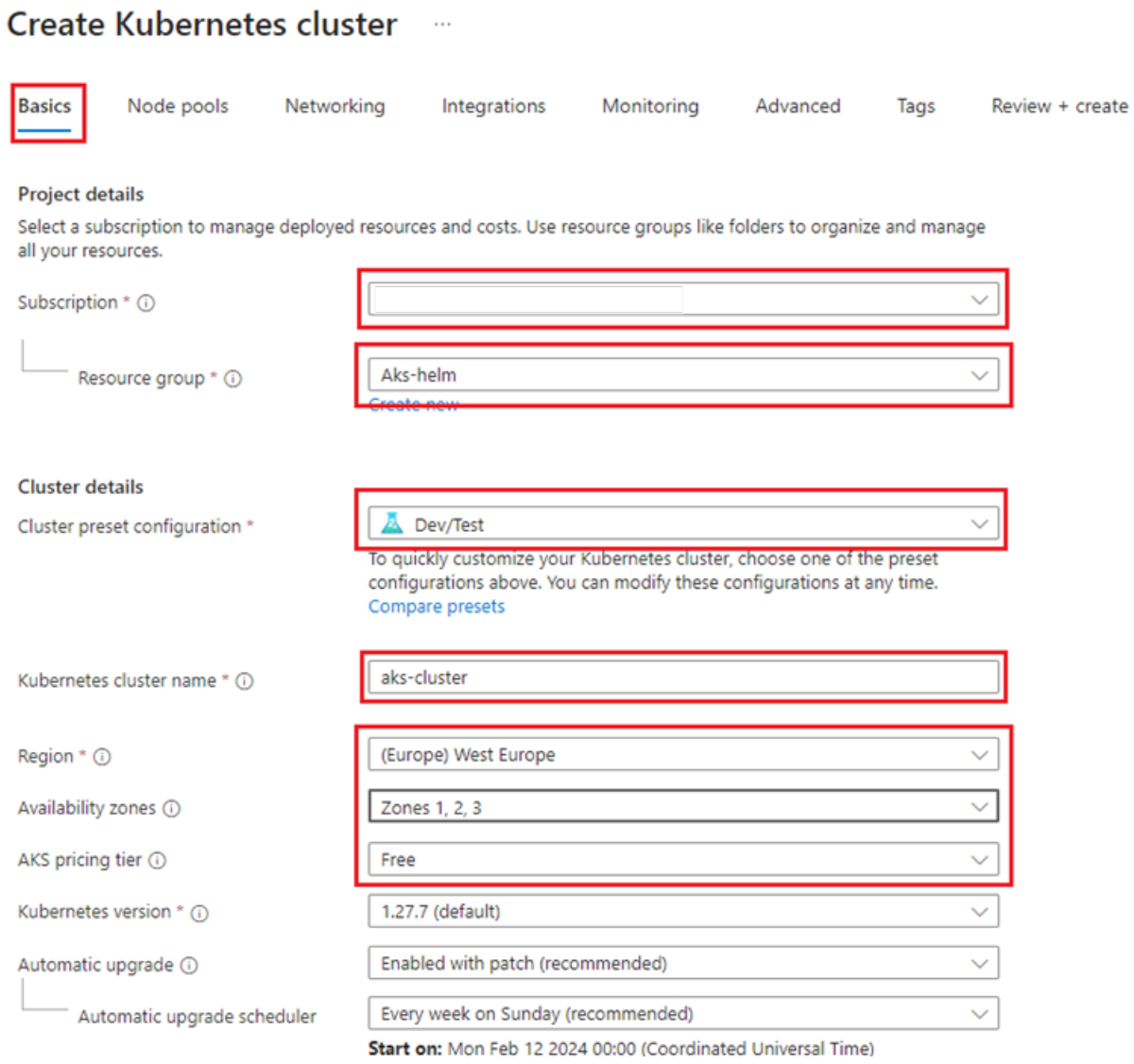
   Under **Project details**:

   - Select the subscription.
   - Select a resource group in the **Resource group** field. If the resource group does not exist, click **Create new** and enter a resource group name.

   Under **Cluster details**:

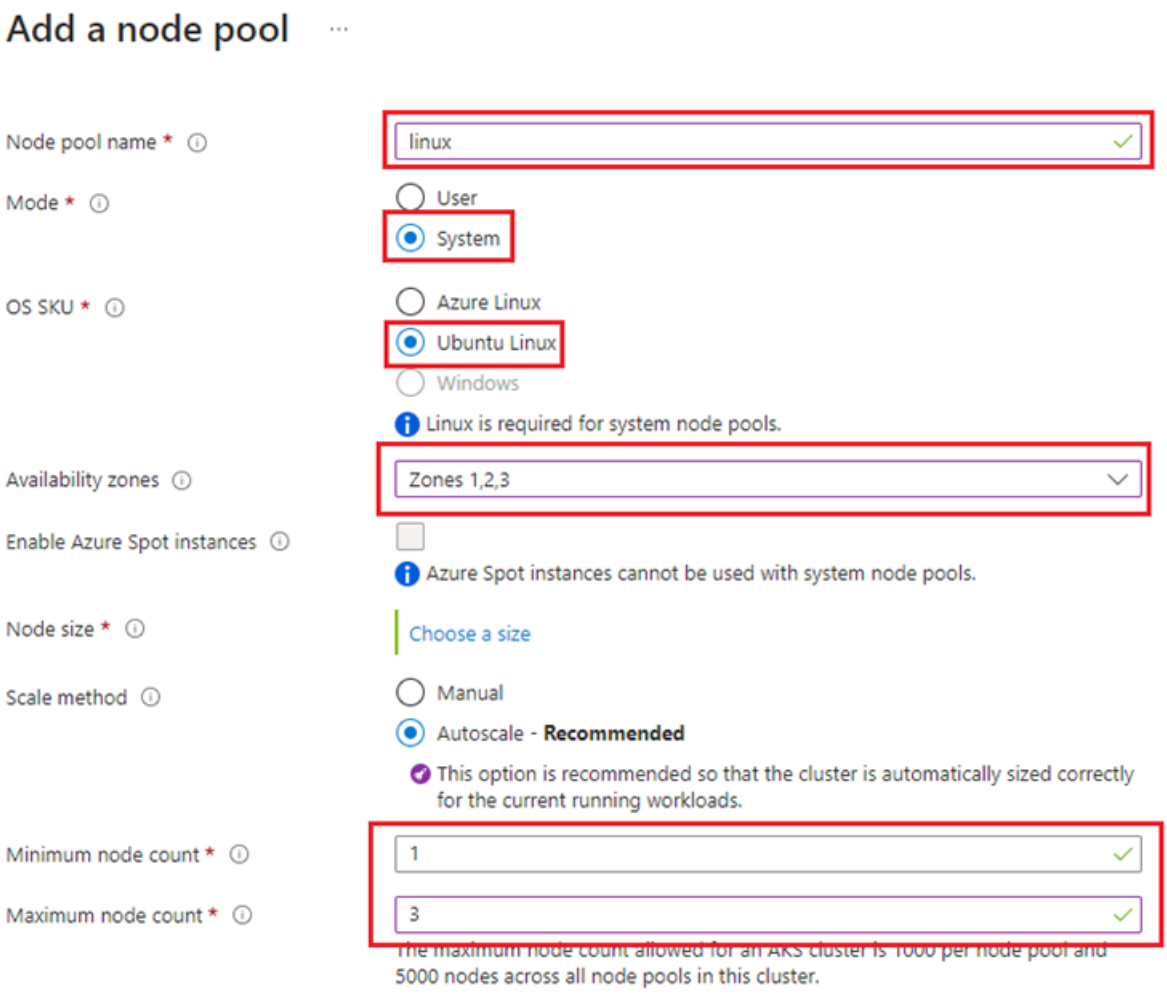
   - In the **Cluster preset configuration** field, select **Dev/Test** for development, testing, or demo purposes.
   - Enter a name for the Kubernetes cluster
   - In the **Region** field, select a region for the AKS cluster.
   - In the **Select Availability zones**, select **Zone 1, Zone 2 and Zone 3**.
   - In the **AKS pricing tier** field, select **Free** for development, testing, or

demo purposes.



4. On the **Node pool** tab, click **Add new node pool**.

5. Enter a name for the node pool and fill in the settings as shown below:



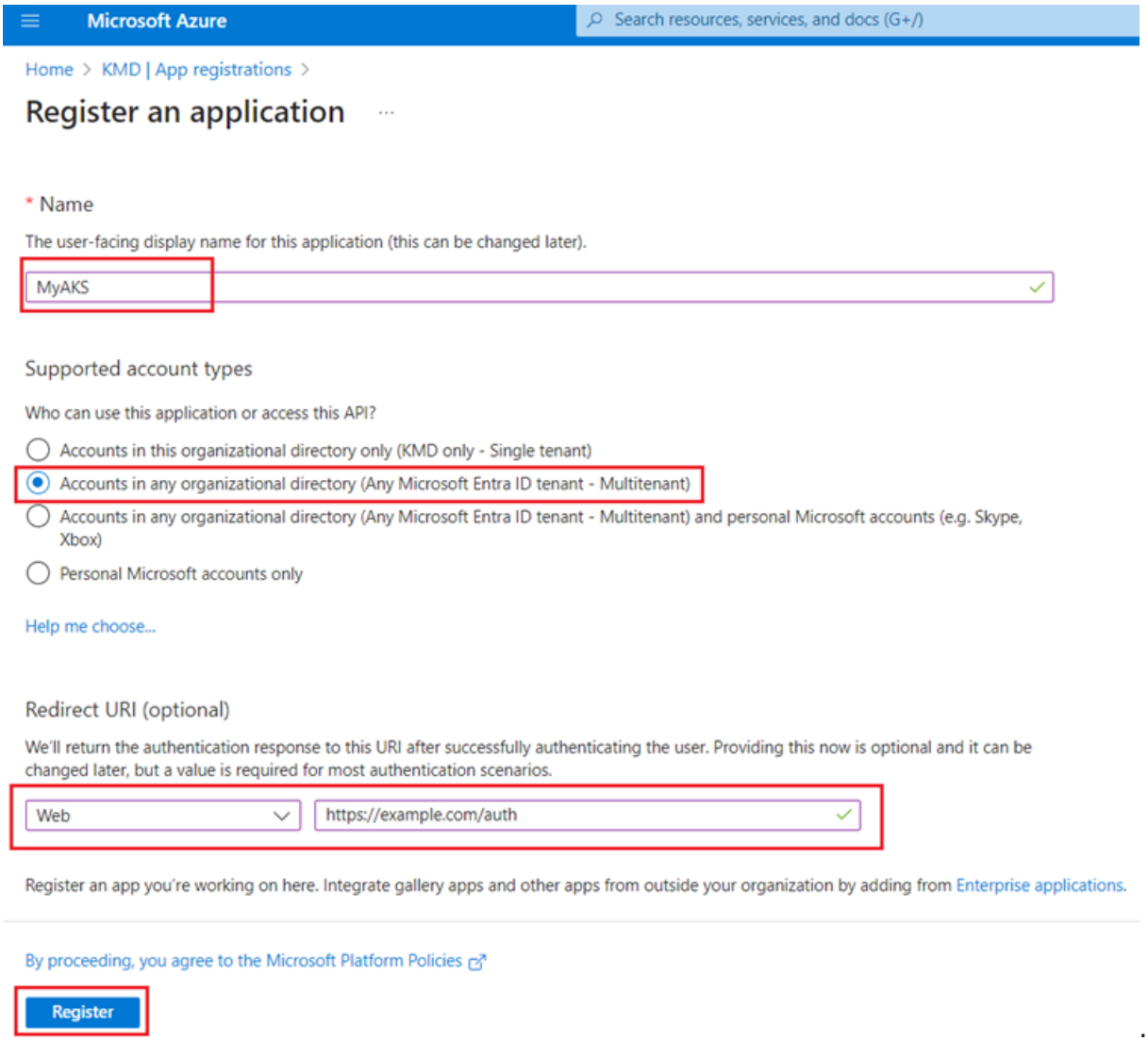
> **Note:** Select the 3 in the **Maximum node count** field for for development, testing, or demo purposes.

6. Click **Add**.
7. Click **Review + create** tab.
8. Client **Create**.

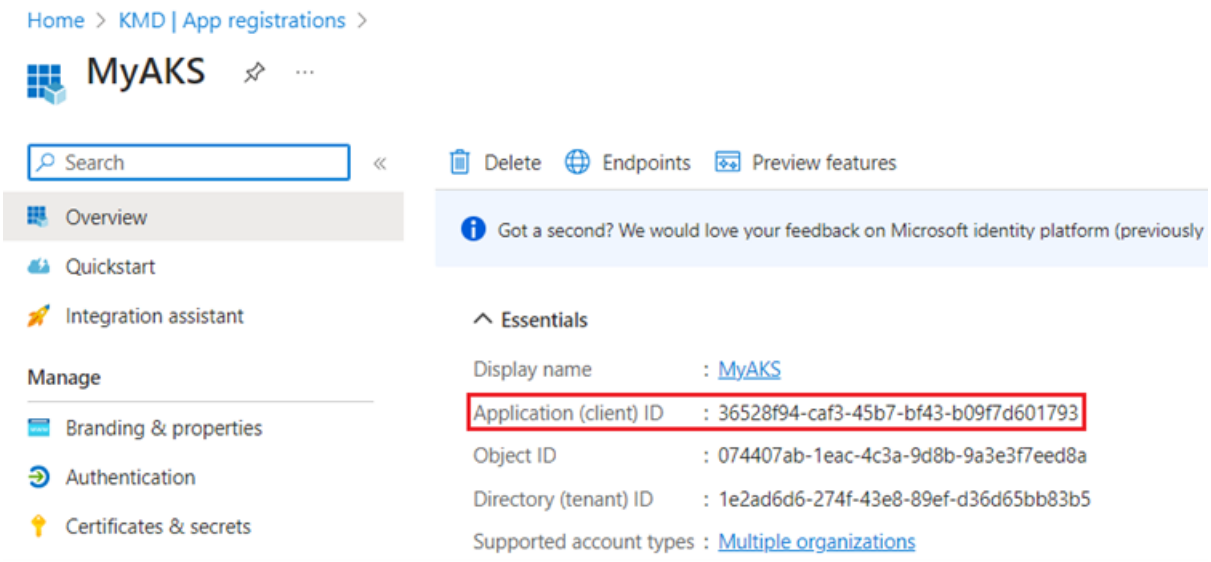
Create a multitenant Microsoft Entra application

You need to create a service principal to get access to pulling images from WorkZone ACR. Follow below steps below to configure a service principal in Azure Entra ID.

1. In the Azure Portal menu, select **Create a resource**.
2. In the Search box, enter **Microsoft Entra ID**, and then select **Microsoft Entra ID**.
3. Under **Manage** in the menu, click **App registrations** > **New registration**.
4. Enter the name of the application (the service principal name).
5. Under **Supported account types**, select **Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)**.
6. Under **Redirect URI (optional)**, select **Web**, and enter any URL. If you have an authentication endpoint for your organization that you want to use, enter it here. Otherwise, you can enter https://example.com/auth.
7. Click **Register.**

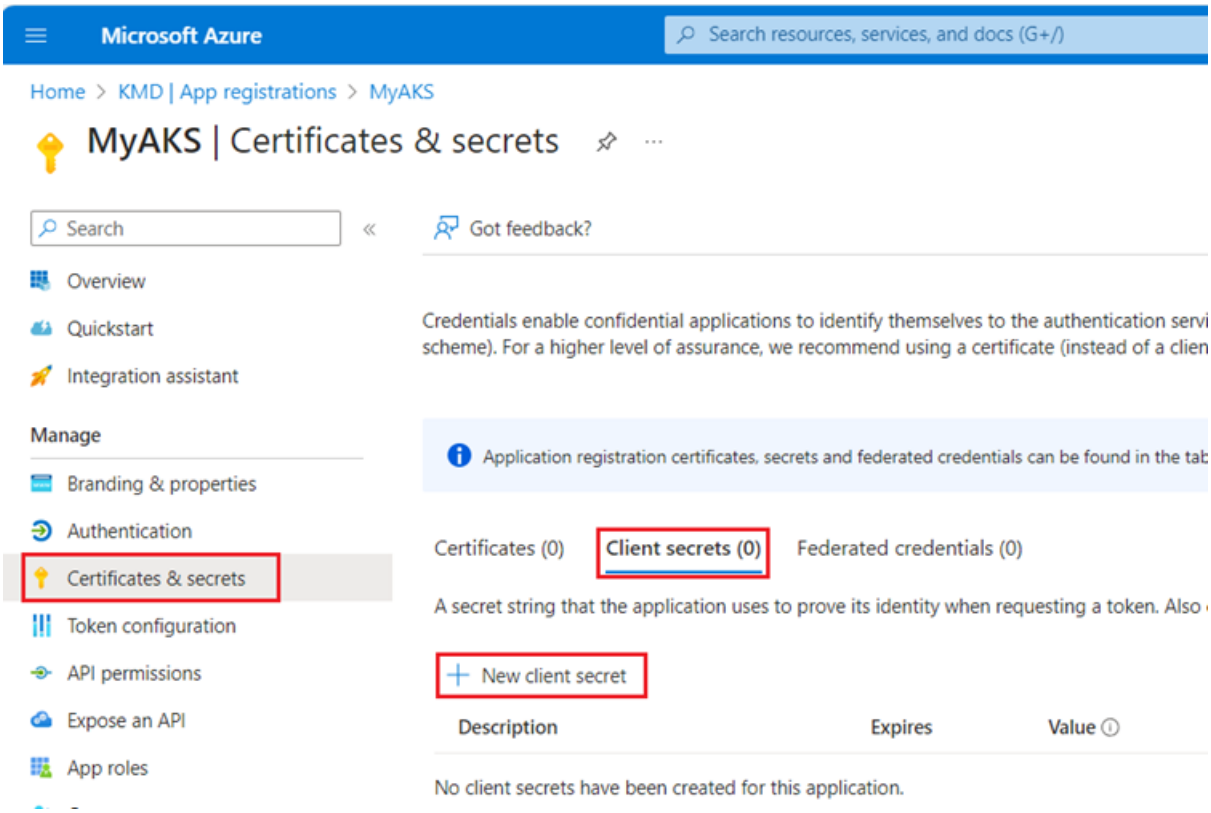


8. Copy the **Application (client) ID**.

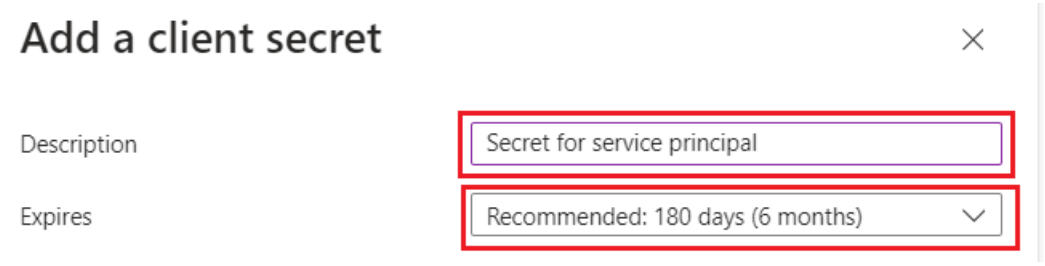


9. Under **Manage** in the menu, click **Certificates & secrets**.

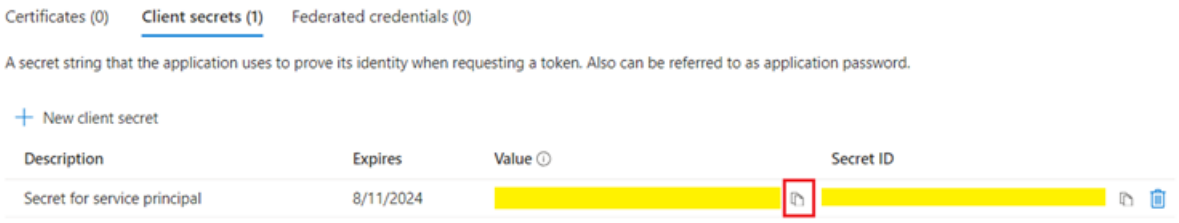
10. Go to the **Client secrets** tab and click **New client secret**.



11. Enter a description, for example *Secret for service principal*, and select when the client secret should expire as per your standards. Click **Add**.



12. Copy the client secret value by clicking on copy icon. You will need it to update the AKS cluster's service principal.



> **Note:** You cannot copy the secret later.

Provision the service principal in the ACR tenant

Follow the below steps to provision the service pincipal in ACR tenant. If you do not have access to provision, you can please send a request to WZ DevOps team by sharing the APP/Client ID, App (Display) Name, and the redirect URL.

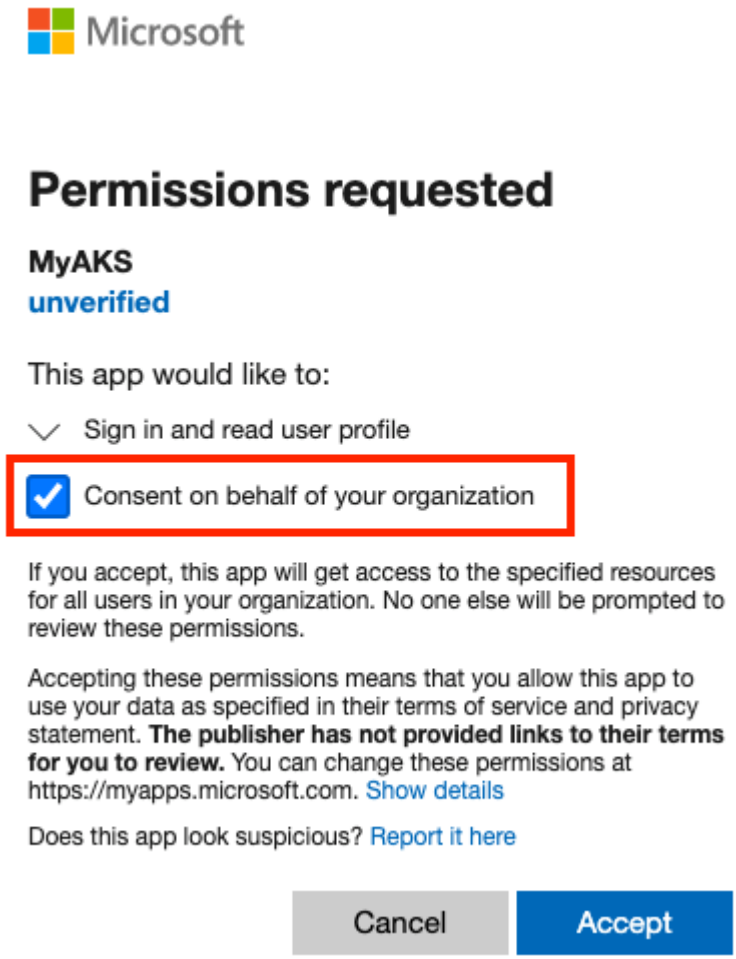
1. Open the following link using an admin account in the ACR tenant. Where indicated, insert the ID of the ACR tenant and the application ID (client ID) of the multitenant app which was created in Service Principal Configuration.

   ```
   https://login.microsoftonline.com/<ACR Tenant ID>/oauth2/authorize?client_id=<Multitenant application ID>&response_type=code&redirect_uri=<redirect url>
   ```

   See Create a multitenant Microsoft Entra application.

2. In the **Permissions requested** window, select the **Consent on behalf of your**

organization check, and click **Accept**.



Grant the service principal permission to pull from Registry

Follow the below steps to grant the service principal in the ACR tenant with AcrPull role.

1. Log in into the Azure Portal.
2. Go to **Container Registry**, and click **Access control (IAM)**.
3. Click **Role assignments**, select the service principal, and assign the **AcrPull** role.

