Installation Guide

2022.0

Contents

Installation Guide for WorkZone 2022.0

Related product documentation

- WorkZone Release Notes
- WorkZone Support Matrix
- WorkZone Configurator Administrator Guide
- WorkZone Client Administrator Guide
- WorkZone Mobile Administrator Guide
- WorkZone PDF Administrator Guide
- WorkZone Process Administrator Guide

WorkZone links

- WorkZone documentation
- WorkZone support
- WorkZone website

What's new

WorkZone 2022.0

WorkZone Process

The NgDP integration has been adapted to reflect the latest changes to NgDP released by the Agency for Digitisation. The WorkZone NgDP integration can be used in production when the Agency for Digitisation releases NgDP November 2021.

Stand-alone e-Boks Push Service for NgDP

You can now install the WorkZonee-Boks as a stand-alone service on a Windows server.

See Install a stand-alone e-Boks Push Service.

WorkZone 2021.3

Added guidelines for registering the WorkZone application at Azure and using it for WorkZone services authorization (in WorkZone Cloud Edition installations). See Register WorkZone in Azure .

WorkZone for Office

It is recommended, that you add the Required 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).

WorkZone I/O Manager

Added guidelines on how to set up and configure WorkZone I/O Manager with WorkZone (a typical integration example with the most common tasks). See Install WorkZone I/O Manager.

WorkZone Process

WorkZone e-Boks Push Service supports NgDP

WorkZonee-Boks Push Service now supports Next generation Digital Post (NgDP). See Install and configure WorkZone e-Boks Push Service.

WorkZone 365

Added guidelines on how to install and deploy the WorkZone Teams app to collaborate on WorkZone content directly from your channels and private chats in Microsoft Teams. See Install WorkZone Teams.

WorkZone 2021.2

As of this release the HTTP protocol is no longer supported.

WorkZone Content Server changes

Re-indexing required when upgrading

If you upgrade your WorkZone Content Server 2021.0 or WorkZone Content Server 2021.1 installation to WorkZone Content Server2022.0, the meta data for the **File**, **Record**, **Contact**, and **Address** tables must reindexed. Reindexing the meta data for the **Document** table is not necessary.

WorkZone Client and WorkZone Configurator

Default Content Security Policies

Default Content Security Policies have been configured and enabled upon installation for WorkZone Client and WorkZone Configurator to enhance effective security controls available to the web browser and help prevent client-side attacks, such as Cross-Site Scripting.

If connectivity issues or issues with the execution of scripts or other code snippets in browsers accessing WorkZone Client or WorkZone Configurator are experienced, these issues might be attributed the default Content Security Policy values.

The default Content Security Policies can be checked and configured on the Microsoft IIS 7 server in the IIS Manager form to see if the policy performs as expected and adjust the policy values if necessary.

The Content Security Policy settings can also be checked by using the developer tools in the relevant browser or by using 3rd party development tools – for example Postman (a platform for API development).

A Content Security Policy cannot stand alone and should be considered a defense-in-depth measure for injection attacks, as it is dependent on browser support.

Cross Origin Resource Sharing (CORS) updated

Cross-Origin Resource Sharing (CORS) used in WorkZone services, such as WorkZone PDF Engine, WorkZone Process and WorkZone OData has been updated.

If WorkZone services are to be requested from browsers or web clients from other domains (for example WorkZone Client and WorkZone Configurator applications hosted on a different host than Process service), system administrators must configure the Cross-Origin Resource Sharing parameters **AllowedCorsOrigins** and **AllowedCorsHeaders** for WorkZone PDF Engine, WorkZone Process and the optional silent installation parameter **CORSORIGINS** for WorkZone OData.

Cross Origin Resource sharing can be configured manually in the WorkZone config files after product installation.

WorkZone Process

Microsoft Graph integration - sending smartmails and email notifications

In previous releases, sending smartmails and email notifications in WorkZone Process was implemented using the EWS (ExchangeWebServices) library. EWS supported both the on-premises and the cloud version of Exchange server.

To strengthen the security of WorkZone and ensure continuous updates of the library, the Microsoft Graph library is now used instead of the EWS library to send smartmails and email notifications in cloud environments.

For on-premises installations, EWS is still used. It is also possible to use EWS in a cloud installation but only with basic authentication. To be future-proof, it is recommended to use the Microsoft Graph library.

See Configure WorkZone Process and Command line configuration.

> **Note:** In this release, only sending emails using Microsoft Graph is supported. Receiving emails is not yet supported. This means that, for example, the Mailbox Monitor service workflow still uses the EWS library, and that this service is not yet supported in WorkZone Cloud Edition.