Update AKS with the Azure Microsoft Entra ID application secret

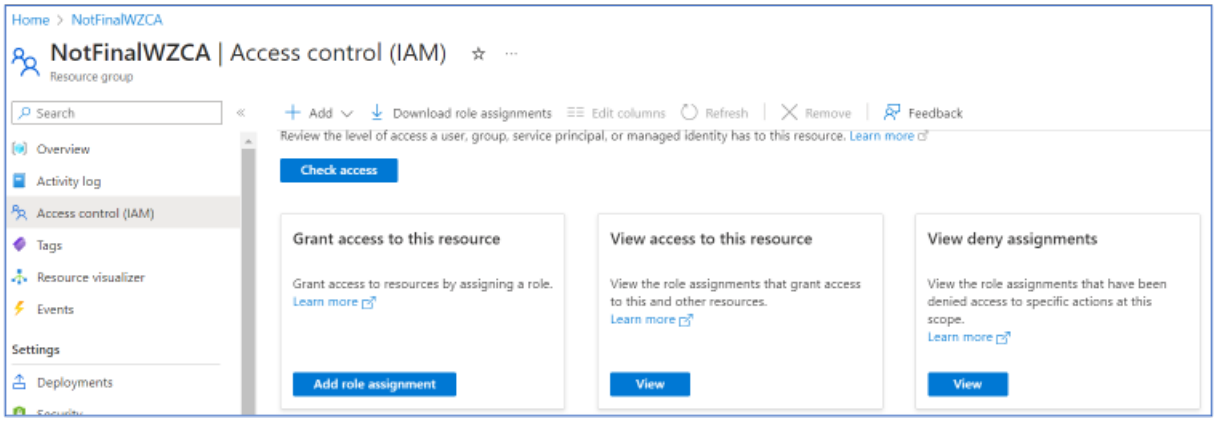
In the tenant where you created the service principal, run the command to update the AKS cluster with the service principal credentials:

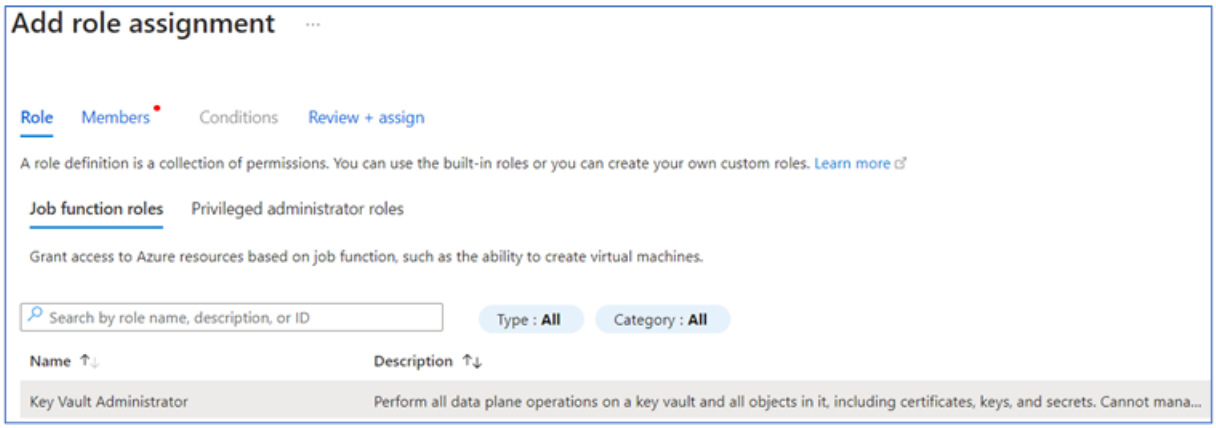
```
az aks update-credentials --resource-group <resource group name> --name myAKSCluster --reset-service-principal --service-principal "$SP_ID" --client-secret "${SP_SECRET}"
```

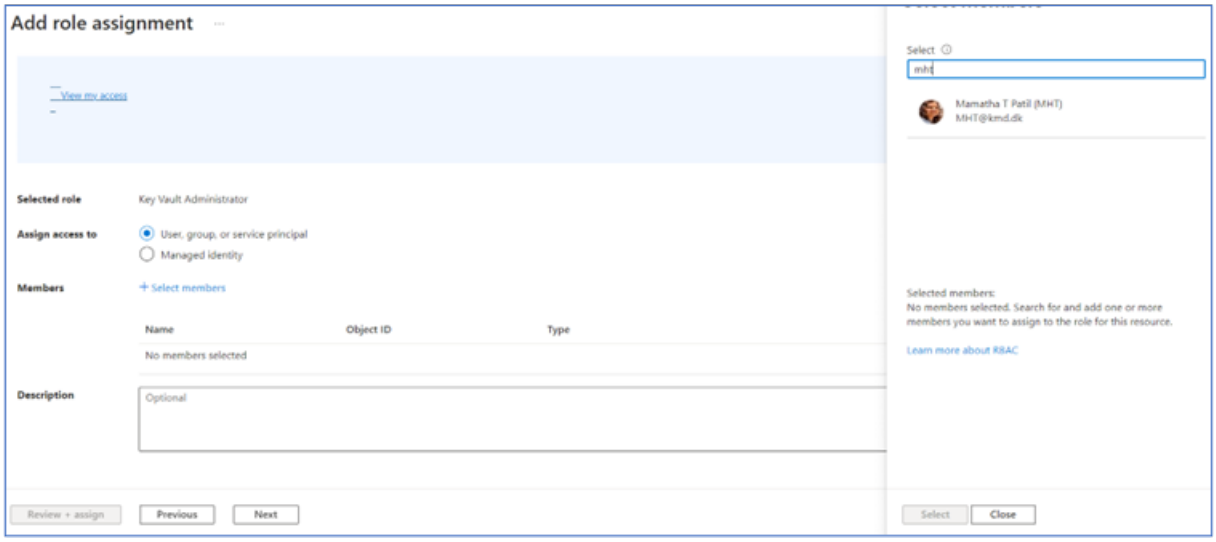
Configure Azure API Management

Follow the below steps to configure the Azure API Management.

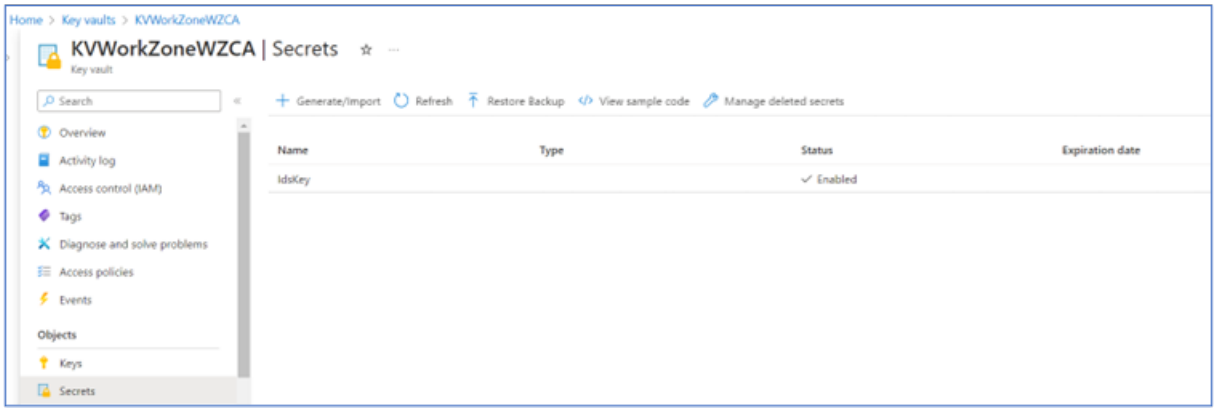
1. In the Azure Portal menu, select **Create a resource** to create a new resource group by providing a name and the location.
2. Add administrator rights to key vault for a specific (logged- in) user.







3. Go to **Key vaults**, and create a new key vault with the secret name **IdsKey** and the value: <secret value>. The value must be the same as ApiSettings.Key in IDS.



4. Copy files below from the CitizenAccess Repo under the folder Source/ApiManagement.

    - Deploy.ps1
    - Parameters.json
    - Template.json

    In the parameters.json file, the names for the API- Management deployment are predefined. You can change the names if needed.

The name of Api- Management service must match the parameter while executing the deploy.ps1 file.

5. Execute the Deploy.ps1 file to create an API- Management deployment.

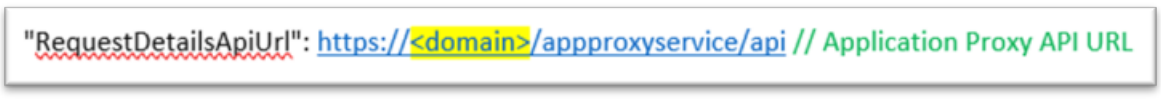
   a. `./deploy.ps1 <resource group name> <api-management service name>`

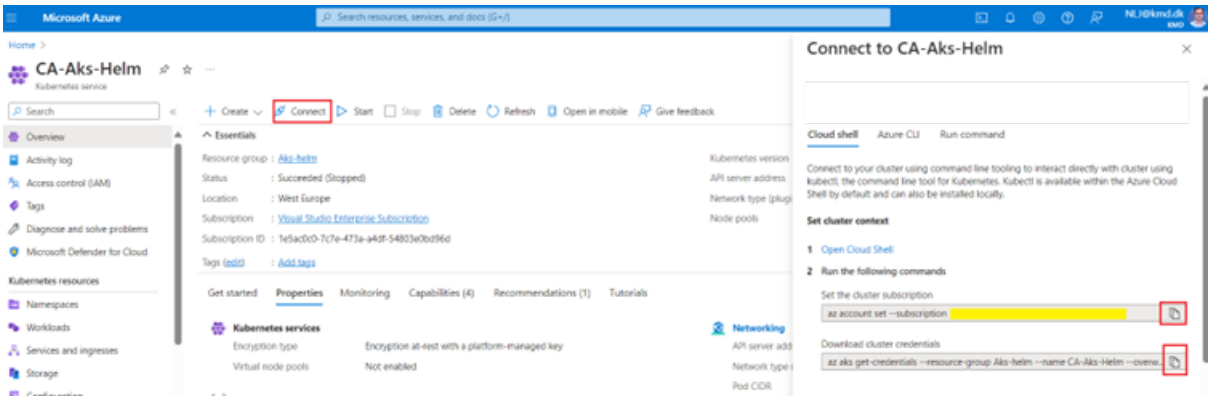
6. When completed, validate it through Postman.

Configure application proxy

Follow the below steps to configure the Application Proxy Application.

1. Log into Azure Portal where the service principal is created.
2. Click **Show Portal Menu** > **All resources**.
3. Click the Kubernetes services that were created earlier.
4. Click **Connect**, and copy the commands from the right- side window.
5. Once the pod is deployed, update the application proxy url in the client application in appSettings.json file.



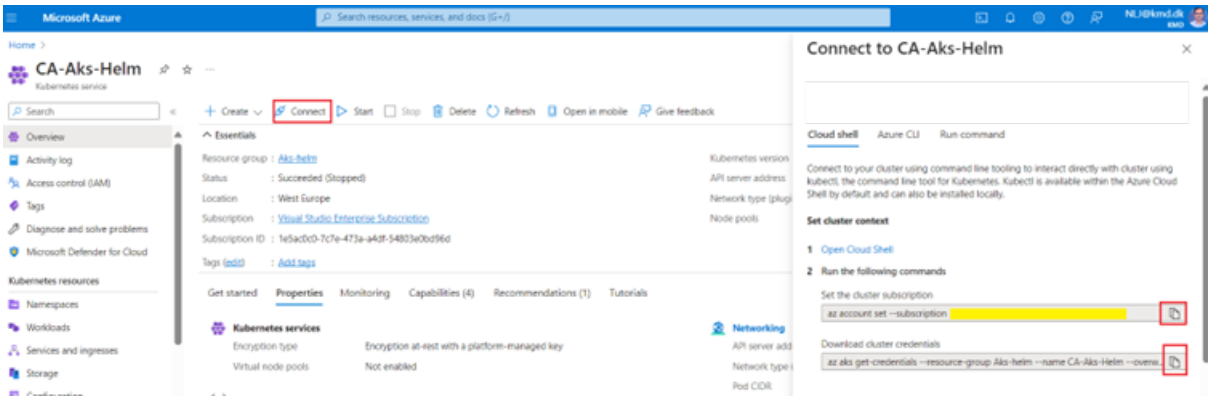


6. Execute the commands that you just copied in PowerShell in administrative mode.
7. Run the command:

```
kubectl run appproxyservice --image-
=wzco-
mmon-
weuac-
r.azurecr.io/workzone/wzcitizenaccess/appproxyservice:latest
```

Configure IDS

1. Log into Azure Portal where the service principal is created.
2. Click **Show Portal Menu** > **All resources**.
3. Click the Kubernetes services that were created earlier.
4. Click **Connect**, and copy the commands from the right- side window.



5. Execute the commands that you just copied in PowerShell in administrative mode.
6. Run the command:

```
kubectl run ids --image-
e=wzcommonweuacr.azurecr.io/workzone/wzcitizenaccess/ids:latest
```

Helm chart changes

In Power Shell, run the command:

```
helm upgrade workzone --values values.yaml --set workzone.wzcit-
izenaccess.ids.url=https://wzcitizenaccess-ids/ids --set workzone.wzcit-
izenaccess.appproxy.url=https://wzcitizenaccess-
appproxyservice/appproxyservice --set
workzone.wzcitizenaccess.appproxy.apiGatewayUri=https://<APIM url> --set
workzone.wzcit-
izenaccess.appproxy.openIdUrl=https://identity.kmd.dk/adfs/.well-
known/openid-configuration
```

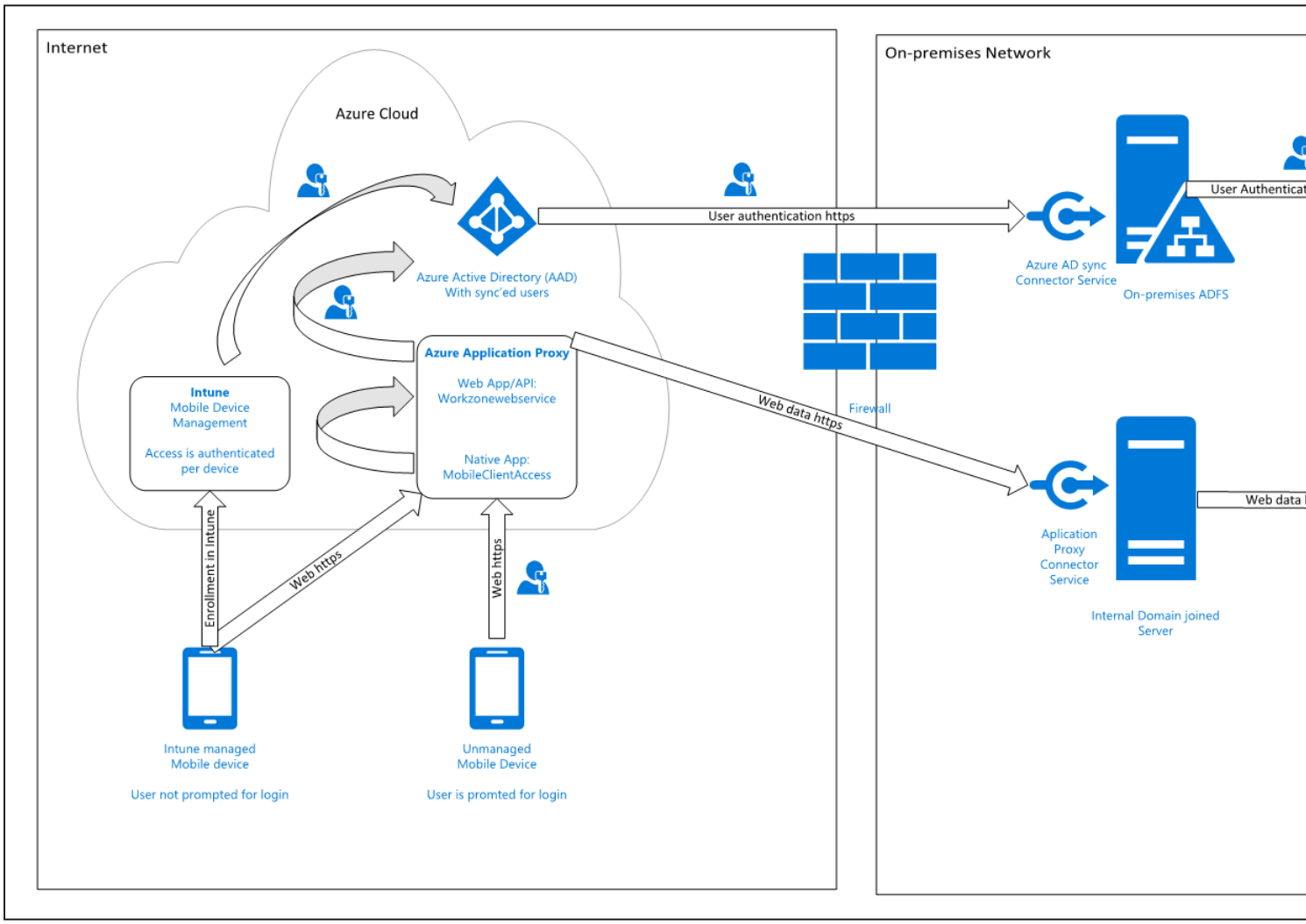
Microsoft Enterprise Mobility Suite (Intune) infrastructure

You can deploy WorkZone Mobile using Microsoft Intune.

Requirements

Mobile Device Management Systems	iOS	Android
Microsoft Enterprise Mobility Suite (Intune)	13	-

The diagram below shows a conceptual overview of the components in the infrastructure and how they are set up to support WorkZone Mobile with Microsoft Enterprise Mobility Suite (EMS). The number of real servers, firewalls, load balancers, and so on varies depending on how the environment is set up for a specific organization.



Some configuration of an organization's infrastructure actions must take place to allow WorkZone Mobile access to on- premise WorkZone through Microsoft Enterprise Mobility Suite:

Syncronization of internal users to Entra ID

You can do this in several different ways but to be able to use multifactor authentification, and thereby also conditional access, the only supported solutions is to federate your internal domain using an on- premises ADFS solution. This means that user login requests are forwarded to an internal ADFS service. Furthermore, it means that there are no passwords or password hashes in Azure. This is also the only solution that offers users the full single sign- on experience across internal systems, for example Microsoft Office 365 apps.

Azure Application Proxy with a Proxy Connector service installed

Azure Application Proxy pre- authenticates users in Entra ID and provides access to underlying applications, in this case the internal WorkZone web service. A Proxy Connector service is installed on an internal server, which is in the same domain as the resources that are to be exposed, in this case the internal WorkZone web server.

When the Azure Application Proxy service approves a request, it connects to the internal Proxy Connector, and requests it to access the internal resource (the WorkZone web server) on behalf of the current user, and send data back to the user/device on the other side of the Azure Application Proxy service.

Azure Web App publication of internal WorkZone services

The internal WorkZone web site must be published using Azure Application Proxy as a Web App/API type, so that it can be accessed externally with the same URL as the internal clients use on the domain. Furthermore, it requires that WorkZone is set up to use the HTTPS.

You set it up so that it is required that users are pre- approved with Entra ID before they get access to the internal resources. As a second factor, besides user name and password, you can add a so- called Conditional Access Policy in Azure that only allows access if the user uses a device, which is managed by Intune. This means that you can use the actual device as the second factor.

It is also possible to use other built- in two- factor features in Entra ID, for example sms code or voice call. This will, however, add an extra step to the user's login process.

Internal WorkZone must run with HTTPS

To publish a web service using Azure Application Proxy, HTTPS is required and as WorkZone does not support HTTPS off- loading,the underlying WorkZone server must also use HTTPS.

Flexible management of security

Because you use Entra ID, you also have access to all the options for managing access. When Microsoft releases new features, you will also be able to use these features to manage the access to the WorkZone Mobile app.

Intune deployment of WorkZone Mobile and Microsoft Office 365

To get the full benefit of WorkZone Mobile, it must be deployed along with Office 365, which offers the possibility to edit Office documents.

Configure WorkZone Mobile in Microsoft Azure Portal

When the requirements to the infrastructure are fulfilled, you can move on to setting up and configuring WorkZone Mobile in Microsoft Azure Portal. See Administrator Guide for WorkZone Mobile.

Deploy WorkZone Integration Platform

The WorkZone Integration Platform is an online tool that you can use to create integrations between WorkZone and external systems. The WorkZone Integration Platform uses SnapLogic tools for connecting cloud data sources. The WorkZone Integration Platform is available on the Public and EU- Cloud, however, it is not accessible to customers who operate in air- gapped environments.

To learn more about SnapLogic and deployment, see Deploying a Groundplex in Kubernetes in the SnapLogic documentation.

This page describes how to set up SnapLogic to integrate with WorkZone and synchronize data.

Prerequisites

Before deploying the WorkZone Integration Platform, ensure that your environment meets the following prerequisites :

- **SnapLogic portal**

  Ensure access to the SnapLogic portal for the EMEA region (Europe, the Middle East, and Africa). You need an active account and an individual project on the SnapLogic portal.

  Go to https://cdn.emea.snaplogic.com/sl/designer.html# to access the SnapLogic portal for the EMEA region.

- **SnapLogic image**

  Ensure that the SnapLogic image is available in all the required ACR (Azure Container Registry) tenants.

- **Memory and CPU per JCC (Java Component Container) node**

  - Memory: 3Gi
  - CPU: 1100m

- **Deployment in KMD EU Cloud**

  If you deploy SnapLogic in KMD EU Cloud, order the following should at KMD Cloud Center of Excellence (CCoE) for each environment where SnapLogic will be installed (SnapLogic should only be installed in production unless otherwise specified).

  Allocate one node of the type DS3_ v2 (2 vCPU, 16 GB RAM).

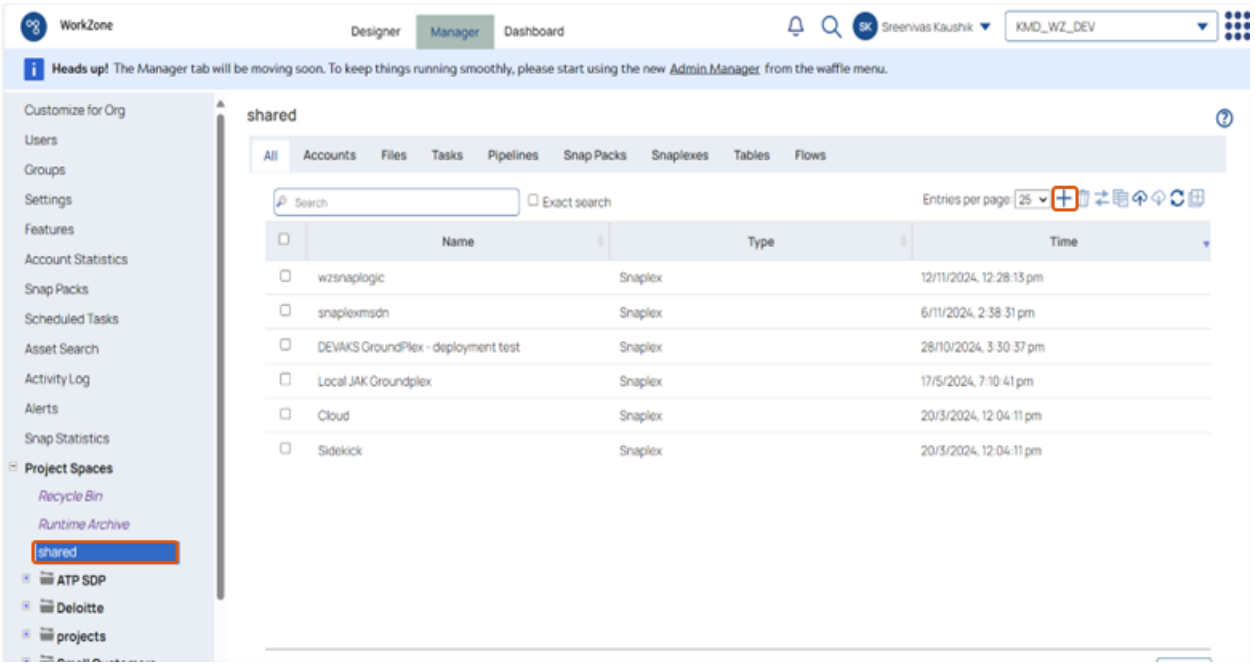
  > **Note:** If you plan to use the SnapLogic instance towards other environments outside the AKS cluster where SnapLogic is installed, ensure that the necessary firewall openings are in place.

  If you deploy in KMD EU Cloud, order the following at CCoE for each environment that SnapLogic should be able to communicate with:

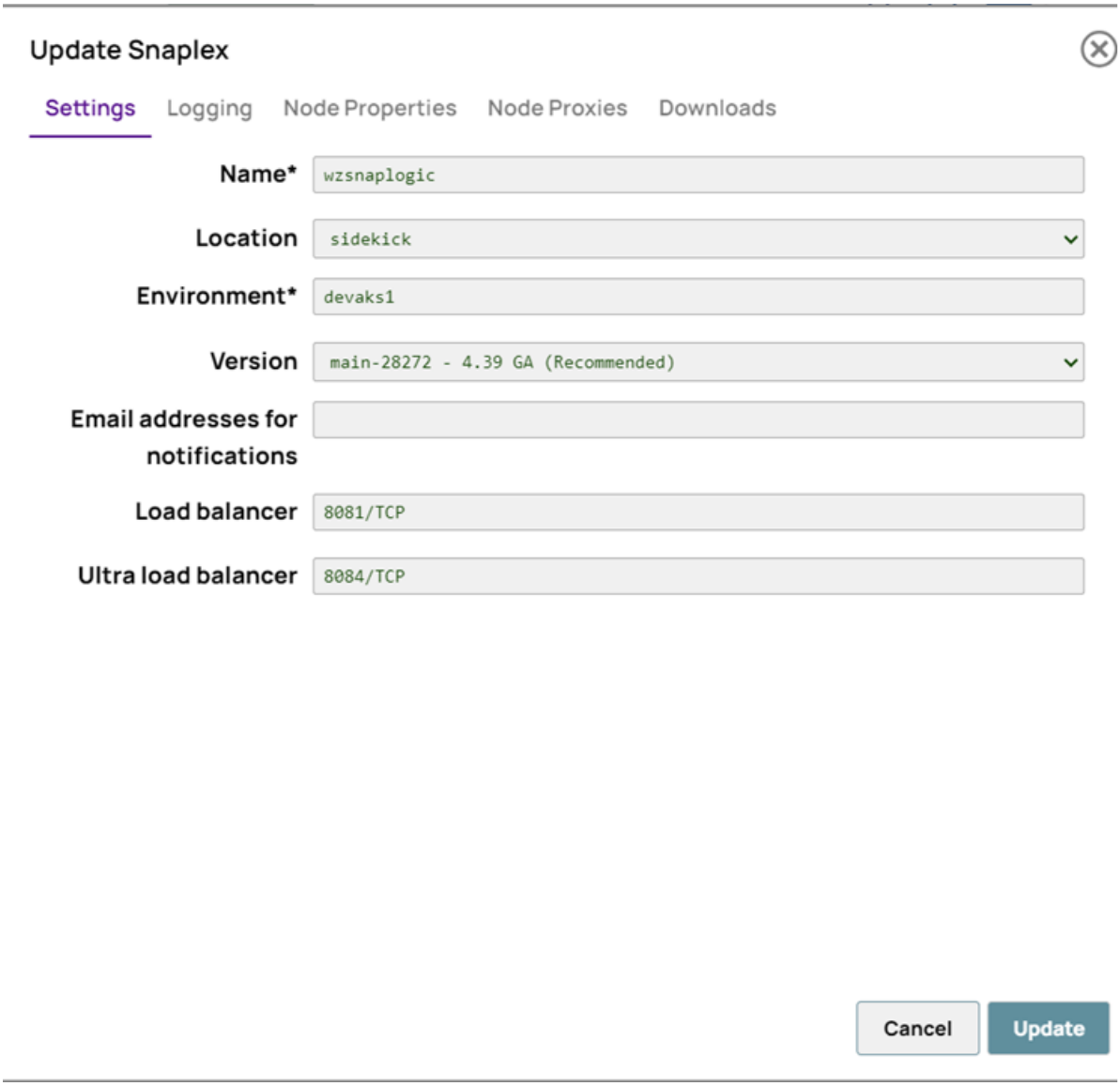
- **Source and destination environment/protocol and port**: HTTP/HTTPS 80/443 between <company name>.test.workzone.cloud and <insert company namer>.workzone.cloud

Creating a Snaplex

1. In the SnapLogic portal, go to the **shared** folder, and click **+** and select **Snaplex**.



2. Fill in the required field as shown below.



Deploy SnapLogic Groundplex in AKS

1. In the Azure portal, open Cloud Shell and create a new directory for SnapLogic.
2. Run the command below to download the Helm charts.

   ```
   wget https://docs-snaplo-gic.atlassian.net/wiki/download/attachments/855836057/helm_chart_v2.zip?api=v2
   ```

3. Unzip the Helm chart:

```
unzip helm_chart_v2.zip\?api\=v2
```

4. Run the curl command below to get the config link url:

   ```
   curl -u <userid> https://{controlplane_path}/ap-
   i/1/rest/public/snaplex/config/{plex_path}? {query_parameters}
   ```

5. Open the SnapLogic Control Plane: elastic.snaplogic.com. To open either the UAT (User Acceptance Testing) Control Plane or the EMEA Control Plane, substitute the name for `elastic`.

   UAT Control Plane: uat.snaplogic.com.

   EMEA Control Plane: emea.snaplogic.com.

6. Specify the plex path. The syntax for building the SnapLogic plex path is:

   ```
   Plex_path Format: = /{env_org}/{project_space}/{project_name}/
   {snaplex_name}
   ```

   Use the query parameters = Expire_ hours or Version.

   For example:

   ```
   curl -u ftf@kmd.dk https://cd-
   n.emea.snaplogic.com/api/1/rest/public/snaplex/config/KMD_WZ_
   DEV/shared/wzsnaplogic?expire_hours=336
   ```

7. You will be asked to enter password to log in to the SnapLogic portal and get your specific control_ plane path. Enter the password for the SnapLogic account.

8. The response from the above curl command would look something like the example below, but you only need the config link from the response.

{"response_map": {"pkgs": {"plex-rpm": {"comment": "4.39 GA Linux/RPM", "uri": "https://snaplogic-prodeu-sldb.s3.eu-west-1.amazonaws.com:443/pkgs/snaplogic-sidekick-4.main-28272-x86_64.rpm", "driver": null, "signatures": {"md5": "xxxxxxxxxxxxxxxxxxxxxxxxfd70"}, "pkg_file": "snaplogic-sidekick-4.main-28272-x86_64.rpm", "kind": "plex-rpm", "version": "main-28272", "compatible_version": "main-28272", "status": "active", "create_time": "2024-11-14T20:10:36.603000+00:00", "_id": "xxxxxxxxxxxxxxxxxxxxxxxxxe4e6"}, "plex-deb": {"comment": "4.39 GA Linux/DEB", "uri": "https://snaplogic-prodeu-sldb.s3.eu-west-1.amazonaws.com:443/pkgs/snaplogic-sidekick-4.main-28272-x86_64.deb", "driver": null, "signatures": {"md5": "xxxxxxxxxxxxxxxxxxxxxxxx5742"}, "pkg_file": "snaplogic-sidekick-4.main-28272-x86_64.deb", "kind": "plex-deb", "version": "main-28272", "compatible_version": "main-28272", "status": "active", "create_time": "2024-11-14T20:10:44.876000+00:00", "_id": "xxxxxxxxxxxxxxxxxxxxxxxx9e"}, "plex-win": {"comment": "4.39 GA Windows/ZIP", "uri": "https://snaplogic-prodeu-sldb.s3.eu-west-1.amazonaws.com:443/pkgs/snaplogic-sidekick-4.main-28272.zip", "driver": null, "signatures": {"md5": "xxxxxxxxxxxxxxxxxxxxxxxxd3561"}, "pkg_file": "snaplogic-sidekick-4.main-28272.zip", "kind": "plex-win", "version": "main-28272", "compatible_version": "main-28272", "status": "active", "create_time": "2024-11-14T20:10:50.834000+00:00", "_id": "xxxxxxxxxxxxxxxxf2095"}}, "config": "https://emea.snaplogic.com/api/1/rest/plex/config/<OrganizationName>/<snaplexfolder>/<SnaplogicName>?expires=1733474178&user_id=ftf%40kmd.dk&_sl_authproxy_key=PAvuqDku6yhWfPCZEHw0e%2Food%2FtfcxBiqZKGZ5lrdfo%3D"}, "http_status_code": 200}

9. Change the directory to helm_chart_v2 and open the values.yaml file with the command "`vi values.yaml `".

   Copy or download the file Values.yaml file.

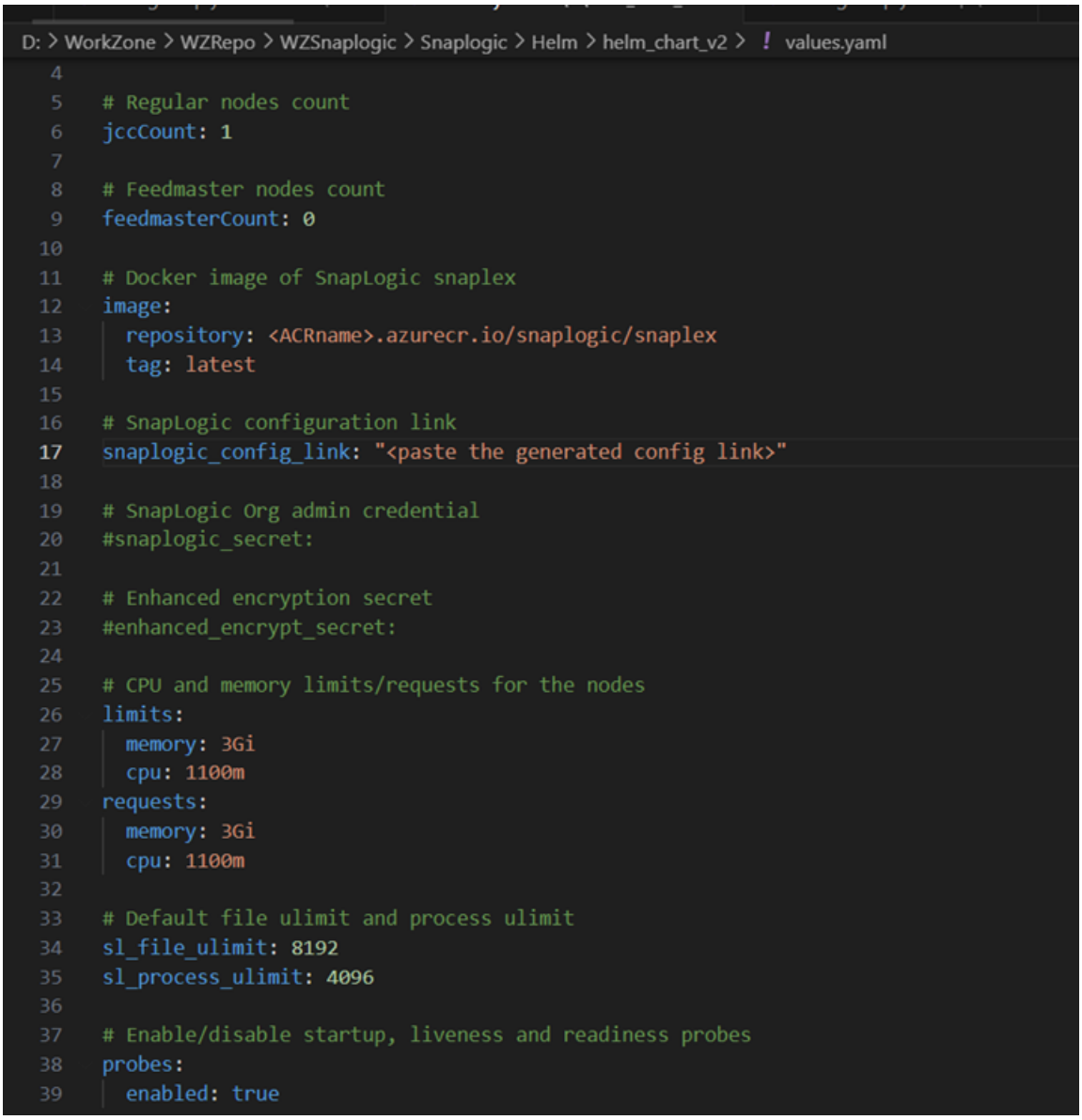
```
                # Default values for snaplogic-snaplex.
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

# Regular nodes count
jccCount: 1

# Feedmaster nodes count
feedmasterCount: 0

# Docker image of SnapLogic snaplex
image:
  repository: snaplogic/snaplex
  tag: latest

# SnapLogic configuration link
snaplogic_config_link: https://e-
mea.snaplogic.com/api/1/rest/plex/config/KMD_WZ_DEV/shared/wz-
snaplogic?expires=1734330726&user_id=ftf%40kmd.dk&_sl_
```

```
authproxy_key-
y=dFdPVa9My9NoWyYO8OyY%2BUDuOZYupAc2C34OuOCP%2BJc%3D

# SnapLogic Org admin credential
#snaplogic_secret:

# Enhanced encryption secret
#enhanced_encrypt_secret:

# CPU and memory limits/requests for the nodes
limits:
  memory: 3Gi
  cpu: 1100m
requests:
  memory: 3Gi
  cpu: 1100m

# Default file ulimit and process ulimit
sl_file_ulimit: 8192
sl_process_ulimit: 4096

# Enable/disable startup, liveness and readiness probes
probes:
  enabled: true

# JCC HPA
autoscaling:
  enabled: false

  minReplicas:
  maxReplicas:

  # Average count of Snaplex queued pipelines (e.g. tar-
getPlexQueueSize: 5), leave empty to disable
  # To enable this metric, Prometheus and Prometheus-Adapter
```

```
are required to install.
  targetPlexQueueSize:

  # Average CPU utilization (e.g. targetAvgCPUUtilization: 50
means 50%), leave empty to disable.
  # To enable this metric, Kubernetes Metrics Server is
required to install.
  targetAvgCPUUtilization:

  # Average memory utilization (e.g. tar-
getAvgMemoryUtilization: 50 means 50%), leave empty to disable.
  # To enable this metric, Kubernetes Metrics Server is
required to install.
  targetAvgMemoryUtilization:

  # window to consider waiting while scaling up. default is 0s
if empty.
  scaleUpStabilizationWindowSeconds:
  # window to consider waiting while scaling down. default is
300s if empty.
  scaleDownStabilizationWindowSeconds:

# grace period seconds after JCC termination signal before
force shutdown, default is 30s if empty.
terminationGracePeriodSeconds: 900

# Enable IPv6 service for DNS routing to pods
enableIPv6: false
```

10. Change the limits and request parameters according to the AKS configuration and specify the image that is available in the ACR.

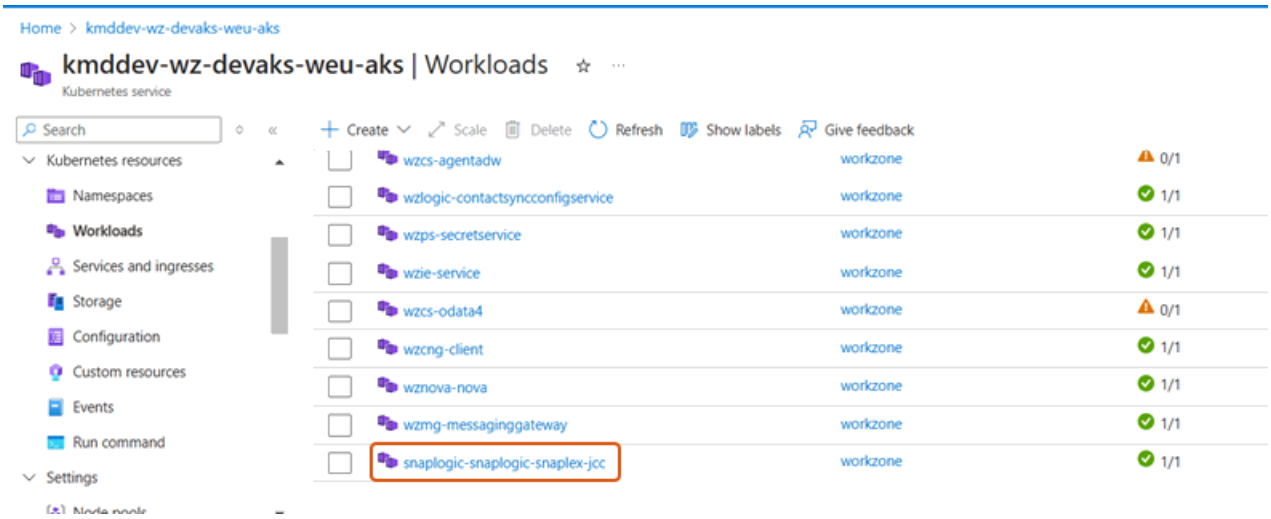
- Set the JCC node count as per the requirements.
- Set the FeedMaster node count to 0.
- Delete all the FeedMaster related files from the template.



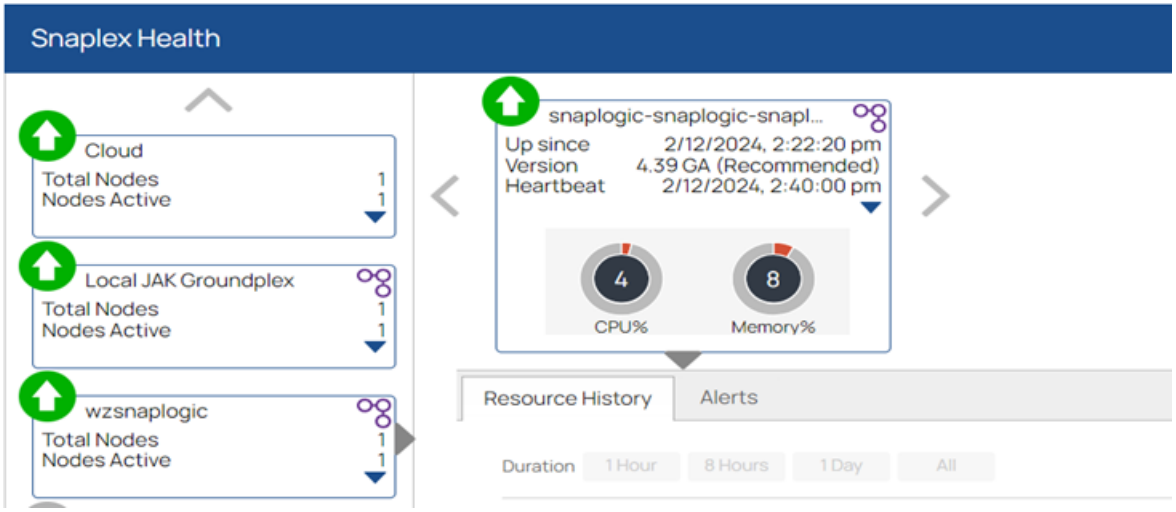
11. Go back to the root directory and run the command below to install the Helm chart:

    ```
    helm install snaplogic helm_chart_v2 --namespace workzone - -set-string snaplogic_config_link='<paste the config link>'
    ```

    The deployment is ready:

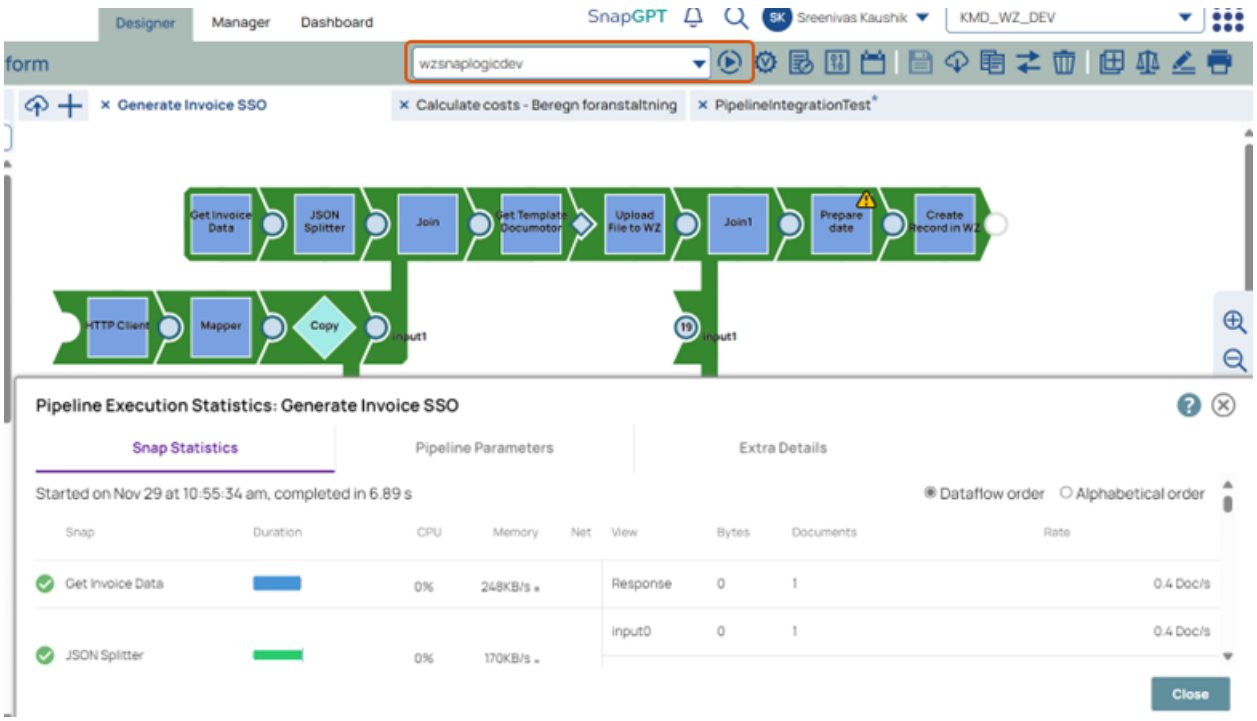


The JCC node should be up and running as shown below without any errors and alerts.



Test the Snaplex JCC node

To test if the deployed Snaplex JCC node works, you can go to the **Designer** tab and select any sample pipeline or build a pipeline as per the requirements. Select the required Snaplex against which you want to run the pipeline and click the **Execute/Run** button.



If the pipeline state is green, the deployment was successful and the data is being integrated.

Deploy the SnapLogic Groundplex in EU Cloud

Resource configuration in production: DS3_ v2 (2 vCPU, 16 GB RAM).

Deploy SnapLogic Groundplex

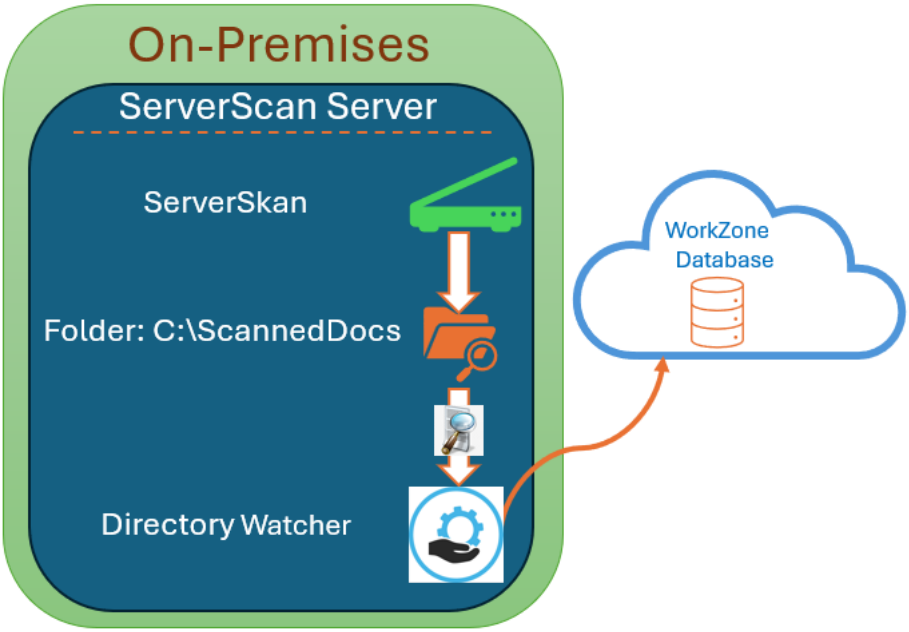
1. Create Service connection (SPN) to access the resources from Azure.
2. Ensure that the SnapLogic docker image is available in the kmdworkzone ACR (kmdworkzone..azurecr.io/snaplogic/snaplex:latest).
3. Add the image pull secret to the environment configuration.

Install and configure ServerScan Directory Watcher Service

ServerScan Directory Watcher Service is a Windows service that uploads scanned documents and their metadata to cases in WorkZone.

About ServerScan Directory Watcher Service

ServerSkan and ServerScan Directory Watcher Service are installed in an on- premises environment while the WorkZone database is installed in the cloud.



ServerSkan scans documents and copies or creates XDI folders that contain the scanned documents. The XDI folders are located in a specific folder that ServerScan Directory Watcher Service monitors. In this example, the monitored folder is: C:\ScannedDocs. You can configure the folder to be monitored before you install ServerScan Directory Watcher Service. See Install ServerScan Directory Watcher Service.

ServerScan Directory Watcher Service reads a metadata file named sjFesdPacket.xml and uploads the documents with their metadata to the corresponding cases in WorkZone using OData. See Sample metadata XML templates.

The ServerScan Directory Watcher Service supports:

- Windows 10 Pro (version 22H2) with 64- bit
- Windows Server 2022 with 64- bit
- Windows Server 2019 Standard with 64- bit

Note:

- The case number must be specified for the documents. This release of ServerScan Directory Watcher Service does not support upload of documents without case numbers to WorkZone.
- The maximum size of a document that ServerScan Directory Watcher Service can upload to WorkZone is 178 MB, but it can vary depending on the network bandwidth.

See also:

WorkZone Content Server Imaging Installation Guide (2024.4)

ServerSkan brugervejledning (in Danish)

Install and configure ServerScan Directory Watcher Service

Prerequisite:

- .NET 8 SDK (Download .NET 8.0) .
- Access to OData to update the documents and metadata for respective cases (URL).
- Permission to use a Microsoft Windows Installer (MSI) file to install the ServerScan Directory Watcher Service.
- Application ID and secret, and Tenant ID of the WorkZone application.
- Windows Server 2022 with 64- bit.
- All Danish names must be replaced with English names in XSLTToSj.xsl file. See Sample metadata XML templates.
- Access to login.microsoftonline.com from ServerSkan.
- The files in the Components folder must be located in the installation package.

- Make sure that the following information types (custom labels) exist in WorkZone:

  Of the type AO (dokumentoplysning):

  - **SSURI** (File path of the scanned document)
  - **AO** (Document)
  - **IndScanPers** (Person who scanned the document)
  - **IndScanSide** (Number of pages)
  - **IndScanTid** (Time of scanning)

  Of the type AP (Aktpart):

  - **Forfatter** (Author)
  - **Afsendt af** (Sent by)
  - **Afsendt fra** (Sent from)
  - **Modtager** (Recipient)
  - **CPR- nr** (CPR No.)