WorkZone 365 changes

Updated guidelines on how to Install WorkZone 365 to use meetings in Microsoft Outlook 2016 and 2019.

WorkZone I/O Manager

A new module, WorkZone I/O Manager, is now available in WorkZone. See Install WorkZone I/O Manager.

WorkZone 2021.1

WorkZone 365 changes

The paths to WorkZone 365 manifests have been updated. See Install WorkZone 365.

WorkZone Mobile changes

New **Custom filters** and **Delegated tasks** modules can now be enabled and disabled in WorkZone Configurator (under **Global** > **Feature settings** > WorkZone Mobile > **Task**). Ensure that you have enabled all modules your users will need to use. See Feature settings in the Administrator Guide for WorkZone Configurator.

WorkZone Process changes

A new **advanced submission** process has been added to the Extended process package. See About process packages.

A new **STEPSUBMISSION** access code has been introduced. It provides access to the new **Advanced submission (Extended)** process. See Access codes.

WorkZone 2021.0

WorkZone Process changes

New DBOnly configuration option

A new **DBOnly** role has been added to the WorkZone Process Configuration Wizard and to command line configuration. Select the **DBOnly** role, if you only want to configure the database for WorkZone Process.

See Configure WorkZone Process and Command line configuration.

New PackageLoadTimeout parameter

A new optional **PackageLoadTimeout** parameter has been added to the command line configuration. The **PackageLoadTimeout** parameter controls the timeout for loading a process package. See Command line configuration.

WorkZone 365 changes

OAuth2 authentication is required for enabling merge functionality for the users.

WorkZone Mobile changes

New **Browse** module (an experimental feature) can now be enabled and disabled in WorkZone Configurator (under **Global** > **Feature settings** > WorkZone Mobile). Ensure that you have enabled all modules your users will need to use. See Feature settings in the Administrator Guide for WorkZone Configurator.

WorkZone 2020.3

WorkZone is now supported on macOS devices and works in Google Chrome and Safari browsers for macOS. See Overview of supported 3rd party products.

Support for OAuth2 authentication framework

Define OAuth2 settings during installation of WorkZone Content Server

The OAuth2 Authentication framework can be selected as the authentication method for WorkZone users instead of the standard Windows authentication during installation. The framework can be used to authenticate WorkZone users in a cloud-based WorkZone installation.

If OAuth2 authentication is selected, you must define correct OAuth2 parameters to the Azure Active Directory: Tenant ID, Client ID and Client Secret.

The OAuth2 Authentication framework is automatically installed and enabled during installation of WorkZone Content Server, but must be configured correctly in order to be utilized. See Install WorkZone Content Server

> **Note:** Performing case and document searches directly from File Explorer is not supported in a cloud setup as OAuth2 authentication is not supported by Windows Federated Search. See Supported Authentication Protocols (External link)

WorkZoneActive Directory replication changes

Active Directory replication in an OAuth2/Azure environment requires specific manual set up and configuration in order to enable the continuous replication of the Active Directory structure from an on-site domain controller to the WorkZone Content Server installed in an Azure environment. See Active Directory replication in an OAuth2 setting

WorkZone Process OAuth2 changes

- New OAuth steps in the **KMD WorkZone Process Configuration Wizard**. See Configure WorkZone Process.
- New **OAuthClientSecret** parameter and required specification of Exchange configuration parameters in command line configuration. See Command line configuration.
- Updated WorkZone Process post-installation checklist.
- New OAuth specific parameters in the Package Loader used for installing and activating customized process packages. See Install and activate customized process packages.

WorkZone PDF OAuth2 changes

- The `CrawlerClientId` and `CrawlerClientSecret` parameters must be defined when installing WorkZone 2020.3.
- Crawler user settings removed from the database configuration. See Perform database configuration and Deploy reports.
- By default, the Crawler user is defined as *system*. In this case, the WorkZone PDF Crawler service will be executed as a Local System. See Microsoft documentation.
- If you want to upgrade from version 2020.2 or earlier, you must uninstall the old version before installing the new one.

WorkZone for Office OAuth2 changes

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

WorkZone Process changes

- The behavior of the **SetupDatabase** parameter has changed. It set to True by default. See SetupDatabase.

WorkZone 2020.2

Define OAuth2 settings during installation of WorkZone Content Server (2020.1 Hotfix 1)

The OAuth2 Authentication framework can be selected as the authentication method for WorkZone users instead of the standard Windows authentication during installation. The OAuth2 authentication framework can be used to authenticate WorkZone users in a cloud-based WorkZone installation.

If OAuth2 authentication is selected, you must define correct OAuth2 parameters to the Azure Active Directory: Tenant ID, Client ID and Client Secret.