  If you do not have these information types, you can add them in WorkZone Configurator. Go to **Document** > **Informantion types**. See Information types.

  Note that you need to write the custom labels in lower case in the cfg files in the CFG folder. Read about the CFG folder in Configure WorkZone Content Server Imaging (2024.4).

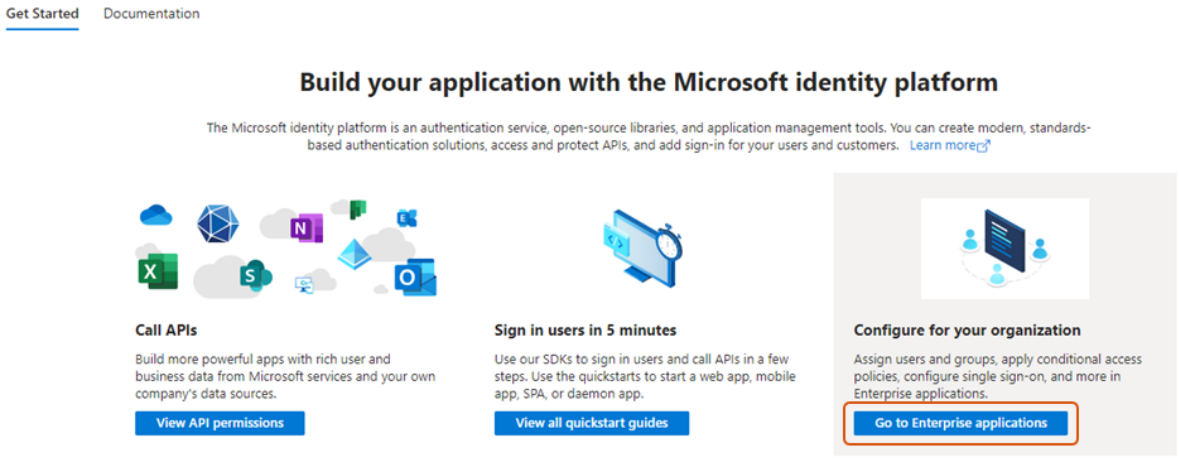
App registration

Start by registering ServerScan Directory Watcher Service as an app in your Azure tenant.

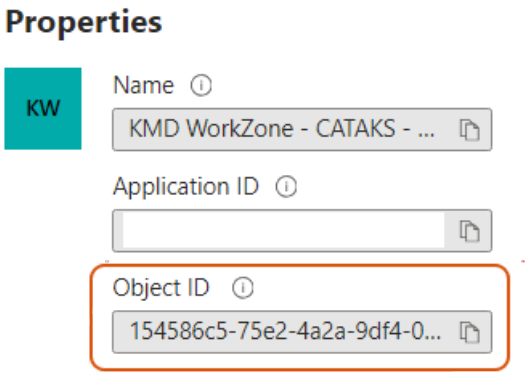
1. Follow steps 1 and 2 only in Set up third- party integrations in Azure.

> **Note:** While registering the app, make a note of Application (Client ID), Tenant ID, Client Secret, and Enterprise Application Object ID.

2. Go to **Entra ID** > **App Registration**, and select your app.
3. Click **Go to Enterprise applications** at the bottom right of the page.



4. Copy the **Object ID** (Enterprise Application Object ID) and paste it to, for example Notepad, as you will need it later for configuration in WorkZone Configurator.



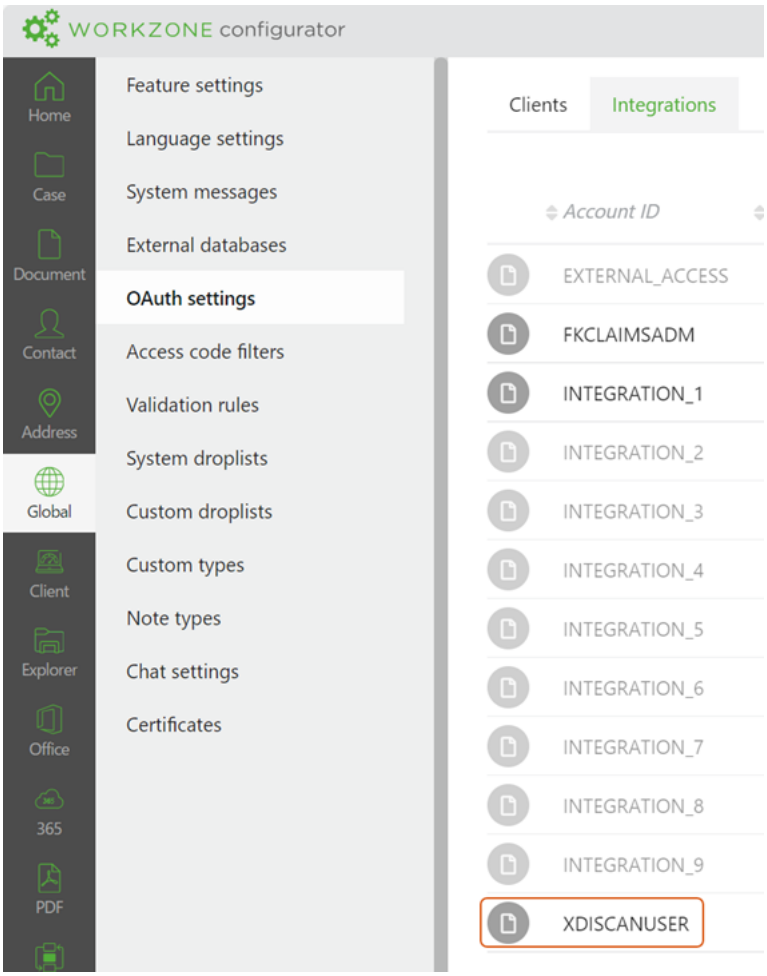
5. To configure the Enterprise Application Object ID in WorkZone, see Configure APP Enterprise Application ID.

Configure APP Enterprise Application ID

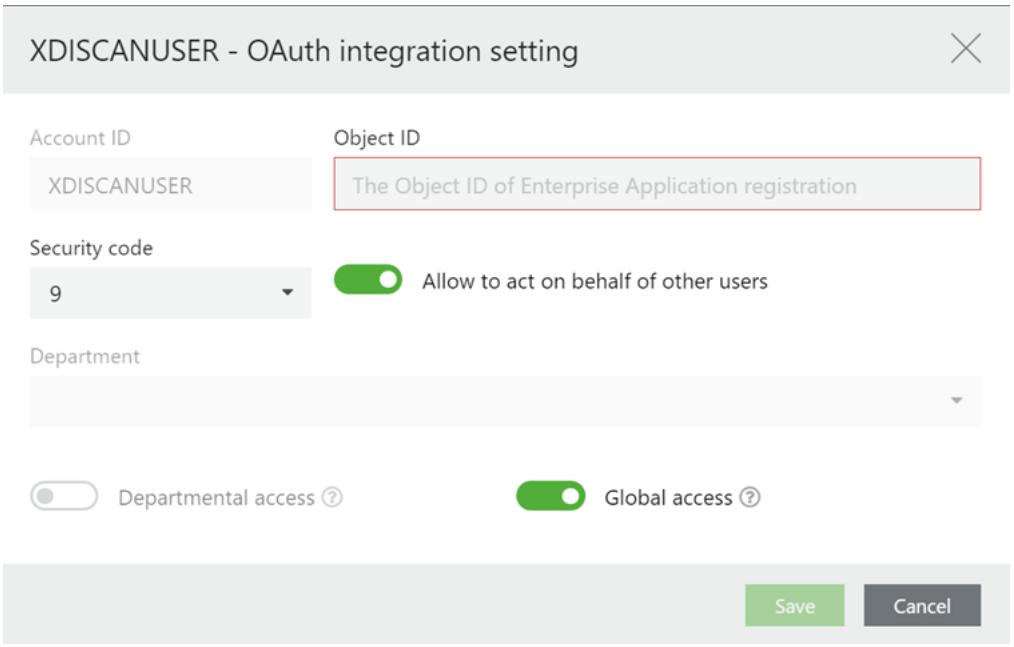
When you have registered ServerScan Directory Watcher Service as an app, you need to configure the access to WorkZone in WorkZone Configurator.

1. Log in to WorkZone and open WorkZone Configurator.

2. Go to **Global** > **OAuth settings** > **Integrations** tab, and click **Edit** next to the **XDISCANUSER** account.



3. Enter the Enterprise Object ID of the Azure Entra ID app in the **Object ID** field, turn on **Allow to act on behalf of other users**, and select the security code 9 in the **Security code** field.



4. Click **Save**.

Download the folders

Before you can start the installation, you need to download two folders from the release drive ..\Release\WorkZone Directory Watcher:

- **Deployment** folder that contains the deployment script for automatic installation and configuration files.
- **WZSS_ Setup** folder that contains the installer.

Install ServerScan Directory Watcher Service

> **Prerequisite:** To install and uninstall ServerScan Directory Watcher Service, you need to have administrative rights.

Run the installer

1. Right-click Windows PowerShell and select **Run as Administrator**.
2. Go to the WZSS_Setup folder that contains the KMD.WorkZone.ServerScan.Setup.MSI file.
3. The table below shows the parameters that are required to install ServerScan Directory Watcher Service:

Parameter	Description	Example
DIRECTORYWATCHER	Path to the folder to monitor for scanned documents.	C:\ScannedDocs
SCHEMA	Path to the Components\Schedules folder. The folder must be named as shown in the example.	C:\Components\Schedules\
TRANSFORMATIONS	Path to the Components\Transformation folder. The folder must be named as shown in the example.	C:\Components\Transformations\
ERRORPATH	Path to the folder that stores error files.	C:\Logs\Errors
OUTPUTPATH	Path to the folder that stores processed files.	C:\ProcessedDocs
CLIENTID	Azure application client ID.	12345678-1234-1234-1234-123456789abc
TENANTID	Azure tenant ID.	87654321-4321-4321-4321-

Parameter	Description	Example
		abcdef123456
CLIENTSECRET	Encrypted Azure application client secret.	EncryptedValue See Encrypt the secret.
REDIRECTURL	Redirect URL for OAuth authentication	https://localhost
AUTHREQUESTURL	URL for authentication requests.	https://<domainname>/.default Replace <domainname> with your domain name.
ODATAURL	URL for OData API.	https://<-domainname>/odata/v3 Replace <domainname> with your domain name.
PROTOCOLANDHOST	Protocol and host for communication	https://<domainname> Replace <domainname> with your domain name.
LOGPATH	The path to the folder that stores logs that are generated daily.	<log file path>\\log.txt Replace <log file path> with the location of logs to be generated. For example: " C:\\WZ\\WZSS\\-log.txt"

4. Use the following command to install the .MSI with all parameters. Replace the placeholders with actual values:

```
msiexec /i "KMD.WorkZone.ServerScan.Setup.msi" DIRECTORYWATCHER-
R="C:\ScannedDocs" SCHEMA="C:\Components\Schedules\"
TRANSFORMATIONS="C:\Components\Transformations\" ERRORPATH-
H="C:\Logs\Errors" OUTPUTPATH="C:\ProcessedDocs" CLIENTID-
D="12345678-1234-1234-1234-123456789abc" TENANTID="87654321-
```

```
4321-4321-4321-abcdef123456" CLIENTSECRET="EncryptedValue"
REDIRECTURL="https://localhost" AUTHREQUESTURL-
L="https://<domainname>/.default" ODATAURL-
L="https://<domainname>/odata/v3"
PROTOCOLANDHOST="https://<domainname>" LOGPATH="<log file
path>\log.txt" /q
```

> **Note:** If a parameter value contains spaces, enclose parameter value in single quotes ' when you pass the command. For example: DIRECTORYWATCHER='" C:\testwzss\Scanned Documents\"'

5. Start the service with the following PowerShell command:

   ```
   Start-Service -Name "KMD WorkZone Directory Watcher Service"
   ```

Encrypt the secret

1. Go to the EncryptionHelper.ps1 file in the Deployment folder.
2. Open Windows PowerShell in administrative mode and run the command.

   ```
   .\EncryptionHelper.ps1 -encryptText "<Secret>"
   ```

3. Copy the Encrypted text and update the ClientSecret value.

> **Note:** Encryption must be done on the machine where ServerScan Directory Watcher Service will be running.

Sample metadata XML templates

- Sample metadata file (XML file)
- English names (XSL file)

Danish names are no longer supported but you can use this file to map Danish names to English names:

Mapping of Danish names to English names (XML file)

Uninstall ServerScan Directory Watcher Service

1. Navigate to the location where you saved the original .MSI installation file.
2. Right-click the .MSI file and select **Uninstall**. This will start the uninstallation process.

If any error occur while uninstalling, follow these steps:

1. Open PowerShell as an Administrator.
2. Run these commands:
    - `sc.exe stop "KMD WorkZone ServerScan Service"`
    - `sc.exe delete "KMD WorkZone ServerScan Service"`

Confirm removal of the installation folder

When you have uninstalled the service, verify that the folder has been removed (C:\Program Files (x86)\KMD.WorkZone.ServerScan). If the folder still exists, you can delete it manually. Administrative rights may be required.

Access codes

Access codes

The table below provides an overview of access codes and what they give access to. Usually the mandatory system access codes are created by script, but if they do not exist in your Active Directory, you must created them manually.

WorkZone operates with three different types of access codes:

- Employee access code (associated with each user from Active Directory)
- Unit access code (associated with each Organizational unit from Active Directory)
- Group access code.

If your organization opted for an installation that utilizes the Corporate Access Code System (CACS), then all cases and documents are created with an access code string of a minimum of two access codes: an organizational access code and a group access code.

Access code	Usage	More information
AFDADM	• Create or modify units. • Assign organizational units as delegates on behalf of other users or units. • Create and maintain organizational units in WorkZone Configurator for WorkZone Cloud Edition installations using Microsoft Azure Active Directory.	• Work with delegates • Organizational units (For WorkZone Cloud Edition using Microsoft)
ALLEEMNER	A corporate system access code. If the Corporate configuration is chosen, then the **Access Code** field of cases and documents must never be left blank. Therefore, all objects of the system that	• Corporate access codes

Access code	Usage	More information
	should be visible to all users must have the ALLEEMNER access code. This is a system access code that all users of the Corporate configuration must be members of.	
CERTADM	Not applicable in this release.	
CONFIGADM	**WorkZone Client:** • Configure and distribute WorkZone Client configurations. • Edit templates for reports. **WorkZone Configurator:** Configure settings of: • WorkZone PDF Crawler • WorkZone PDF Engine • WorkZone Explorer • WorkZone for Office Configure the following additional settings: • Import and export WorkZone configurations • Custom types (requires also DATAADM) • Custom type fields • Document draft version • Office Online Server • Chat settings	• Working with WorkZone Client configurations • Reports • Work with delegates • WorkZone PDF settings • WorkZone for Office settings • WorkZone Explorer configuration • Custom types • Custom type fields • Chat settings
DATAADM	**WorkZone Configurator:**	• Cases, doc-

Access code	Usage	More information
	Configure the following: • Case number format • Classification scheme (case groups) • Contact types (requires also CONFIGADM) • Countries and postcodes • Custom droplists • Custom fields • Date types • Default retention policy • Dictionary and keywords • Document classification • External databases • Facets • Information types • Import WorkZone configurations (requires also CONFIGADM) • Note types • Parties and references • Reason for document deletion • Security group rights • Subnumbers and subnumber types • Supported file types • Validation rules	uments, and contacts • Custom types • Custom type fields • Security group rights
DELEGATEADM	• Assign delegates for other users	• Delegates

Access code	Usage	More information
DEJOURNALADM	**WorkZone Client:** • Move an archived document from one case to another. Moving an archived document to another case is logged and traceable.	• Move document
HARDCOPYADM	WorkZone Client: • Add hard copies and duplicates to a document. • Accept a distribution of a hard document or a duplicate on behalf of another user. • Destroy a hard copy or a duplicate. • Cancel a destruction of a hard copy or a duplicate.	• Manage hard copies of a document
FESD_WS	Call WorkZone Content Server Open WSI and gain access from a third party system. The system user of the third-party system is the member. The FESD_WS access code is an externally used system access code.	
LICENSEADM	Enable and disable WorkZone features and modules in the WorkZone Configurator.	• Feature settings
LOSTANDFOUND	**WorkZone Client**: Edit the **Hidden Dashboard** list. The **Hidden Items** menu group contains the following sub-menus: • Cases	• Hidden entities

Access code	Usage	More information
	• Documents • Contacts **Prerequisite:** Users must have the * access code to display, open and edit the displayed hidden items.	
MASSDISPATCH	Displays the **Mass dispatch** process in the **Process** menu in WorkZone Client and allows users to start a new mass dispatch.	• Start Mass Dispatch
MASSDISPATCHSEND	Allows users to send the documents using the **Mass dispatch** process.	• About Mass Dispatch
MEDARBADM	• Create or modify employees. • Assign departmental access codes to other users (you must also have the AFDADM and STJERNEADM access codes and the WorkZone Corporate Edition installed).	• Active Directory
MULTIEDIT	**WorkZone Client:** • View and edit up to 500 list items on a page. Users that are not assigned the MULTIEDIT access code can view and edit up to 50 list items on a page.	• Work with multiple list items
OAUTH2ADM	Set up and configure the OAUTH2 framework for WorkZone connectivity.	

Access code	Usage	More information
PROCESSADM	**WorkZone Configurator:** • Define general Process settings • Configure processes, service workflows, and case activities • Access process logs. **WorkZone Process:** • Unlock a task locked by another user.	• Process settings • Process logs • Export and deploy case activity graphs • Unlocking a locked task • Work with delegates
PROCESSDEV	**WorkZone Configurator:** • Add and update process packages in WorkZone Configurator,	• Process packages
RETENTIONADM	**WorkZone Client:** • Change the retention policy on a case. **WorkZone Configurator:** • Set up and maintain retention policies.	• Meta data fields • Retention policies
SEARCHADM	Reassign the ownership of shared searches, for example if the original owner is unavailable.	
SOFTDELETE	**WorkZone Client:** • Send cases and archived documents to the recycle bin. • Restore cases and archived documents from the recycle bin.	• Delete a case • Restore a deleted case • Delete a document

Access code	Usage	More information
	• Delete cases and documents permanently if you have access code associated with the case's or document's retention policy.	• Restore a deleted document
STJERNEADM	**WorkZone Configurator**: Grant other users global access (requires having also the MEDARBADM access code) or departmental access (requires having also the MEDARBADM access code and the WorkZone Corporate Edition installed). • Global access: Grant users full access (read, write and delete rights) to all items within the entire organization. • Departmental access: Grant users full access (read, write and delete rights) to all items within the department the user is a member of. **Important:** Global and departmental access allow users view and edit items (cases, documents, contacts, meetings or actor sequences) protected by security access codes that the user is not a part of. Global and departmental access are extensive rights that will allow the user to access sensitive inform-	• Global and departmental access

Access code	Usage	More information
	ation. Assign these rights only when needed.	
TEMPLATEADM	**WorkZone Process**: • Create templates for standard letters used by SmartPost.	• Configure standard letters
USERADM	Access and configure in WorkZone Configurator: • **Users** • **Use Logs** • **Deletion Logs** • Assign users to units in WorkZone Configurator for WorkZone Cloud Edition installations using Microsoft Azure Active Directory.	• Users (for on-premise WorkZone installations) • Use logs • Deletion logs • Users (For WorkZone Cloud Edition using Microsoft)
USELOGADM	**WorkZone Configurator**: • Configure the use log settings and deletion log settings.	• Use log settings • Deletion log settings

Obsolete access codes

New access codes are sometimes introduced in new WorkZone versions as they are needed and existing access codes can also be updated, changed or removed from use, becoming obsolete.

While obsolete access codes no longer are present in the WorkZone program or referenced by WorkZone applications, they may still be present in local, converted databases as the upgrade process does not remove existing access codes, obsolete or not.

The following access codes are currently obsolete.

Access Code	Notes
ABBADM	A system access code for enabling the Subscription Administration menu item
CONTENT_ SERVICES	Enable and disable Content Services.
DIAGADM	Used for tracing logs in the now discontinued WorkZone Configuration Management (Diagnostic module).
FILINGPERIOD	Used in the now discontinued Captia Web Client. A system access code for enabling Filing Period menu items.
LISTCONF	Used in the now discontinued Captia Web Client. A system access code for list configuration.
LUKKET	Used to manage access in the Meeting module for the now discontinued Captia Web Client.
MENUCONF	A system access code for menu configuration.
MODESAG	Used to manage access in the Meeting module for the now discontinued Captia Web Client.
PHRASEEDIT_ DEPARTMENT	Used to manage access to the obsolete and withdrawn Phrases module.
PHRASEEDIT_ ORGANIZATION	Used to manage access to the obsolete and withdrawn Phrases module.
PHRASEEDIT_ USER	Used to manage access to the obsolete and withdrawn Phrases module.
POST	Used to manage access to mail lists.
PROFILADM	Used in the now discontinued WorkZone Configuration

Access Code	Notes
	Management. Used to manage access to Sysadm profile administration module.
RAPDEF	A system access code which provides access to old reports created with Crystal Reports (3rd party product).
STEPSUBMISSION	Displays the **Advanced submission (Extended)** process in the **Process** menu in WorkZone Client and WorkZone for Office, and allows users to start advanced submissions.
TERMSADM	Used in the now discontinued WorkZone Configuration Management to set up and maintain the Terms module.
UNLOCKADM	Used to manage access to relation unlocking menu items.
WORKFLOWADM	Obsolete Workflow access code.
WORKFLOWCREATE	Obsolete Workflow access code.
WORKFLOWSUBSTITUTE	Obsolete Workflow access code.
WORKFLOWSUBSTITUTEGLOBAL	Obsolete Workflow access code.
AABEN	Used to manage access in the Meeting module for the now discontinued Captia Web Client.

Important: The table above is not a list of access codes which should be deleted. Instead, it is a list of access codes which WorkZone no longer uses or references.

The list should be used as a base for further investigation of potentially removable access codes.

Configure Entra ID

Follow the procedures below to provision users from Entra ID to WorkZone - Cloud Edition. You can use this setup if you do not replicate users from on-premises AD but only use Entra ID.

Register WorkZone apps in Azure

WorkZone Entra ID registration

WorkZone uses the Microsoft identity platform for identity and access management tasks. To set up a trust relationship between WorkZone and the Microsoft identity platform, the WorkZone application must be registered. This app registration is created by KMD during WorkZone installation, and an Enterprise application representing this app registration is created in the customer's Entra ID tenant when first users access the WorkZone instance.

The WorkZone SharePoint and WorkZone Process modules require additional application registrations. These need to be created by the customer in their Entra ID tenant.

Create a WorkZone Enterprise application

> **Prerequisite:**
>
> This task must be performed by a user with permission to grant an admin consent in Entra ID (that is, at least a Privileged Role Administrator).

To create WorkZone Enterprise application, open the link provided by the WorkZone consultant. This link will redirect you to WorkZone, and you will need to consent for the required permissions on Entra ID.

Register the WorkZone Process application

An additional registration is needed to send emails from WorkZone Process. This registration will allow interaction with Exchange Online. Because the privileges that are granted are broad, the application access must be scoped down to one mailbox.

To create an application registration for WorkZone Process, run the `New-KmdWorkZoneExchangeApp.ps1` script.

The script uses the following parameters:

- `DisplayName`: Display name of the Entra app.
- `TenantId`: Entra Tenant ID.
- `IdentifierUriPrefix`: Unique name prefix used for application registration Uri.
- `ExchangeOnlineAuthFlow`: ClientCredential (recommended) or PublicClient.

Example:

```
.\New-KmdWorkZoneExchangeApp.ps1 `
       -DisplayName 'KMD WorkZone - Production - Exchange' `
       -TenantId XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX `
       -IdentifierUriPrefix 'Production' `
       -ExchangeOnlineAuthFlow ClientCredential
```

See Command line configuration of WorkZone Process for more details.

The script will output a client (application) identifier, tenant ID, and a client secret that must be delivered to KMD.

After running the script:

1. Inform KMD about the client (application) identifier, tenant ID, and a client secret that the script returns.
2. The script also returns the following message:" Permissions for this App requires Admin Consent. Please go to Azure Portal and 'Grant Permission' for this App or go directly to this consent url and log in as an AAD Admin (ignore that the redirect in the end might not work)" . Follow the instructions in the message to grant Admin Consent to the WorkZone Process application.

Secure WorkZone Process application registration

Important:

Application access must be limited to a single mailbox used by WorkZone Process using an application access policy. For more information, see the Microsoft documentation Limiting application permissions to specific Exchange Online mailboxes. Use the PowerShell script `Set-WZPAppRegistrationScope.ps1` to set the access limitation.

Prerequisite:

The script requires that the PowerShell ExchangeOnlineManagement module is installed. Before you execute the script, you need to connect to Exchange Online by running:

```
Connect-ExchangeOnline -UserPrincipalName <Exchange administrator account>
```

The following parameters are required by the script:

- `wzpMailbox`: The mailbox that the application should have access to.
- `wzpAppId`: The application (client) ID of the WorkZone Process application registration.
- `groupName`: Name of the Entra group that manages security for the application registration.