The OAuth2 Authentication framework is automatically installed and enabled during installation of WorkZone Content Server, but must be configured correctly in order to be utilized.

Note: Performing case and document searches directly from File Explorer is not supported in a cloud setup as OAuth2 authentication is not supported by Windows Federated Search. See Supported Authentication Protocols (External link)

WorkZone Mass Dispatch

WorkZone Mass Dispatch is now released for production. The changes to the installation procedure are:

- The DP2 service is required.

  See Install WorkZone Mass Dispatch.

WorkZone Mobile

WorkZone Mobile **Chat**, **Meeting** and **Notes** modules now can be enabled and disabled under **Global** > **Feature settings** in WorkZone Configurator. Ensure that you have enabled all modules your users will need to use. See Feature settings in the Administrator Guide for WorkZone Configurator.

WorkZone for Office

- TLS 1.2 is now supported.
- WorkZone Meeting functionality has been deprecated from WorkZone for Office, so you can no longer install the WorkZone Meeting client and server. We have released this functionality as part of our new WorkZone Office add-in.

WorkZone PDF

- The procedure for updating reports in the same release has been simplified. The **Version** parameter now includes hotfixes such as builds. See Create the Report JSON file.
- Report progress information is now shown in WorkZone Client. See My reports today list.
- The **ActionsOnDocumentBeforeConversion** parameter now supports flattening of forms and annotations in PDF documents. See Perform database configuration.

WorkZone 2020.1

WorkZone Content Server

Be advised that the network TCP port 1200 (configurable) is now required to be open for incoming traffic on the Web server in order to receive chat notifications from the Oracle database to the new Notifications web application. If the Windows firewall is enabled on the Web server, it will be opened automatically when installing WorkZone Content Server using Olympus.

If the port is not open, the chat feature will not receive notifications regarding changes to chats. If another firewall is configured between Oracle and the Web server, the TCP port 1200 (configurable) must be opened there as well.

If another TCP port number is preferred, the port used can be changed in the “appsettings.json” file (section OracleAQNotificationPort) located in “C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\Notifications\bin” on all Web servers.

WorkZone Process

- The performance of WorkZone Process Configurator has been improved. Process packages are now only loaded once into the database, which makes configuration faster when you want to configure WorkZone Process on multiple web servers. If you need to reload the process packages, you can use a new command line parameter named **ForcePackageLoad**.

  See Command line configuration.

- Access code changes regarding re-ordering user tasks

  Previously, the CONFIGADM access code also granted a user rights to re-order user tasks for other users. Now, only delegates can re-order tasks for other users. Task owners can always re-order their own tasks. See Access codes.

- Access code changes regarding creating delegates for other users

  Previously, you could create delegates for other users if you had the CONFIGADM access code. Now, you can add delegates for the other users only if you already are a delegate for that user and have the ADMIN role. See Access codes.

- The SmartPoste-Boks dispatcher now supports Digital Post 2. To use SmartPost with e-Boks using Digital Post 2, you need to install WorkZonee-Boks Push Service.

  See Install and configure WorkZone e-Boks Push Service.

WorkZone for Office

- You can use four new registry keys to fine-tune a standard behavior of WorkZone for Office according to your needs.

See Registry keys.

WorkZone 365

- WorkZone 365 for Microsoft Word, Excel, and PowerPoint has been released. This is the experimental version with limited functionality where you can only edit existing documents. Each application (Word, Excel, and PowerPoint) requires own manifest.

Moreover, installation and uninstallation processes differ for Office 365.

Word, Excel, and PowerPoint are released not for the production usage. Please install and use them only for testing purposes and sharing your feedback with us. We expect the production version in the 2020.2 release.

See Install WorkZone for Office and Uninstall WorkZone for Office.

WorkZone Mass Dispatch

- Two new access codes **MASSDISPATCH** and **MASSDISPATCHSEND** related to WorkZone Mass Dispatch have been introduced in this release.

  See Access codes.

- You need to install WorkZone Mass Dispatch as a Windows service manually.

  This is not the version to be used in production. Please install and use it only for testing purposes and sharing your feedback with us. We expect the production version in the 2020.2 release.

  See Install WorkZone Mass Dispatch.

WorkZone 2020.0

WorkZone Meeting

- To install WorkZone Meeting Server, you no longer need to specify information on database: database name and user credentials. This information will automatically be updated by WorkZone Content Server.

Active Directory

- When performing Active Directory replication, post codes will not be replicated to user profiles where the country code has not been defined (the country_code field is empty).