Example:

```
.\Set-WZPAppRegistrationScope.ps1 `
       -wzpMailbox example@yourdomain.com `
       -wzpAppId XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
       -groupName "KMD WorkZone Process Production"
```

Register the WorkZone SharePoint application

Follow these steps to register the WorkZone SharePoint application at Entra ID (this is a prerequisite for using the WorkZone SharePoint module to copy the documents from Microsoft SharePoint to WorkZone).

This is done via the `New-KmdWorkZoneWZSPApp.ps1` script provided by KMD technicians.

> **Prerequisite:** You must have the Entra and Azure Az Powershell modules installed, and the Entra admin consent.

Run the `New-KmdWorkZoneWZSPApp.ps1` script, using the following parameters:

- `DisplayName`: Display name of the AD app. For example, KMD WorkZone - WZSP.
- `IdentifierUri`: Identifier URI of the AD app that is also used for updates (script re- runs)
- `TenantId`: your Entra Tenant ID

Example:

```
.\New-KmdWorkZoneWZSPApp.ps1 `
-DisplayName 'KMD WorkZone – WZSP' `
-IdentifierUri 'api://5d3760f7-9e2f-4bf3-a318-b0ea87f66540/wzsp' `
-TenantId '5d3760f7-9e2f-4bf3-a318-b0ea87f66540'
```

Enroll WorkZone - Cloud Edition in Azure and set up SCIM provisioning

To enroll a new WorkZone instance in Microsoft Azure and set up SCIM (System for Cross-Domain Identity Management) provisioning users and groups from Entra ID to WorkZone, you must complete the following steps:

1. Associate UPN with WorkZone SCIMADMIN account
2. Generate secret token
3. Set up Microsoft Entra enterprise application
4. Configure automatic provisioning for the enterprise application
5. Assign users and groups to the enterprise application

1. Associate UPN with WorkZone SCIMADMIN account

> **Prerequisite:** You need to know the User Principal Name (UPN) from an existing account in your organization's Azure tenant that you want to associate with the WorkZone SCIMADMIN account.

To associate the UPN with the WorkZone SCIMADMIN account, run the following SQL against your organization's WorkZone - Cloud Edition database:

```
update users set upn=(UPN) where user_name='SCIMADMIN'
```

- The UPN is case sensitive.
- Note that technicians often carry out this task.

2. Generate secret token

You need to generate a secret token for use in your Entra ID enterprise application setup of the WorkZone provisioning.

1. Log on with the account from step 1.
2. Open WorkZone Configurator and go to **Services** > **SCIM Provisioning**.
3. On the **SCIM Provisioning** page, generate a token and copy it for use in theEntra ID Enterprise Application.

See SCIM provisioning in the WorkZone Configurator Guide.

3. Set up Microsoft Entra enterprise application

Create a new Entra enterprise application registration to be used for SCIM provisioning to WorkZone. The setup of the Entra enterprise application depends on whether your WorkZone - Cloud Edition instance is publicly accessible or not publicly accessible.

WorkZone - Cloud Edition is publicly accessible

For WorkZone Cloud Edition setups where WorkZone is publicly accessible, you need to create a new **non- gallery application** for provisioning in your Azure tenant as shown below.

1. In Azure Portal, go to **Microsoft Entra ID** > **Manage** > **Enterprise applications**.
2. Create a new application.
3. Enter a name for the application, for example *KMD WorkZone - [environmentname] - SCIM*.
4. Select **Integrate any other application you don't find in the gallery (Non- gallery)**
5. Click **Create**..

See the Microsoft article Integrate your SCIM endpoint with the AAD SCIM client for instructions on how to create a non- gallery application.

WorkZone - Cloud Edition is not publicly accessible

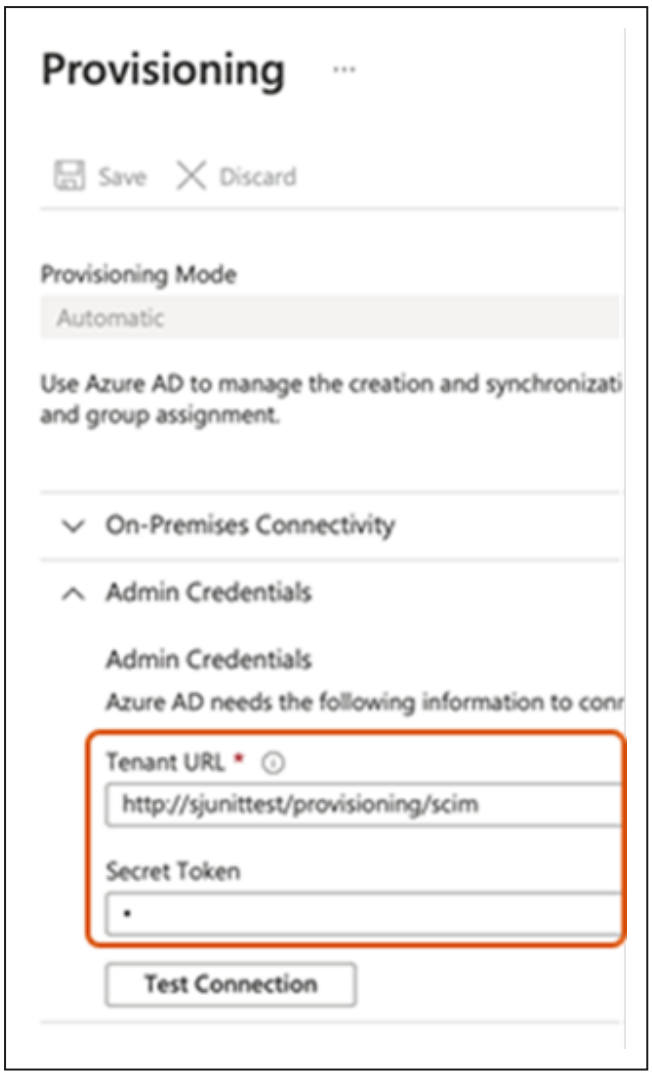
If the WorkZone servers are not publicly accessible, for example when they are hosted in a lab and you want to test or develop in the lab, you will need to use the gallery app named **On- Premises SCIM** app, and additionally install a SCIM agent on the web server.

See the Microsoft article Microsoft Entra on- premises application provisioning to SCIM- enabled apps for instructions on how to create an on- premise application.

4. Configure automatic provisioning for the enterprise application

For both public and non- public WorkZone - Cloud Edition instances, you will need to configure automatic provisioning for the enterprise application that you created in step 3.

1. Under **Admin Credentials**, enter the address to the **WorkZone Provisioning SCIM** web service. For example, `https://CUSTOMER.-workzone.cloud/provisioning/scim`.
2. Enter the secret token that you generated in step 2 in the **Secret Token** field.
3. Click **Test Connection** to test the connection.



4. Click **Save**.
5. Reopen the **Provisioning**. The **Mapping** tab is now available.
6. Under **Mappings**, leave the default settings for mapping users and groups as is to use the default mapping scheme that Azure offers. The default settings are **displayName**, **ObjectId**, and **members**. If you want to provision group descriptions from Entra ID to WorkZone or add guest users, you need to create additional mappings.

   ### Group description

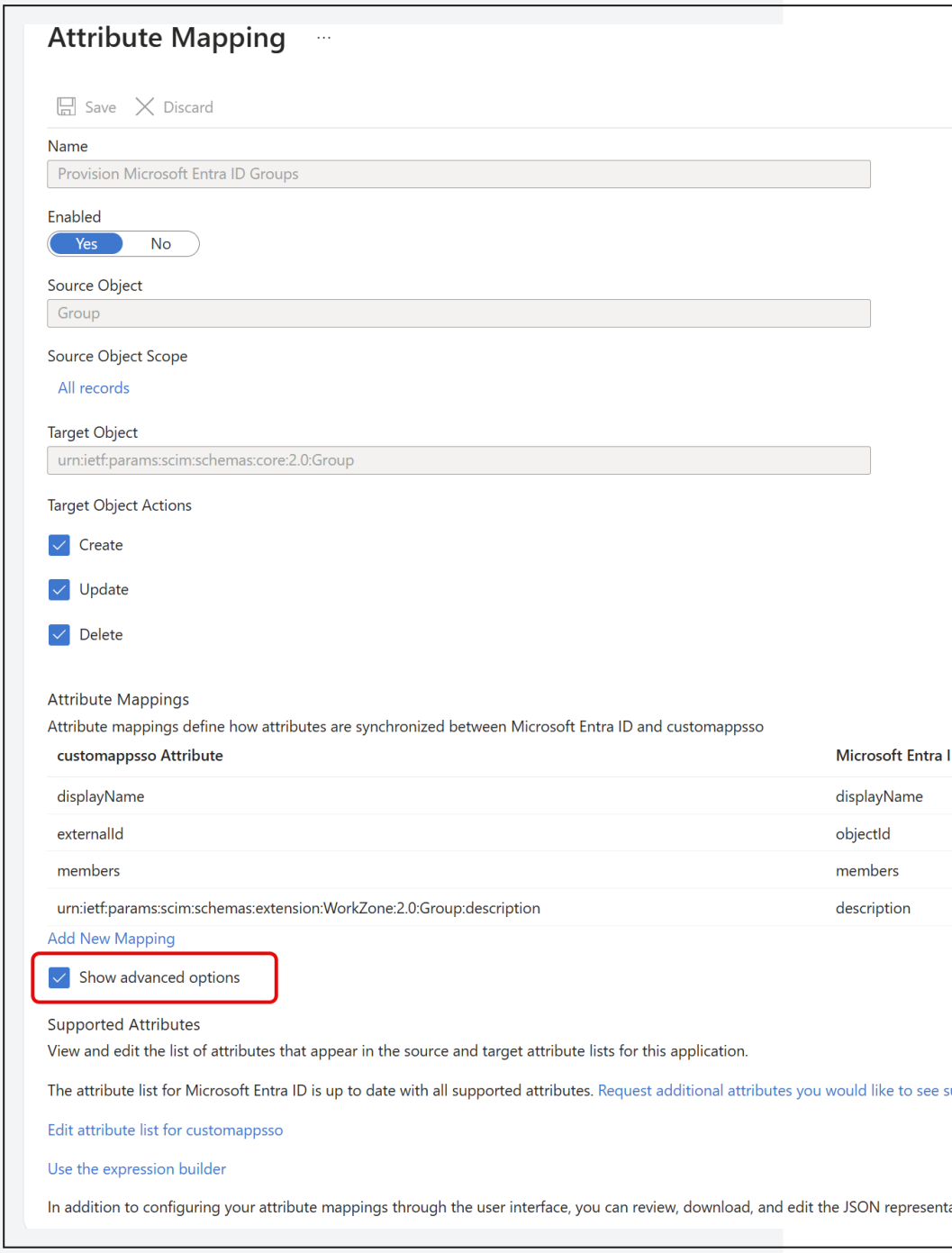
   The group description in Entra ID provides additional information about a group. The description can help you identify the group after the group has been provisioned to WorkZone and added to the **AccessCodeDomain** table as an access code. The group description in Entra ID is not part of the default

mapping scheme, so you will need to add the mapping before you start the provisioning.

Follow the steps below to provision the group description from Entra ID to WorkZone:

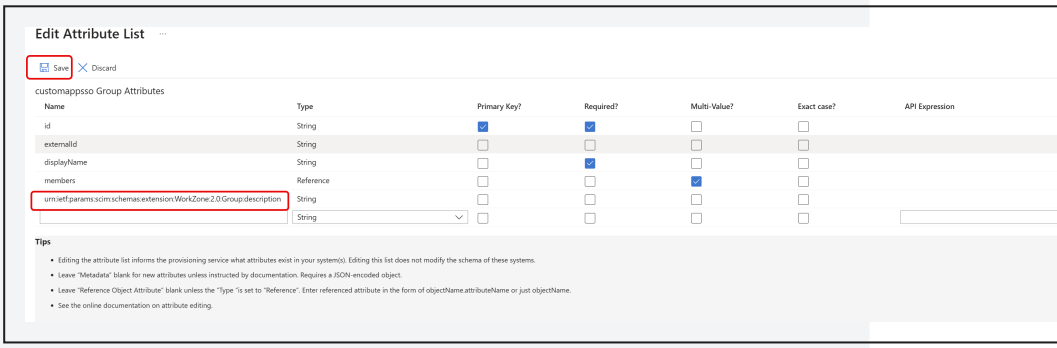
1. Select your "SCIM provisioning" app.
2. Go to **Provisioning** and click **Edit attribute mappings**.
3. Expand **Mappings** and click **Provision Microsoft Entra ID Groups**.
4. On the **Attribute Mapping** page, click **Add New Mapping**.
5. Select **Description** in the **Source attribute** field and **urn:ietf:params:scim:schemas:extension:WorkZone:2.0:Group:description** in the **Target attribute** field.

   > **Important:** If `urn:ietf:params:scim:schemas:extension:WorkZone:2.0:Group:description` attribute is not available for selection, your Azure administrator must add it as follows:
   >
   > a. Under **Provisioning**, click **Provision Microsoft Entra ID Groups**.
   >
   > b. Under **Attribute Mappings**, select the **Show advanced options** checkbox.



c. Click **Edit attribute list for customappsso**.

d. Create a new `urn:ietf:params:scim:schemas:extension:WorkZone:2.0:Group:description` attribute, and click **Save**.



The `urn:ietf:params:scim:schemas:extension:WorkZone:2.0:Group:description` attribute should now appear for selection in the **Target attribute** field.

Guest users

If you want to invite people that are not part of your organization to collaborate with you in WorkZone as guest users, you will need to do additional mapping. See Add guest users.

7. Save the configuration.

5. Assign users and groups to the enterprise application

Assign the relevant users and groups to the application and start the automatic provisioning See Provision Entra ID to WorkZone.

Entra ID runs the provisioning service runs every 40 minutes. During the provisioning, users and groups are added to a set of staging tables in the WorkZone database, and a WorkZone - Cloud Edition application named **SourceImport.exe** creates the WorkZone users and assigns access codes to them based on the data in the staging tables.

It is recommended that technicians set up a scheduled task that will run this application every 40 minutes.

The command line to use is:

```
SourceImport.exe /mode=AZURE_AD /db=<Name of WorkZone database>
```

For example:

```
SourceImport.exe /mode=AZURE_AD /db=db01
```

> **Note:** It may take about 80 minutes for changes to users and groups in Azure to be completed in WorkZone - Cloud Edition.

Staging tables

The three most important tables that are populated with data from Entra ID are:

- SCIM_USER
- SCIM_GROUP
- SCIM_GROUP_MEMBER

The SCIM_GROUP_MEMBER table contains the connections between users and the groups that they are member of as well as connections between nested groups.

Group name restrictions

The following restrictions apply to the AD **Group name (pre- Windows 2000)** field in global security groups used for group access codes.

- All letters are converted to upper case when transferred.
- Maximum 30 characters are converted, additional characters are truncated.
- The only letters and digits allowed are:
  - A to Z
  - 0 through 9.
- The only special characters allowed are:
  - Underscore (_)
  - Dash (-).
- The characters Æ, Ø and Å are converted as shown below:
  - Æ = AE
  - Ø = OE
  - Å = AA.

> **Important:** Æ, Ø, and Å are treated as two characters.

- All special characters other than the above will be removed.
- Space is converted into dash (-).

Provision Entra ID to WorkZone

WorkZone uses users and groups from Entra ID. In WorkZone, users represent WorkZone users and groups represent security codes, access codes, and profiles.

Entra ID runs the provisioning of users and groups from Entra ID to WorkZone - Cloud Edition every 40 minutes. See 5. Assign users and groups to the enterprise application.

Group for WorkZone security codes

The attribute display name must start with a prefix. By default, this is `'WZ_SEC_'` followed by a digit 1 to 9, for example `'WZ_SEC_6'`. The formal display name definition is <prefix><n> where n can be a digit from 1 to 9.

The prefix must be the same for all WorkZone security groups.

Only users can be members of security groups. If a user is member of more than one WorkZone security group, the security code assign to the user will be the highest one.

Group for WorkZone access codes

The attribute display name must start with a prefix. By default, this is `'WZ_ACC_'` followed by the access code, for example `'WZ_ACC_ALLEEMNER'`. The formal display name definition is `<prefix><access code>`.

The prefix must be the same for all WorkZone access codes groups.

Only users can be members of access code groups.

Group for WorkZone - Cloud Edition profile groups

The attribute display name must start with a prefix. By default this is `'WZ_PRO_'` followed by the profile name, for example `'WZ_PRO_OFFICER'`. The formal display name definition is `<prefix><profile name>`.

The prefix must be the same for all WorkZone profile groups.

Members of profile groups can be users, access code groups, profile groups, and security groups.

Only one security group is supposed to be member of a profile. If there are more than one security group, the highest security code is assigned to the profile.

The access code assigned to a profile is the union of access code members in the profile and all other profiles that the profile group s member of directly or indirectly.

> **Example**: If the WZ_ PRO_ OFFICER profile group has the WZ_ ACC_ ALLEEMNER access_ code group as member, and the WZ_ PRO_ ADMIN profile group has the WZ_ ACC_ ADMIN access_ code group and WZ_ PRO_ OFFICER profile group as mem-

ber, then WZ_ PRO_ ADMIN profile group will be assigned ALLEEMNER and ADMIN access code.

A user's security code

If a user is member of more than one security group, directly by being member of a WorkZone security group or indirectly by being a member of a WorkZone profile group, the following rule applies:

- Direct membership overrules indirect membership, and the highest security code is used.
- If a user is not member of any WorkZone security group, the user is not replicated to WorkZone.

A user's access codes

The access code that will be assigned to a user is the union of the access code from the access code group that the user is member of and access code that is assigned to the profiles that the user is member of.

Mapping of columns for a user

Entra ID	WorkZone - Cloud Edition	Note
User principal Name	Users.user_ name, Name.name_ code (name_ type = 'M') Employee.name_ code	The characters from beginning up to the @ character is transferred, it must not exceed the number of characters defined in contact type for name_ type M, no more than 30 characters.
User principal Name	Users.upn	Must be maximum 512 characters long.

Entra ID	WorkZone - Cloud Edition	Note
First name	Name.name1 Employee.name1	Maximum 60 characters is transferred.
Last name	Name.name2 Employee.name2	Maximum 60 characters is transferred.
Steeet address (work)	Name_address.address1 Name_address.address2 Name_address.address3	Maximum 150 characters in address1, 2, and 3, but trying to split by a blank character. It means that maximum 450 characters will be transferred.
Country or region (work)	Name_address.-country	Only transferred, if it matches a country in the WorkZone country table. (ISO alfa2 standard).
Zip or postal code (work)	Name.post_code	Only transferred, if it matches a postal code in the WorkZone postcode table.
Office phone (work)	Name_address.-phone_no	Must be maximum 25 characters long, otherwise it will not be transferred.
Mobile phone (mobile)	Name_address.-cell_phone_no	Must be maximum 25 characters long, otherwise it will not be transferred.
Email (work)	Name.email	Must be maximum 255 characters long, otherwise it will not be transferred.

Creating Organizational units for WorkZone Cloud Edition

If you are operating WorkZone Cloud Edition, the creation and maintenance of your organizational units and unit hierarchy must be performed in WorkZone Configurator > **Organization** > **Organizational units** because Microsoft Entra ID does not currently contain features for the creation and maintenance of organizational units required for WorkZone user administration and hierarchical structure.

> **Prerequisite:** You must be assigned the AFDADM access code to create and edit organizational units in your WorkZone Cloud Edition installation.

On- premise WorkZone installations must utilize an on- premise Microsoft Active Directory, which does contain features for the creation and maintenance of organizational units.

Assigning WorkZone users to organizational units

For WorkZone Cloud Edition, WorkZone users cannot be assigned to organizational units directly in the Microsoft Entra Connector. Instead, WorkZone users created in the Microsoft Entra ID can be assigned to organizational units in WorkZone Configurator > **Organization** > **Users**.

> **Prerequisite:** You must be assigned the USERADM access code to view and assign units to users in your WorkZone Cloud Edition installation.

See also:

Organization units (for WorkZone Cloud Edition)

Users (for WorkZone Cloud Edition)

Add guest users

You can invite people that are not part of your organization to collaborate with you in WorkZone as guest users. You can, for example, collaborate on cases and documents with users across organizations, or you can share access to a WorkZone instance with, for example, subject matter experts or consultants to collaborate on and share the information that they need for specific purposes.

To set up guest users, follow these steps:

1. Set up SCIM provisioning of guest users from Entra ID to your WorkZone tenant.
2. Invite the guest users into your tenant.
3. Assign WorkZone groups to the guest users.

> **Note:** WorkZone Mobile does not yet support guest user access.

Set up SCIM provisioning of guest users

> **Prerequisite:** Upgrade to WorkZone 2023.2 before you configure guest users.

Guest users do not have a UPN (User Principal Name) as part of their token as internal WorkZone users do when they sign in to your WorkZone tenant, see Enroll WorkZone - Cloud Edition in Azure and set up SCIM provisioning. When provisioning guest users to WorkZone, Microsoft Azure Object ID is used instead of UPN to identify users.

To make sure that guest users can log in to WorkZone after SCIM provisioning, you need to map Azure Object ID to the **ExternalId** attribute.

Map Azure Object ID

1. Sign in to the Azure Portal as an Entra administrator.
2. Go to **Enterprise Applications** and select your "SCIM provisioning" app.
3. Go to **Provisioning** and then click **Edit attribute mappings**.
4. Expand **Mappings** and click **Provision Azure Active Directory Users**.
5. On the **Attribute Mapping** page, click the **ExternalId** attribute, and change the

source attribute to **ObjectId**. If the **ExternalId** attribute does not exist, you can add it.

Invite guest users

Invite guest users in to your tenant from the Azure Portal. Guest users use their own accounts. You must have a role as an Entra administrator to be able to add guest users. Read more about adding guest users and sending invitations in the Microsoft Entra documentation, for example in the Microsoft article Quickstart: Add a guest user and send an invitation.

Naming convention for guest users

When a guest user that has an email address with another domain than your primary domain, the user name of that guest user will be <Username_ 1>, where the suffixed number is a running number that ensures that no username is used twice for different users.

> **Important:** It is recommended that your organization uses unique usernames for your users, even if you use subdomains. If your organization does not maintain a unique naming of their users across the primary domain and its subdomains, non-unique users will named as guest users.

Example

At your organization, your domain is *organization.com*. Your e- mail address is *abc@organization.com* and therefore, your WorkZone username is 'abc'.

You create a guest user account for an external consultant, whose e- mail address is 'abc@othercompany.com'. WorkZone does not recognize this domain as your primary domain, and therefore creates the user as abc_ 1.

The user abc_ 1's colleague is also invited to work on the project as a guest user. Their e-mail address is xyz@othercompany.com. Even though there is no other user in your organization with that user name yet, the user is still created as xyz_ 1, because their domain is not the same as your primary domain.

Assign groups to a guest user

1. Sign in to the Azure Portal as an Entra administrator.
2. Navigate to the external users, you have invited.
3. Go to **Groups** to add WorkZone groups that represent security codes, access codes, and profiles. See Provision Entra ID to WorkZone.

Remove a guest user

Delete a user from Entra ID

When you delete a guest user from your WorkZone tenant, the guest user will be able to work and refresh an already opened WorkZone session for some time, depending on the lifetime of the token. The user will not be able to log in to WorkZone on a new tab.

Close a contact in WorkZone

If you set an end date on guest users in WorkZone, the users will be deleted from Entra ID. See Close a contact.

Re- add a guest user

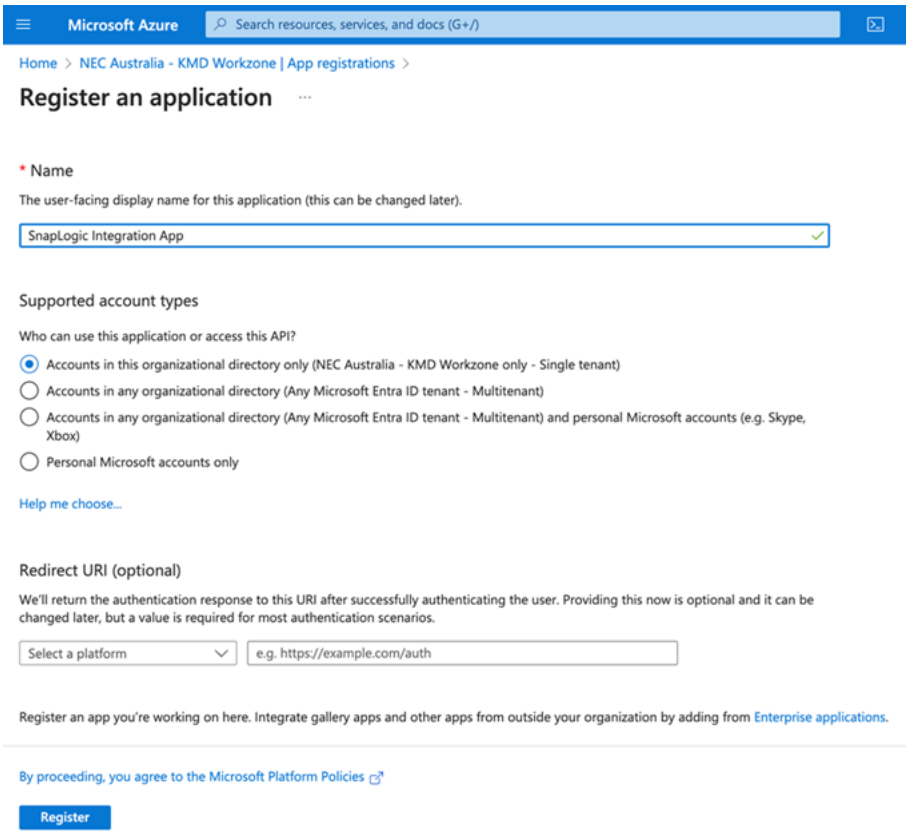
If you re- add a guest user, the guest user's UPN (email) is used to see if the user has had access to WorkZone previously.

Set up third-party integrations in Azure

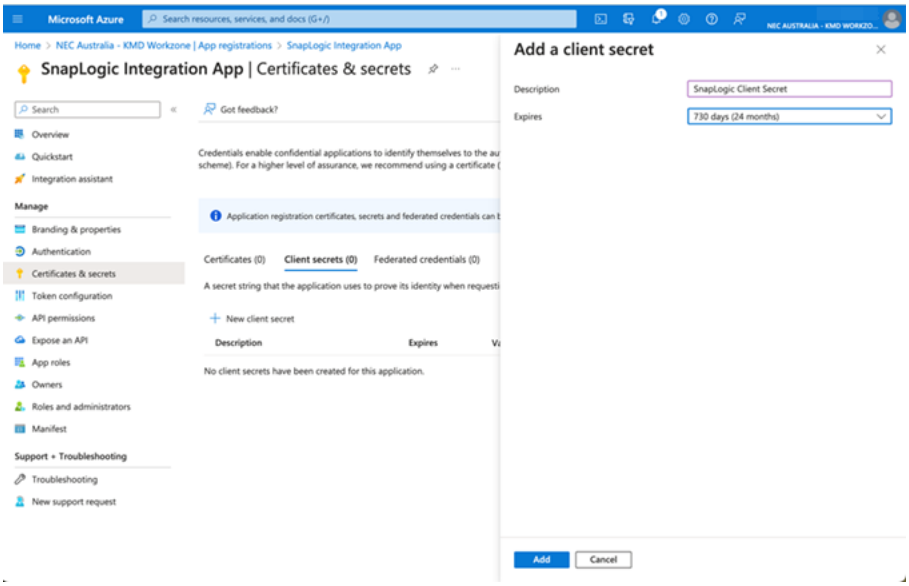
To configure a third- party app to integrate with WorkZone, you need first to register the third- party app in your Entra tenant, and then configure the access to WorkZone in WorkZone Configurator. This topic describes how to set up integration accounts in Azure Portal and get the information that you to need to configure the integration in WorkZone Configurator. The third- party app SnapLogic is used as an example in the procedure below.

Set up an integration account in Azure

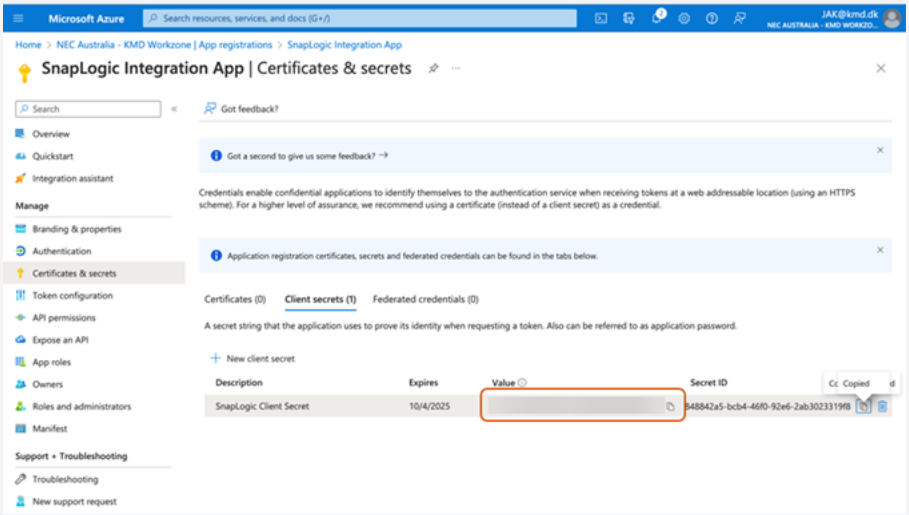
1. In your Entra tenant, go to **App registrations** and create a new app registration. You only need to fill in the name of the app, and then click **Register**.



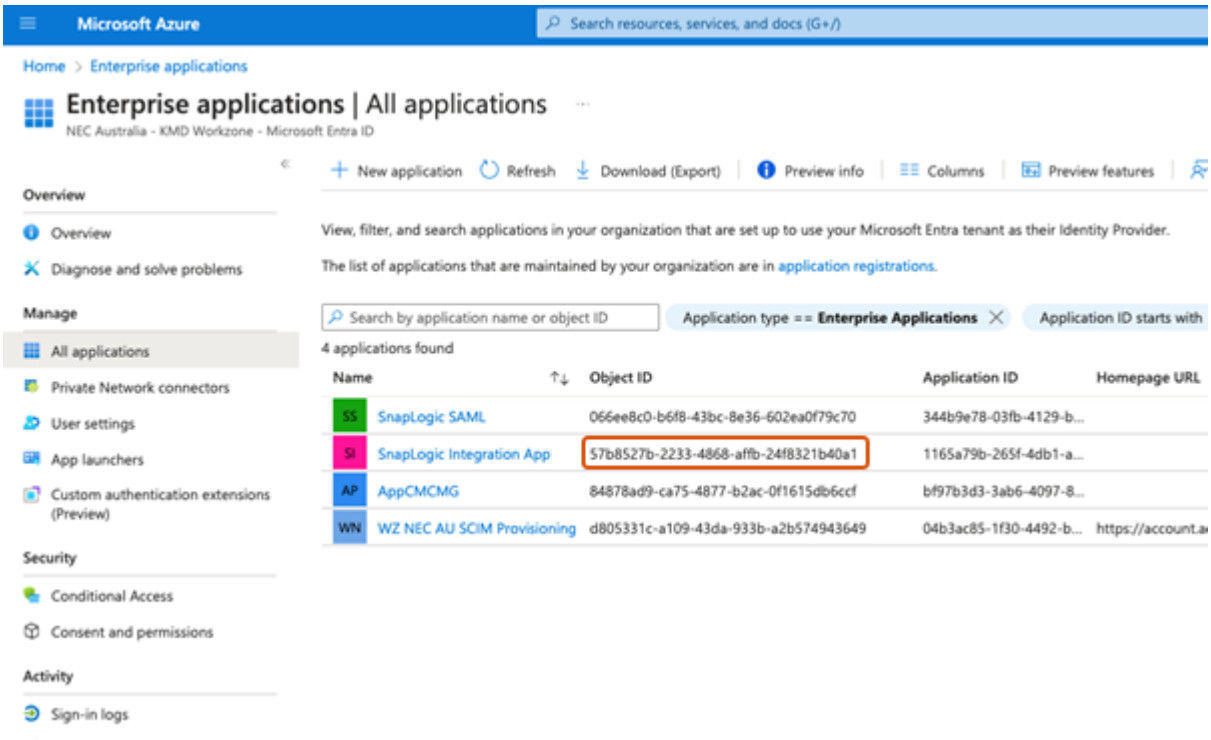
2. Go to **Certificates & secrets**. Add a client secret, and click **Create**.



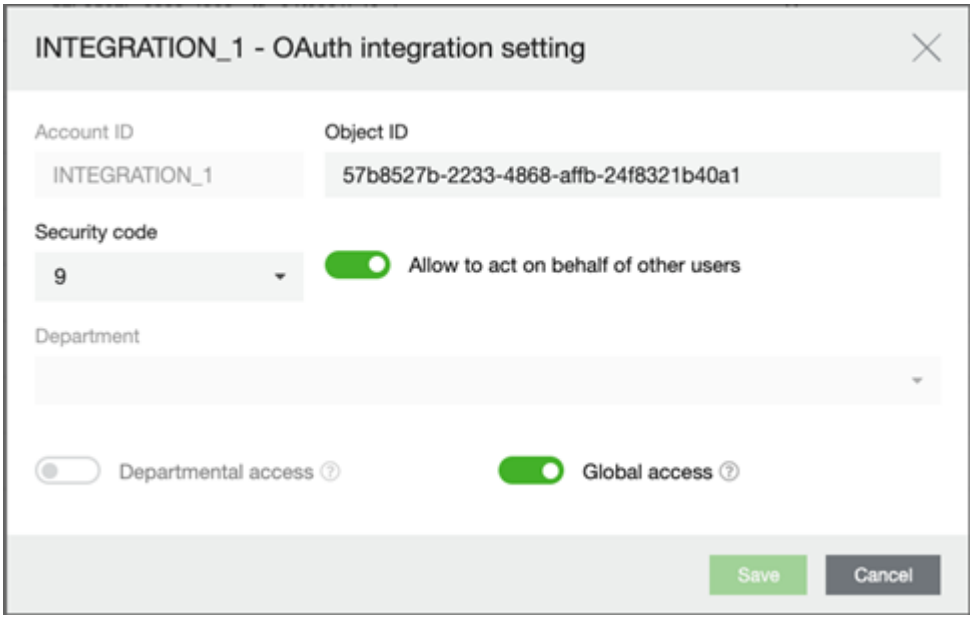
Important: Immediately after clicking **Create**, copy the client secret and paste it to, for example Notepad, as you will need it later. This is the only time that the client secret is shown. If you do not copy it right away, then you have to create a new client secret.



3. Go to **Enterprise applications** > **All applications** to see the object ID for the app registration, in this example SnapLogic app.

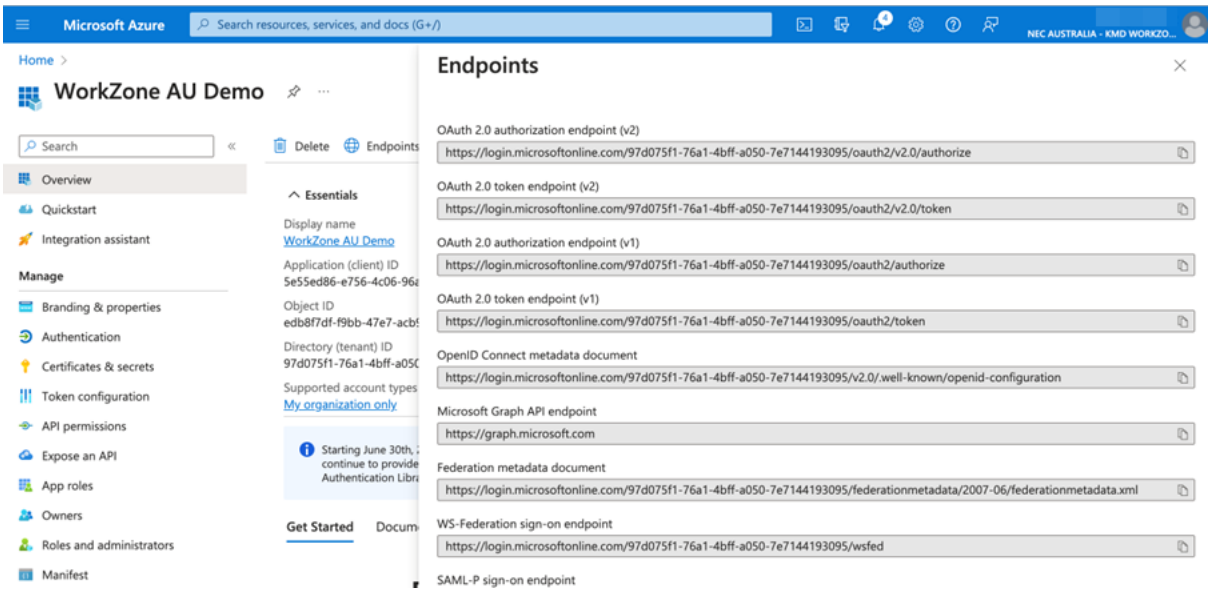


4. In WorkZone Configurator, go to **Global** > **OAuth Settings** > **Integrations** to set up the OAuth integration. Follow the steps in the WorkZone Configurator guide (Integrations tab). Enter the newly created object ID for the corresponding enterprise application in the **Object ID** field. In this example, it is the object ID of the SnapLogic app (see step 4).

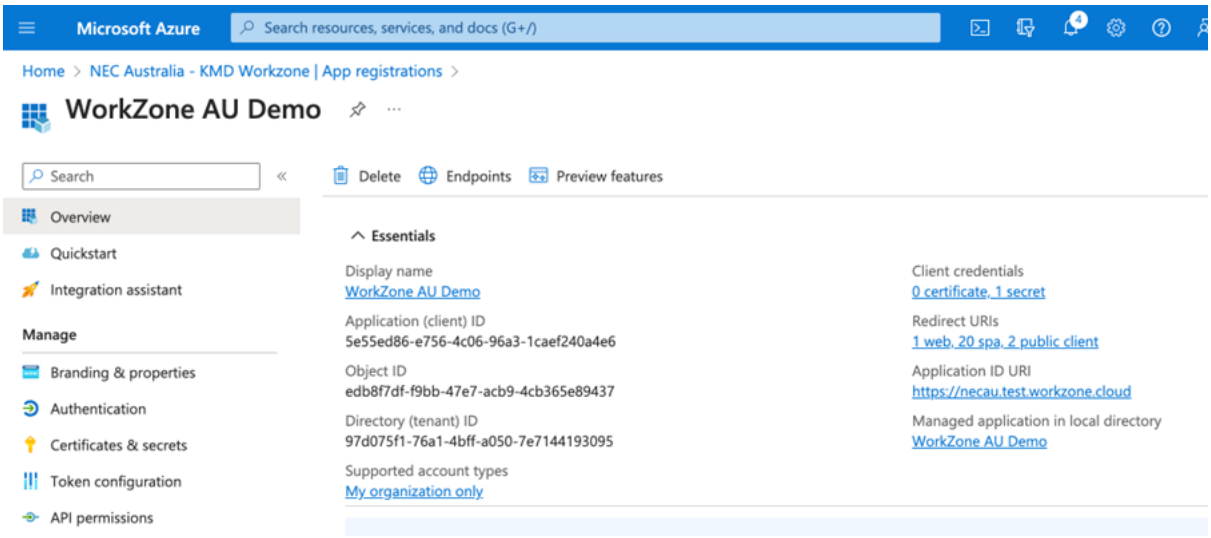


5. Note down the Client ID, the Tenant ID, the Client Secret from before (see step 3), the OAuth2 endpoints and the WorkZone Application ID URI (both which can be found on the App Registration for WorkZone).

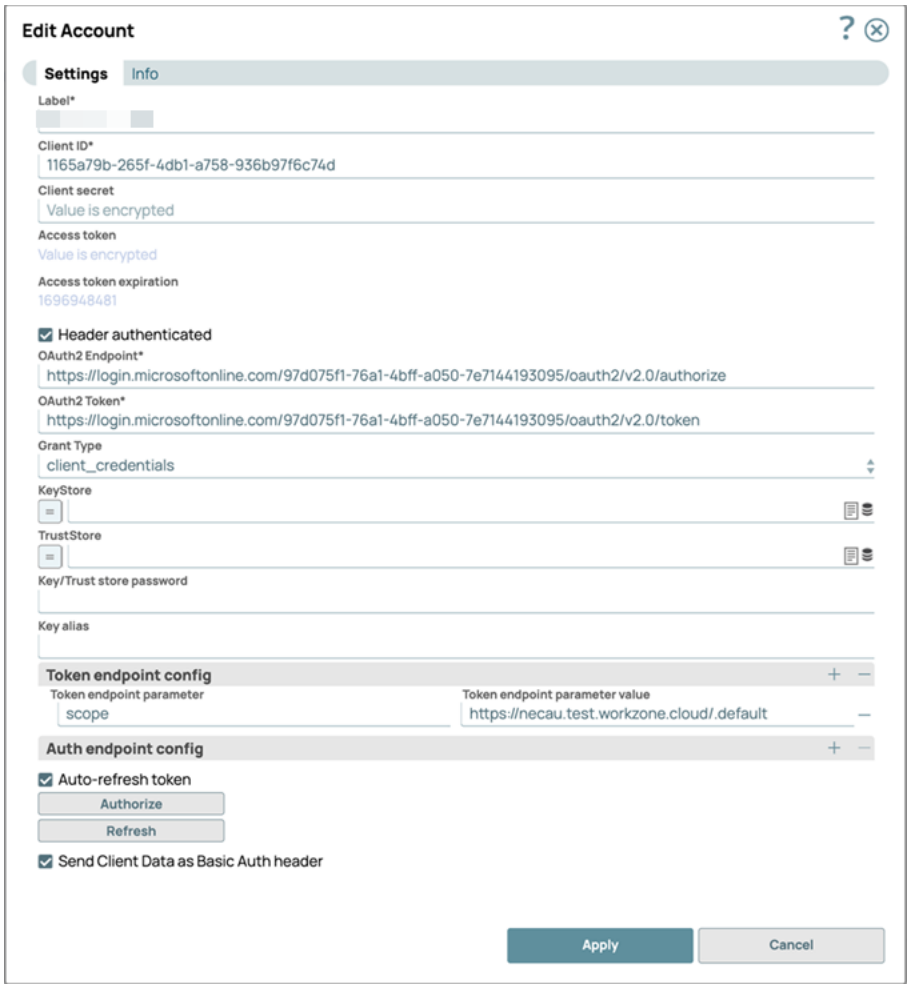
Oauth2 endpoints:



Application ID URI:



Example: SnapLogic settings for a WorkZone OData account



Access control using Microsoft Entra Conditional Access

In WorkZone, it is your organization's security policies that control the access. When a user logs in, the request is sent to your tenant, where Conditional Access policies determine whether access should be granted. This means that your organization has full control over which devices, locations, accounts, and log in methods (for example, multifactor authentication) are allowed.

To ensure effective and secure access management, we recommend utilizing your organization's existing Conditional Access policies to define specific rules for who can log in and how. For example, you can restrict access to only approved devices, preventing employees from inadvertently logging in from personal devices or external networks. This approach is also used in other systems, such as Office 365.

We do not recommend a whitelist- based solution for access management due to its complexity and ongoing maintenance requirements for both your organization and KMD. A whitelist- based solution presents several challenges:

- **Mobile devices**: To secure mobile access, it requires routing through the organization’s network, which can slow down the experience and require setup of mobile VPN solutions.
- **Guest access and external consultants**: External users, such as KMD consultants, will not be able to access the system outside your network, which can complicate remote support and setup.
- **Third- party integrations**: Integrating with external systems require access to your network or continuous whitelisting, which can lead to administrative challenges.

Instead of whitelisting, we recommend using Conditional Access to achieve the desired security control in a flexible and maintenance- friendly manner.

We also advise against using geographic IP filtering as a security measure. Hackers often use VPN solutions to hide their true location. VPNs can bypass geo- blocking on streaming services and mask a user’s actual location providing a false sense of security and creating access issues for legitimate users working from abroad or via changing networks.

We support using the organization’s existing security setup, but we are not specialists in setting up Conditional Access policies. Therefore, we recommend involving your IT managers or security advisors to ensure that access policies fulfill your needs and security requirements.

Read about Microsoft Conditional Access in Microsoft Entra Conditional Access documentation.

Replicate WorkZone users and access codes from a local AD

If you use WorkZone version 2024.1 or newer versions, you must use Entra ID to authenticate your WorkZone users. If your organization has a local Active Directory, it is possible to replicate the users, access codes, and organizational units that you have in that local AD to WorkZone.

This setup is relevant for organizations who upgrade from an on- premises version of WorkZone where the Authentication was locally stored, or for organizations that have a need to create and maintain complex access structures from a local AD.

> **Prerequisite:** Before you can get started with replicating users, access codes, and OU's to Entra ID, you must first:
>
> - Create and configure the relevant AD groups and have a valid ADreplicator config file. See Pre- configure with the wizard.
> - If you have user provisioning set up using SCIM, you need to disable it.
>
> See Access Active Directory and the rest of the AD guide for more information.

To get started, you must:

1. Install the WorkZone ADreader service on an internal server and make sure that it has access to the local domain. See Install the AD reader.
2. Create an application registration in Entra ID for the WorkZone ADreader service to connect to WorkZone and update users. Configure the replication settings.
3. Set the service to run at a schedule to apply on- going changes to the local AD in the WorkZone database.

Active Directory replication from an on-premises AD

In a situation where the domain controller (and therefore the active directory) is located on an on- premises machine and WorkZone is installed and runs in an Azure environment, you must still be able to replicate the active directory structure from the on- premises domain controller to the WorkZone database in the Azure environment.

WorkZone Cloud and Active Directory synchronization diagam

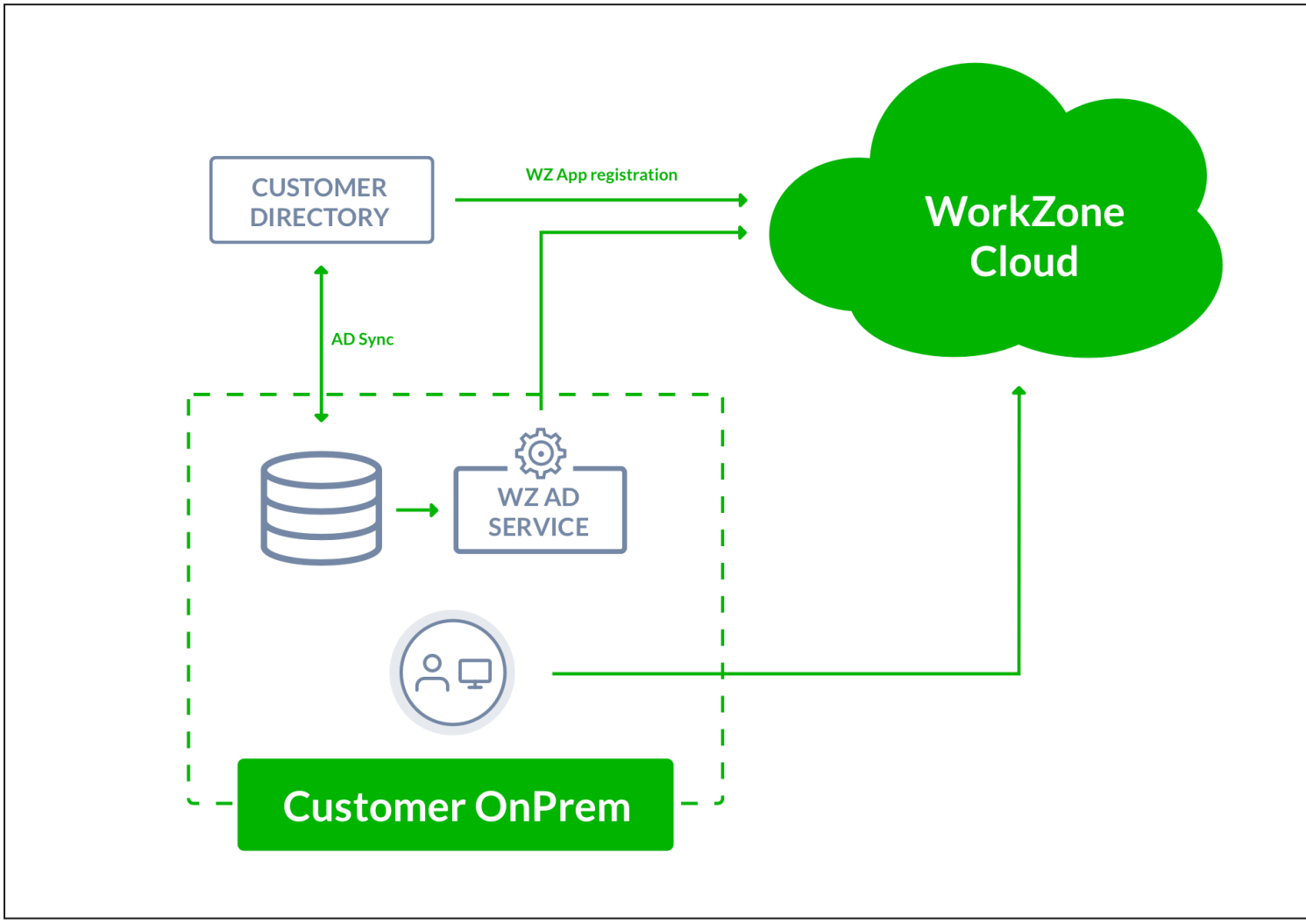


Diagram notes

In this example, an on- premises setup contains the Active Directory servers and data as well as clients. WorkZone is also installed on the on- premises site in order to run the WorkZone Active Directory service for synchronization purposes.

The customer setup also includes synchronization with Entra ID as well as utilization of the Microsoft Office 365 suite in the Azure cloud environment with Entra ID users.

The organizational structure as well as other WorkZone- relevant data from the Active Directory is published to the WorkZone public endpoint.

User authentication is performed in the customer's Entra ID, where an app registration is used for WorkZone Cloud to authenticate the users.

The customer has an on- premises setup that contains the Active Directory servers and data as well as clients. A WorkZone Active Directory is required on the on- premises site in order to synchronize organizational structure as well as access codes.

Customers connect to the public endpoint. The public endpoint only grants access to WorkZone services such as OData, WorkZone Client, and WorkZone Configurator, but does not grant access to internal cloud infrastructure such as virtual machines and other "hardware" based cloud services.

Differences between an On- premises and WorkZone Cloud Active Directory replication

Running this type of replication in a WorkZone Cloud setting closely resembles running an Active Directory replication in an on- site setting with an on- site domain controller and network users using windows authentication but there are several important differences due to the capabilities of the Entra ID and the two different environments.

These differences are:

- You must set up the active directory replication to export the active directory structure from the on- premises domain controller to the WorkZone database in the Azure environment. The export also creates an update task in the WorkZone database on the Azure environment.
  You can set up the program that exports the Active Directory structure as a recurring windows task. This ensures replication of the active directory structure at a time that fits your organizations' non- working hours, maintenance schedule, and back- up timetable.
- A Windows service is installed when WorkZone is installed in the Azure environment.
  The service is enabled and automatically started on the WorkZone and will execute the update task and update the WorkZone database with the active directory structure that is exported by the active directory reader on the on- premises server that is connected to the domain controller.

See also

- Automation of active directory replication

Upgrade from an on-premises ADReplicator

This topic contains relevant information for users that want to upgrade from using the sjActiveDirectoryReplication.exe program (AD Replicator) to using the wzActiveDirectoryReader.exe program (AD Reader).

The AD Replicator is an on- premises service that reads data from your Active Directory and applies it to WorkZone via a direct ODBC database connection. The wzActiveDirectoryReader.exe file is installed on an on- premises server that is connected to the Domain Controller. Once installed correctly, the AD Reader reads data from your Domain and stores it via OData in JSON format on your WorkZone database.

> **Note:** The AD Reader has the same user interface as the old AD Replicator.

The Active Directory Writer service

The Active Directory Writer is a container service that is installed with the rest of the WorkZone Cloud containers. It transforms domain data that is saved by the AD Reader and applies it to WorkZone. Beginning from WorkZone 2025.0, AD Reader is no longer configurable via WorkZone Configurator. See Install the AD reader and Configure the replication settings

Install the AD reader

The **wzActiveDirectoryReader.exe** program must be installed on an internal on- premises server that has access to the local domain controller machine because it opens the **Active Directory Connector** form which it uses to find, export, and transfer the active directory structure to the WorkZone machine in the Azure environment.

> **Prerequisite:** Before you install the AD reader, there are some required changes on both the customer side and in the WorkZone database. It is necessary that you synchronize your work with the WorkZone technician who manages your upgrade/installation. See the required tasks below.

Before you upgrade the AdReader/WorkZone

> **Important:** When upgrading from WorkZone 2024.5 or older to WorkZone 2025.0 or newer versions, you must create an app registration in your Entra ID tenant before the WorkZone upgrade, and send the Enterprise Application Object ID to KMD. See Configure the replication settings.

1. The KMD technician must add the Object ID that you send to them to the WorkZone database before you can continue.

```
update users set oid='<Enterprise Application Object ID>'
where user_name = 'SJADREPLICATORUSER';
```

```
commit;
```

2. You can now your make your changes to the wzActiveDirectoryReader replicator config file. If you use a Client Secret, please note that the Client Secret encryption must be done on the new AD Reader and not in the old AD Connector.

Install the wzActiveDirectoryReader.exe program on an internal server

1. On the machine where WorkZone is installed, locate the **wzActiveDirectoryReaderSetup.msi** installer. The default path to the program is `C: > Program Files(x86) KMD > WorkZone > Program > wzActiveDirectoryReader`. This location may be different if you have changed the default installation location of your version of WorkZone.
2. Copy and paste the **wzActiveDirectoryReaderSetup.msi** installer to the on- site domain controller machine that contains the active directory for the on- site users that you want to replicate to WorkZone.
3. Run the **wzActiveDirectoryReaderSetup.msi** installer.
4. When the installation is finished, the **wzActiveDirectoryReader.exe** program will be located in the `C: > Program Files(x86) KMD > WorkZone > Program > wzActiveDirectoryReader` folder.

See also

Configure the replication settings

WorkZone Active Directory Connector

To make Active Directory comply with WorkZone once the data is transferred, you must perform initial configuration using the WorkZone Active Directory Connector.

You can access the application from the default path at (x86)\KMD\WorkZone\Program\wzActiveDirectoryReader. Run the `wzActiveDirectoryReader.exe` application as administrator.

WorkZone Active Directory Connector facilitates the transfer (replication) of data from Active Directory to WorkZone. The administration of users, user security codes, access codes, units, and committees are maintained in AD but this data must continually be updated and transferred to the WorkZone database.

In order for WorkZone to correctly receive the transferred data, it is essential that the Active Directory configuration and the WorkZone configurations are aligned.

The tasks of transformation of data and alignment are handled by the WorkZone Active Directory Connector.

Configure the replication settings

Defining the replication settings in the WorkZoneActive Directory Connector form for an Entra ID authentication is identical to defining the replication settings, for example, for an on- site client- server environment, but you must also define the Entra ID app registration for the Entra ID authentication in WorkZone. User authentication is performed in Entra ID where an app registration is used for WorkZone Cloud to authenticate the users.

> **Important:** The AD Connector only works with Entra ID. That means that the AD Connector must be created as a separate application in the Entra tenant. There is a dedicated script for that. It registers Entra application called kmd- workzone- ad- reader. In multi- tenant architecture where WorkZone is hosted on another server than your tenant application, the kmd- workzone- ad- reader must be registered as an application in your Entra ID tenant.

Register the app with the script

To register the application in your Entra tenant, you can run the designated script that is delivered with the wzActiveDirectoryReader installer.

Run the script with the following parameter:

```
\AdReaderConfigure.ps1 -TenantId [guid]
```

When you have run the script, it should provide the following output. It is important that you copy and paste this information locally as you will need it later.

```
ClientPortalUrl: https://portal.azure.com/
#view/Microsoft_AAD_RegisteredApps/Application
MenuBlade/~/Overview/appId/[Guid: Application Client ID]
Client ID: [Guid: Application Client ID]
Client Secret: [Application Client Secret]
Enterprise Application Object ID: [Guid: Application Service Principal]
```

Register the app manually on the Azure Portal

The first steps in the app registration process is similar to third- party app registration. See Set up third- party integrations in Azure.

1. In your Entra tenant, go to **App registrations** and create a new app registration.
2. Fill in the name of the app (The recommended name is `kmd-workzone-ad-reader`), and click **Register**.
3. Go to **Certificates & secrets**, add a client secret or a certificate, and then click **Create**.

> **Important:** Immediately after clicking **Create**, copy the client secret and paste it to, for example Notepad, as you will need it later. This is the only time that the client secret is shown. If you do not copy it right away, you have to create a new client secret.

4. Go to **Enterprise applications** > **All applications** to see the object ID (Enterprise Application Object ID) for the app registration.

Configure active directory replication for an Azure environment

You can either create a new active directory connector configuration with the wizard and then configure the file manually, or edit an existing configuration directly.

1. On the on-site server, run the **wzActiveDirectoryReader.exe** program with administrator privileges to open the **WorkZoneActive Directory Connector** form.
2. In the **WorkZoneActive Directory Connector** form, click **Edit** to open the **WorkZone Active Directory Connector Configuration** form.
3. In the **WorkZone Active Directory Connector Configuration** form > **Client Secret** field, enter the Entra ID authentication client secret that you have saved during one of the previous steps.
4. Set up all other active directory connector configuration settings as you normally would for replicating the active directory in a solely on-site environment and click **Save** to save your changes.

The Entra ID authentication client secret or certificate for active directory replication

To connect to the WorkZone database in the Azure environment, you must specify the Entra ID authentication client secret in the **WorkZone Active Directory Connector Configuration** form or the certificate path in the configuration file. If the Entra ID authentication client secret is incorrect or omitted, the Active Directory replication will fail.

See also:

- Install the AD reader

User account permissions

User account

It is important that the user account that is used to run the Active Directory Connector has the necessary permissions to run the Active Directory Connector before you start the configuration.

User permissions

User permissions are essential in two aspects:

- The permissions that a user needs to run the wizard in Active Directory Connector.
- The permissions that a user needs to run the scheduled task transfer of data from Active Directory to WorkZone.

Permissions to initiate the wizard

The first time you run WorkZone Active Directory Connector (`wzActiveDirectoryReader.exe`), the **WorkZone Connector Setup** wizard is initiated. It guides you through the alignment between Active Directory and WorkZone. You only have to establish this alignment once. It is important that you have write access, for example as an Administrator, to the **WorkZone Connector Setup** wizard's installation folder because the config file needs to be saved there.

> **Note:** If you want to represent Organizational units in WorkZone as Active Directory groups instead of Active Directory organizational units, you must start the Active Directory connecter with the `useGroupAsOU` option, see also Command line parameters.

The wizard writes directly to AD and it is therefore essential that the user account has the necessary permissions to create the following objects in AD:

- Organizational unit with the `ScanJourCaptiaAdministration` title in the root of Active Directory.
- 11 universal distribution groups in the subtree of `ScanJourCaptiaAdministration` Organizational unit

- `ScanJourCaptia<database name><i>` I =1- 9 - used to align users' security levels. Each distribution group represents equal security groups in WorkZone.
- `ScanJourCaptia<database name>Groups` - used to identify the access codes.
- `ScanJourCaptia<database name>Committees` - used to identify committees.
- `ScanJourCaptia<database name>OUs` - used to identify the root Organizational units. It is only added if the option **useGroupAsOU** is used.

Note: `<database name>` must be substituted with the current ODBC database name.

To create these 11 groups, click **Create** in the **Active Directory Connector** wizard. See Pre-configure with the wizard.

Permissions to run a scheduled transfer task

To run a scheduled task of transferring data from Active Directory to WorkZone, you must use a user account with rights to;

- **View** the relevant Organizational unit's, groups, and users in Active Directory.
- **Write** entries in the event log.
- **Create** and **update** in the following sub key entries in the Windows Registry:

```
HKLM\SOFTWARE\SCANJOUR\SJAD class-
="code">HKLM\SYSTEM\Cu-
rrentControlSet\Services\Eventlog\Application
```

Pre-configure with the wizard

The wizard guides you through the following steps during the pre- configuration of Active Directory Connector:

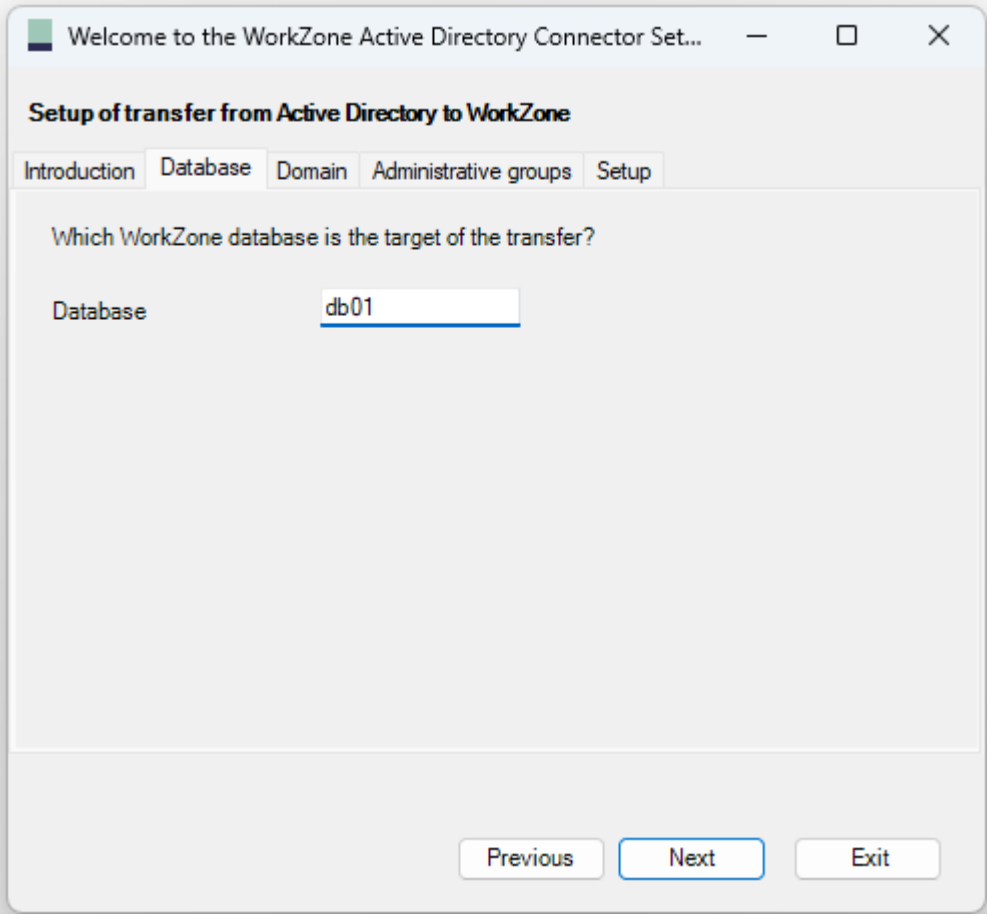
- Specification of the database name.
- Specification of the domain server name.
- Initiation of the needed distribution groups in WorkZone dedicated AD.

- Initiation of the creation of the configuration file that secures the alignment between AD and WorkZone.
- Creation of a desktop shortcut to Active Directory Connector for easy maintenance access.
- Configuration of a scheduled task which periodically automatically secures alignment of data.

Preconfiguration wizard

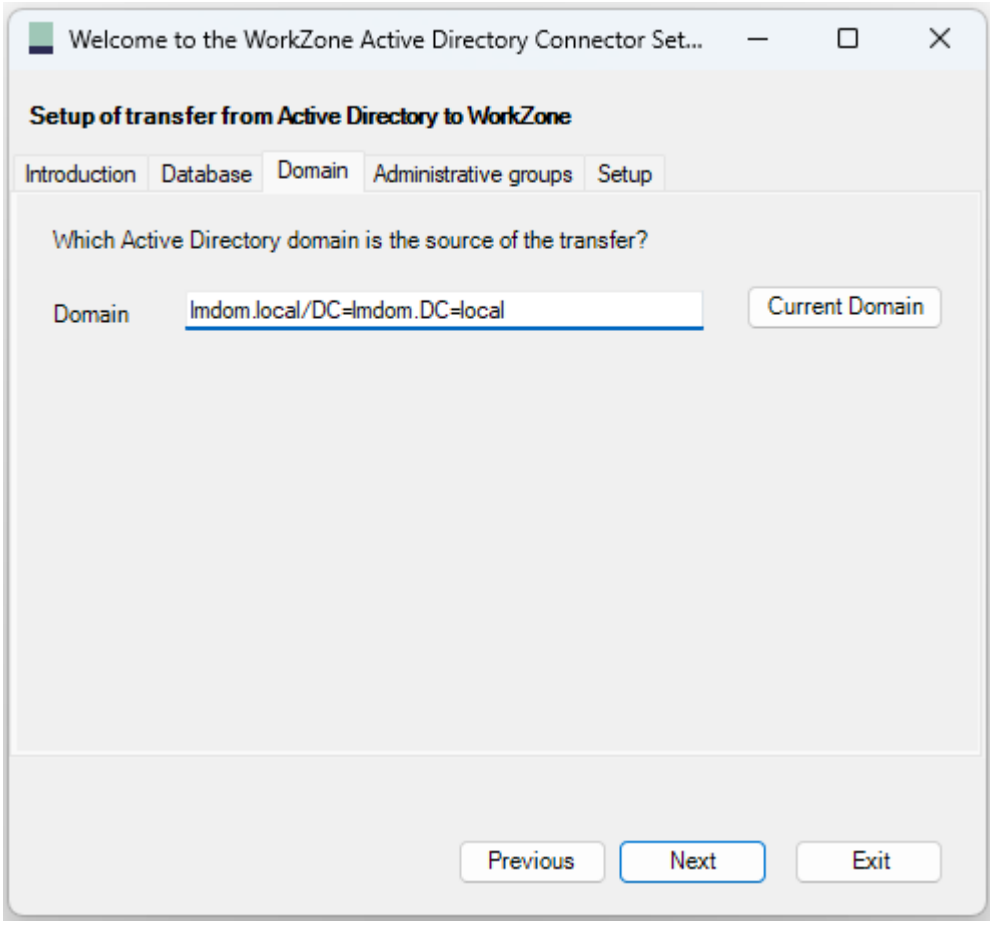
1. In the WorkZone program folder `C:\Program Files (x86)\KMD\WorkZone\Program\wzActiveDirectoryReader`, double- click the `\wzActiveDirectoryReader.exe` file to start the Active Directory Connector Wizard.
2. Click **Next**.
3. On the **Database** tab, enter a name. The field is only used to generate the configuration file name and Administrative Group prefixes and is not used for connection purposes.

4. Click **Next**.



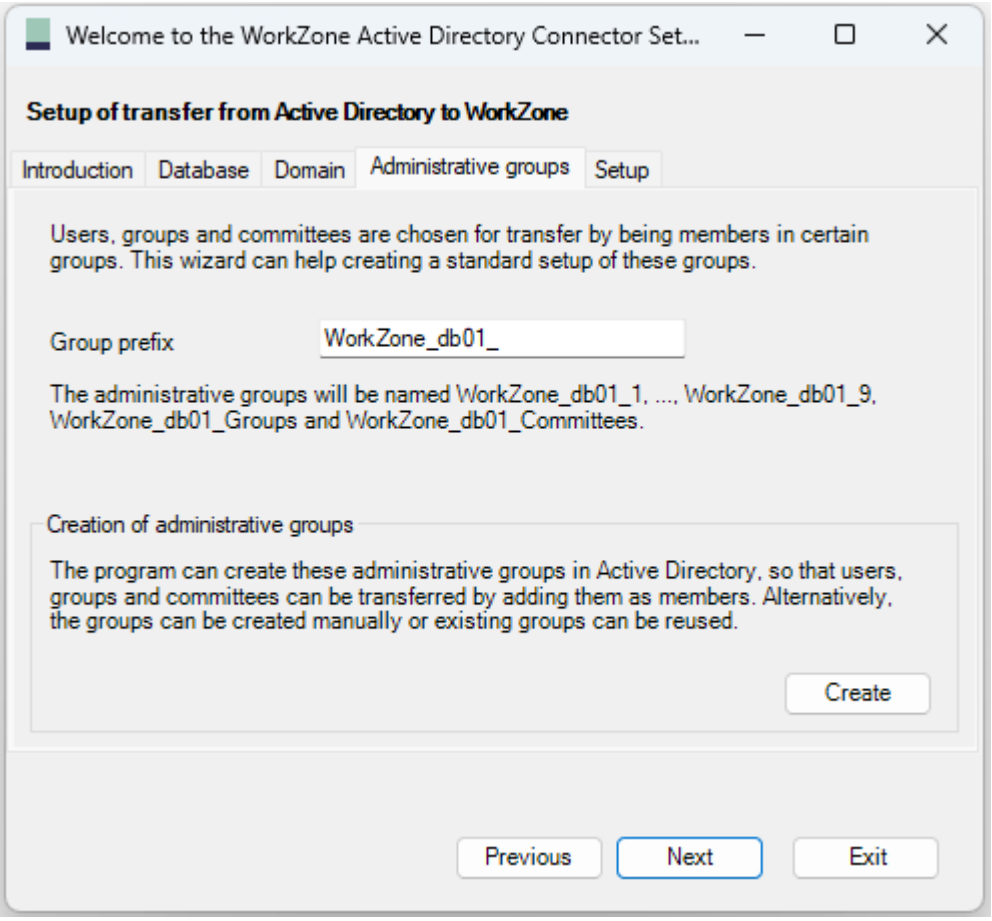
5. On the **Domain** tab, click **Current Domain** to insert the name of the current domain, or enter the name of your server domain in the **Domain** field. Click

Next.

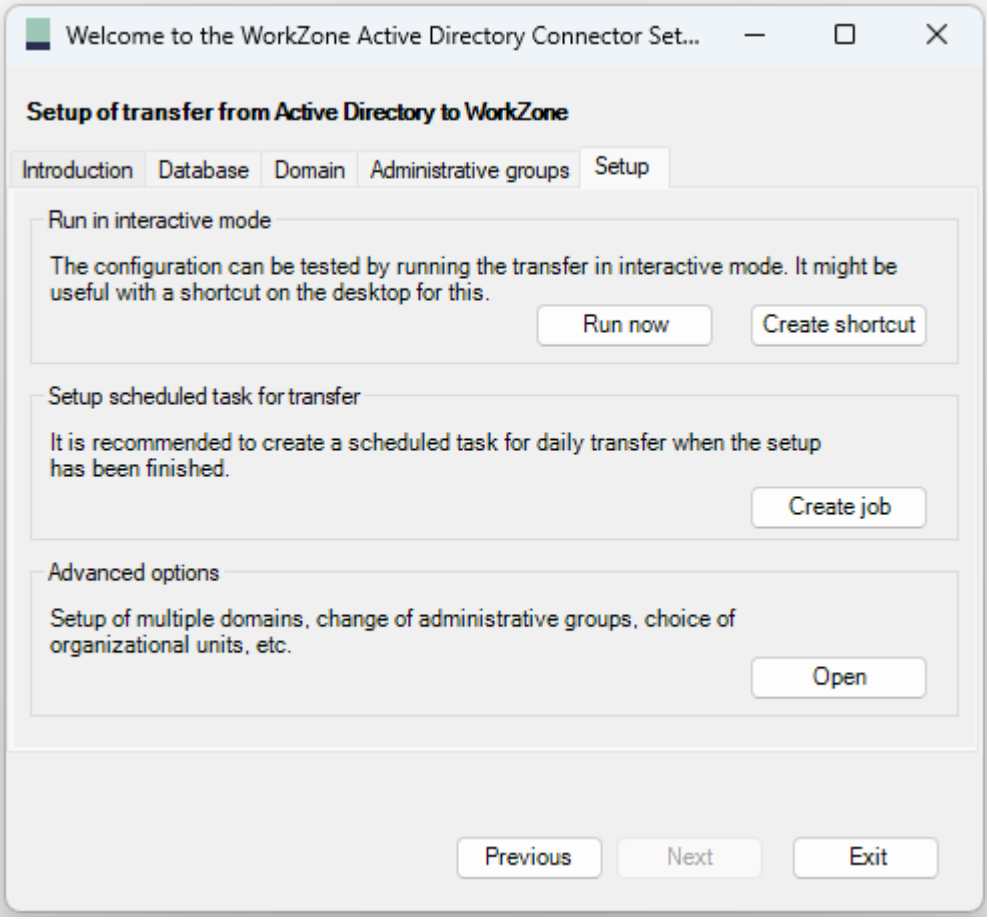


6. On the **Administrative groups** tab, in the **Group prefix** field, the wizard suggests a prefix for the 11 distribution groups that it is about to setup for the transfer of security codes, committees and group access codes – `ScanJourCap-tia<database name>`.

   To enhance legibility, it is recommended that you add a separating character such as a dash after the `<database name>`.

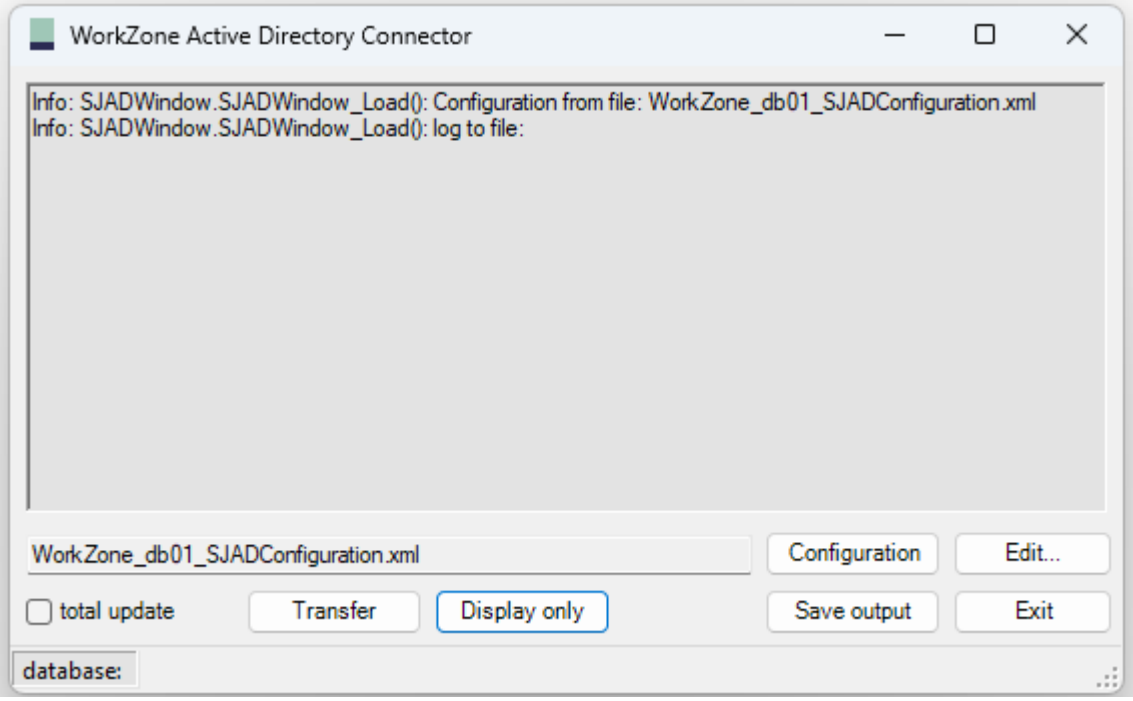


7. Click **Create**.
8. In the **Creating groups in AD** dialog box, click **OK**. The groups are created in the `ScanJourCaptiaAdministration` entry in the AD. You can rename the entry.
9. Click **Next**.
10. On the **Setup** tab, in the **Run in interactive mode** section, click **Run now** to create the configuration file.

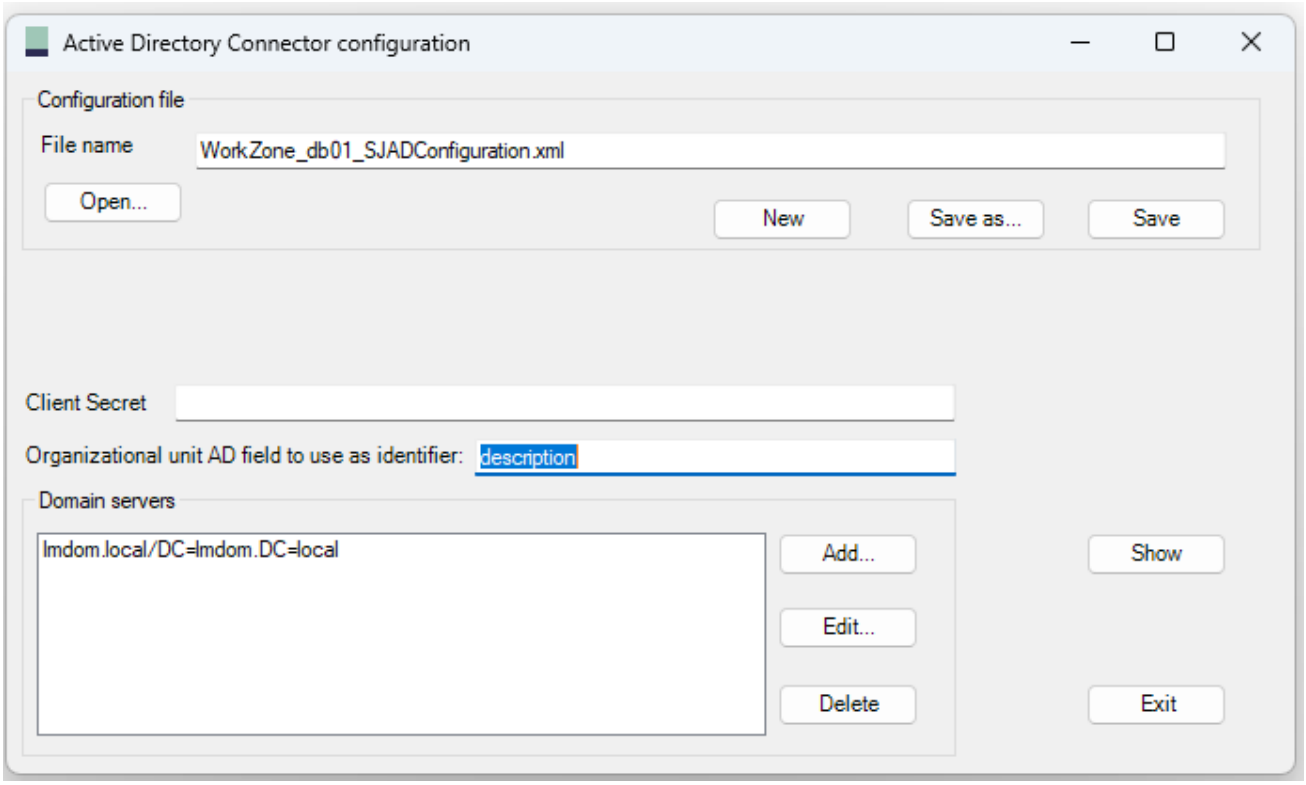


The file is called `SJADConfiguration<database name>.xml` and can be found in the KMD program folder. It is used in the alignment of transferred data from AD to WorkZone.

The `SJADConfiguration<database name>.xml` file is shown.



11. Click **Edit**. The **Active Directory Connector configuration** window appears.



12. In the **Client Secret** field, paste your client secret. It is important that the client secret is unencrypted because the AD Reader will not be able to process the secret if it is encrypted. The secret will be encrypted once you click **Save** in the

next step.

13. In the **Configuration file** section, click **Save**. The configuration file is now saved with an encrypted client secret and your entries in the KMD program folder.
14. Click **Exit**.
15. In the **Run in interactive mode** section of the **WorkZone Active Directory Connector** wizard, click **Create shortcut**.

    A desktop shortcut icon linking to the Active Directory Connector for easy access is placed on your desktop with the title `wzad<database name>`, for example, `wzadfortest`. When you click the shortcut, the Active Directory Connector will open on the screen that is shown in the second screen shot in step 10.

Connect Entra to a local AD

Update configuration file

The AdReader configuration file must be completed with the following items. Note that Client Secret or Certificate can be provided to authenticate.

```
<configuration>
...
<azureTenantId>tenant where application is located, same as set in WorkZone OData endpoint configuration]</azureTenantId>
<azureClientId>[Application Client ID]</azureClientId>
<azureClientSecret>[Client Secret(plain text or encoded)]</azureClientCertificatePath>
<azureClientCertificatePath>[Instead of Client Secret certificate can be provided]</azureClientCertificatePath>
<oDataUrl>[Url to WorkZone ODatav3 service]</oDataUrl>
</configuration>
```

Additionally, dedicated WorkZone users must be updated in the WorkZone database.

update users set:

```
update users set oid='<Enterprise Application Object ID>' where
user_name = 'SJADREPLICATORUSER';
```

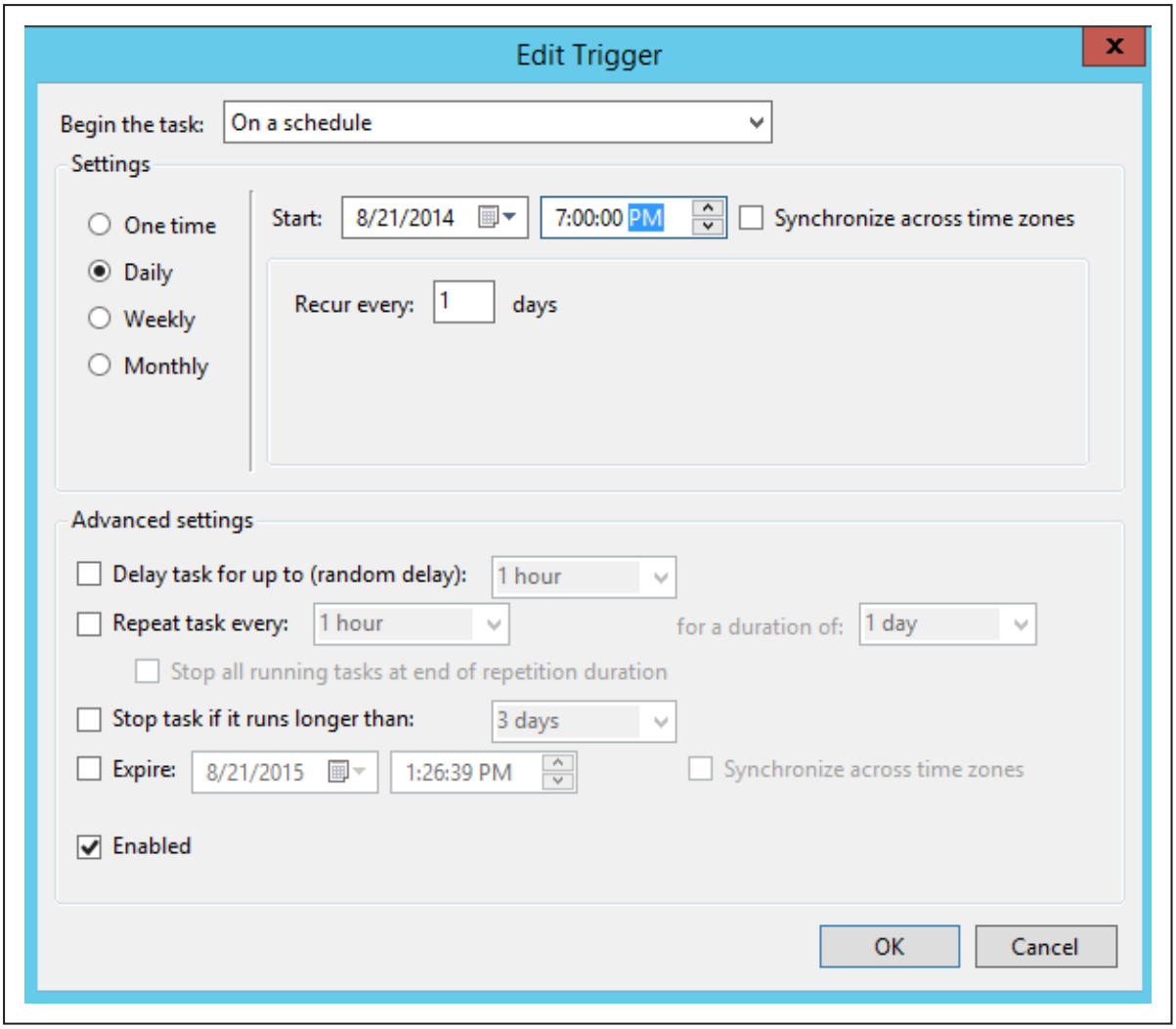
```
commit;
```

Note: The column **Ntauthentication** in the **users** table must be set to 'J' for 'SJADREPLICATORUSER'.

Create a scheduled task transfer

1. Start WorkZone Active Directory Connector.
2. In the **SJActive Directory Connector** window, click **Run Wizard**.
3. In the wizard, click the **Setup** tab.
4. In the **Setup scheduled task for transfer** section, click **Create job**. The task is now available via Windows Task Scheduler.
5. In Windows Task Scheduler, click **Task Scheduler Library** to view the task. The task is named `wzADreplication_<database name>`.
6. To set the task up to run at a specific time, right-click on the task and select **Properties**. On the **Triggers** tab, click **Edit** to open the **Edit Trigger** window and

set up when the task should be performed and at which interval.

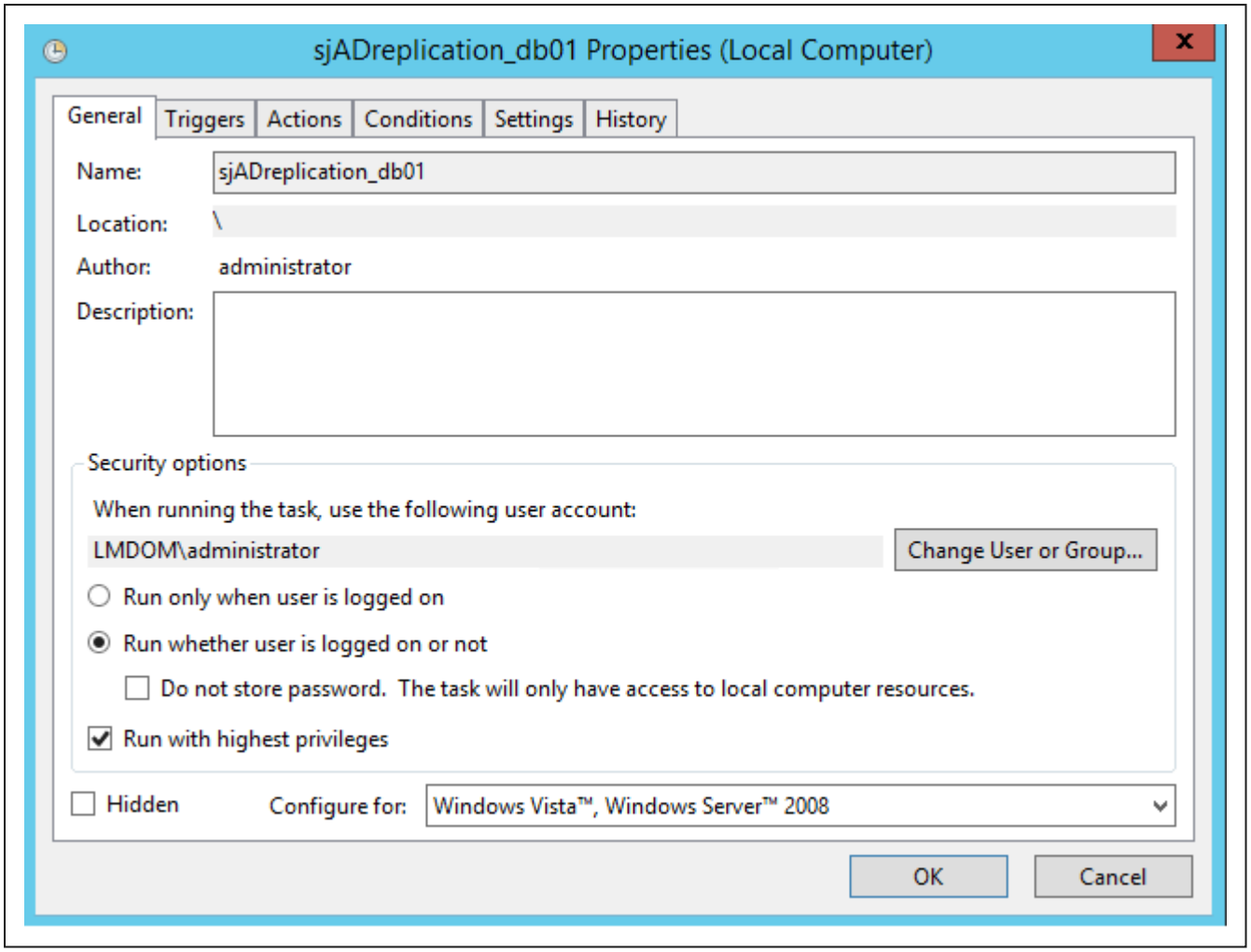


Note: It is recommended that you disable the task until you have finished your AD configuration. To do this, clear the **Enabled** check box in the **Edit Trigger** dialog box.

Log on options

When the Active Directory Connector wizard is used to create a scheduled task for the replication, the job is created with the **Run only when user is logged on** option.

If you want to change this to **Run whether user is logged on or not**, you must also select the **Run with highest privileges** option.



Command line parameters

Command line parameters are used while running the scheduled task, see Create a scheduled task transfer and its default setting from the initial setup may be changed.

To change the setup, open the **Scheduled Task** window and select the **Task** tab. In the **Run** field, you can see the default command line parameters.

In the table below is an overview of command line parameters, their default values and comments:

Parameter	Default value	Comment
`/db=<database name>`	No default value.	Defines the WorkZone database. This field cannot be empty, but the value is not used for connection.

Parameter	Default value	Comment
`/window /nowindow or /wizard`	If the database is specified, `/window` is the default. If the database is not specified, `/wizard` is the default.	Defines whether the program should show GUI and whether it should be the transfer status window (`\window`) or the wizard (`\wizard`).
`/forceupdate`	No default value.	Configuration file changes since last transfer will be checked. Displays all data (user, user information, and so on) that needs to be updated. If it is not specified, the modified date in Active Directory is compared with the last transfer.
`/config=<file name>`	`SJADConfiguration<database name>.xml`	Defines the location of the configuration file.
`/setsid=<SystemUser>`	No default value.	This user must be present in Active Directory, but should not be included as a member of any of the administrative groups or access code groups. As a result, the system user is looked up in the domain where the SID is read and is written into the database, so that the user can log on to WorkZone. Normal replication is not performed - only this single user is handled.
`/useGroupAsOU`	No default value.	When used, the wizard uses the template `SJADConfiguration-`

Parameter	Default value	Comment
		`templateOU.xml` instead of the template `SJADConfiguration-template.xml`, and this way forces use of AD groups to represent OUs instead of AD organizational units.
`/readcheck`	No default value.	If this parameter is applied, a check is carried out and only if no errors are found, the replication is performed.
`/logfile`	`sjad_replication.log`	The log file will be located in the folder where Active Directory Connector is run from. You can use the option `/logfile` when the option `/nowindow` is used. The information that is displayed on the screen when clicking **Transfer**, is logged to a file, either to the default file or to a specific file, for example `/logfile=c:\ADlogs\ADrep.log`.
/Showrenaming	No default value.	If this parameter is applied, the following check boxes will be displayed in the **Active Directory Connector configuration** form: • Allow renaming of users • Allow renaming of org. units • Allow renaming of groups

Parameter	Default value	Comment
		• Allow renaming of committees • Allow new instances users The settings determine if users, organizational units, group and committees can e renamed in the Active Directory.

Best practices and recommendations

Below you will find recommendations, best practices, and general advice concerning WorkZone Active Directory Connector and pre- transfer issues.

Monitor first transfer in the Event Log

It is recommended that you monitor your first transfer of user data from Active Directory to WorkZone with WorkZone Active Directory Connector The trial transfer is described in Transfer data.

All errors are reported in the Windows event log. You should monitor the event log carefully through the initial transfer. Fix the errors that occur while monitoring the event log. You can check the event log in Event Viewer.

- To open Event Viewer, click **Start** > **Control panel** > **Administration tools** > **Event Viewer**.

You must run a total update enabled transfer. To do this, in the **WorkZone Active Directory Connector** form, select the **total update** check box before you start a transfer.

One Configuration File per Database

- You must have only one configuration file per database. Make sure that your scheduled tasks use the correct configuration file.
- If you transfer manually, always disable the scheduled task.
- Perform only one transfer per database at any time.

- If you are doing major maintenance in AD, stop your scheduled task while you are manually monitoring you transfer.
- Enable the scheduled task when the procedure is completed, see Re- enable the scheduled transfer task.

Do not Change the name codes

If you need to change user names, unit names, or pre- Windows 2000 group names, do not make these changes in Active Directory without analyzing and mapping the consequences. If you do, the transfer will report the changes as errors.

If you need to change, for example, the initials of a user, it is recommended that you delete this user and create a new one. After this, you will have to change the deactivated user to an active user on cases, objects protected with a user access code, personal and general drafts that has not been archived yet, ownerships of reminders, personal preferences in the user interface, and so on. You have to transfer, or mass edit, or move the ownership to the new user.

You should also configure the new user as the old user, see Apply security groups to users.

Domain Server Connection

For each domain server you must enter the name of the server (or its IP address). If the program is not running as a trusted user of the domain, you have to specify the user name and password of a user that has permissions to read in AD's file catalog. The domain name may also be entered as a LDAP distinguished name as: `DC=scanjour,DC=dk`.

The WorkZone Active Directory Connector supports specification of logon information to be used for reading from the domain. This information is stored in the XML configuration file in the form of a user name and a password in encrypted form.

As in earlier versions, it is still possible to avoid specifying any logon information in the WorkZone Active Directory Connector itself. Instead, it can be run under an account with the needed permissions to read from the domain.

The password is encrypted in such a way that it can only be decrypted on the same machine as the one that was used during encryption. Encryption happens when you click **OK** in the **Domain Server** dialog box where the logon information has been specified.

This means that if you move the XML configuration file to another server because you want to use it with WorkZone Active Directory Connector, you need to re- enter the pass-

word of the logon information in the **Domain Server** dialog box after having moved the XML configuration file to the new server.

Users

The **Groups identifying ScanJour WorkZone users** list in the **Domain server** window in **WorkZone Active Directory Connector** lists the global distribution groups that identify users to be transferred.

If a user is a member of more than one group, he/she is automatically assigned the highest security code.

OUs and Units

The **Units** list in the **Domain server** window in Active Directory Connector displays the Organizational units that identify the Organizational unit to transfer into units in WorkZone.

If the **Recursive** check box is selected for an Organizational unit, all underlying Organizational units will be transferred as well, see Register Organizational units in WorkZone Active Directory Connector, step 5.

The Scheduled Task Transfer

When your transfer runs without any errors (and the event log also has no errors) you must configure a scheduled transfer task at a regular interval between 2 hours and once a day, depending on the size of your organization.

You can set up a scheduled task from the wizard, see Create a scheduled task transfer

If you change your scheduled task or make changes to the configuration file, make sure that the configuration is reflected in the command line parameters, see Monitor the transfer.

Mapping the AD Fields to WorkZone Fields

The configuration file contains the information regarding which AD field is transferred to which WorkZone database field. This information can be maintained directly in the XML configuration file.

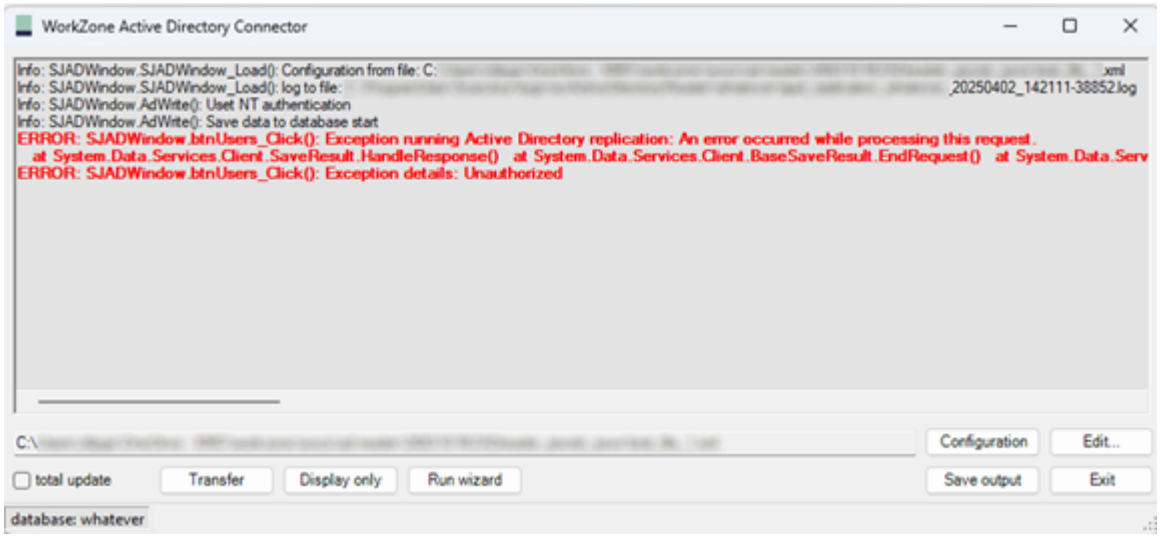
> **Note:** You must make changes manually in the XML- file using a text editor.

The XML file contains a number of `<userField>`, `<UnitField>`, and `<CommitteeField>` with specifications of what is transferred from where to where.

Changes can be made but consult your software provider and your KMD technician, see Field to field transfer between Active Directory and WorkZone and ADSI field names.

Troubleshooting

The WorkZone Active Directory Connector window prints all log on its screen. All issues are printed in red color (see the screenshot below for an example). Some error messages contain detailed information. To make the error message more readable, you can copy the error message and paste it in your preferred text editor.



Common configuration errors

Below you can see a list of common errors that may occur during configuration, and how you can solve them.

AADSTS7000215: Invalid client secret provided. Ensure the secret being sent in the request is the client secret value, not the client secret ID, for a secret added to app '<ClientID>'

If you get this message, check that the specified client secret is correct and that it has not expired.

AADSTS7000229: The client application <ClientID> is missing service principal in the tenant <TenantId>. See instructions here: https://go.microsoft.com/fwlink/?linkid=2225119

Make sure that the ClientID and Client Secret that you have specified are registered in the tenant with the specified ID <TenantId>.

Exception running Active Directory replication: Unauthorized

This error occurs because OData can't authorize the access token from from Entra. The reason may be that the tenant that provided the token is not known by WorkZone OData.

To fix this issue, make sure that the app is registered in the correct tenant. It should be the same tenant that runs WorkZone OData authorization.

Exception running Active Directory replication: Forbidden

This error occurs because the Service Principal (Enterprise Application) Object ID is not set in the SJADREPLICATORUSER oid column.

To fix this issue, run the following command on the WorkZone database:

```
update users set oid='<Enterprise Application Object Id>' where
user_name = 'SJADREPLICATORUSER';
```

```
commit;
```

Terms and conditions

Intellectual property rights

This document is the property of KMD. The data contained herein, in whole or in part, may not be duplicated, used or disclosed outside the recipient for any purpose other than to conduct business and technical evaluation provided that this is approved by KMD according to the agreement between KMD and the recipient. This restriction does not limit the recipient's right to use information contained in the data if it is obtained from another source without restriction set out in the agreement between KMD and the recipient or by law.

Disclaimer

This document is intended for informational purposes only. Any information herein is believed to be reliable. However, KMD assumes no responsibility for the accuracy of the information. KMD reserves the right to change the document and the products described without notice. KMD and the authors disclaim any and all liabilities.