WorkZone Explorer

- WorkZone Explorer can now be activated and deactivated from WorkZone Configurator > **Global** > **Feature settings** > **Client** > **Explorer**.
    - If WorkZone Explorer is activated, the **Explore** button in the main ribbon in WorkZone Client will be displayed and the WorkZone Explorer feature will be accessible.
    - If WorkZone Explorer is deactivated, the **Explore** button in the main ribbon in WorkZone Client will not be displayed and the WorkZone Explorer feature will be inaccessible.

WorkZoneCVR Integration

The **Co.** field for companies is now included in WorkZoneCVR Integration.

USELOGADM and USERADM access code changes

The USERADM access code is now required to access, search and view the Use Log module and the USELOGADM access code is required to start and stop the Use Log. This change affects all methods of accessing the Use Log (either through WorkZone Configurator or the ODATA interface.

WorkZone 2019.3

- The Monitoring section has been moved to the new WorkZone Operations Guide.
- WorkZone PDF pre-installation checklist has been added to the guide.
- WorkZone PDF and WorkZone for Office post-installation checklists have been added to the guide.

WorkZone PDF

- WorkZone PDF no longer performs the following database configuration:
    - database structure change
    - maintenance of WorkZone registers

  These settings were moved to WorkZone Content Server.

- The `ClearConfidentialInformation` has been renamed `Actions-sOnDocumentBeforeConversion`.
- The ActionsOnDocumentBeforeConversion parameter can be now fine-tuned for each document type and each review information type. Please revise its settings according to your business needs.
- By default, WorkZone PDF Crawler is now disabled after the installation. You can enable it in WorkZone Configurator.
- Setting of the WorkZone PDF Engine and WorkZone PDF Crawler parameters is no longer available during the database configuration. Please set the parameters in WorkZone Configurator, in the WZPDF_CONFIGURATION table, or in the Web.-config file afterward.

WorkZone Process

Doc2Mail is renamed to OneTooX

The name change is implemented in both the user interface and the documentation.

WorkZone Configurator

- The installer now provides **Repair** option to fix a damaged installation.
- WorkZone Configurator now does not require individual installations on multiple databases: once installed on the web server, it will work on all databases installed on the same web server.

WorkZone for Office

- During the WorkZone for Office installation, server's and client's versions are now checked for their compatibility.
- WorkZone for Office now represents items in lists based on their rank.

WorkZone Meeting

New prerequisite has been added:

- You cannot use both WorkZone Meeting and WorkZone 365. Only one application must be installed to assure the correct work of WorkZone.

Active Directory

The STJERNEADM and MEDARBADM access codes enable a system administrator to grant Global or Departmental access rights to other users. Departmental access rights can only be granted if the organization uses WorkZone Corporate Edition.

USELOGADM and USERADM access code changes

The USERADM access code is required to see the Use Log menu in WorkZone Configuration Management. Both the USERADM and the USELOGADM access code are required for a user to access, search and view the Use Log module as well as start and stop the Use Log.

The USELOGADM access code also grants access to the Use Log through the ODATA interface.

WorkZone 2019.2

This is the first version of the WorkZone Installation Guide. Installation content from WorkZone product specific installation and administrator guides have been merged in to this guide.

News in this guide:

- Architectural overview of WorkZone.
- Overview of supported 3rd party product releases that WorkZone supports.
- Prerequisites cover all products.
- Overview of access codes and what they are used for.
- A Monitor section that describes tools and log files that can be used for monitoring WorkZone.

WorkZone Content Server

New WorkZone Content Server installer

All WorkZone Content Server features now installed automatically when you install WorkZone Content Server. You still have to manually set up database access during installation. The installed WorkZone Content Server features can be individually activated or deactivated in WorkZone Configurator or WorkZone Configuration Management.

When you install WorkZone Content Server, you must select which program features are to be installed:

- **Oracle client:** Installs the Oracle client in the path. The **Oracle ODBC driver** feature is installed by default.
- **Web server:** Installs all common web services, Microsoft Office services and collaboration services required by WorkZone.
- **Agent server:** Installs all agents required by WorkZone not included Web server program features.

If you uninstall WorkZone Content Server, all WorkZone Content Server features will also be uninstalled automatically.

Installation of facets

Case facets are now automatically installed during installation of WorkZone Content Server. Additionally, when upgrading your database, facets are automatically selected for upgrade.

CPR/CVR integration

The CPR/CVR integration is now automatically installed during installation of WorkZone Content Server.

WorkZone Client

New WorkZone Client installer

All WorkZone Client features are now installed automatically when you install WorkZone Client. You still have to manually set up database access during installation. The installed WorkZone Client features can be individually activated or deactivated in WorkZone Configurator.

If you uninstall WorkZone Client, all WorkZone Client features will also be uninstalled automatically.

WorkZone for Office

- WorkZone for Office Administrator guide has been fully moved to the Installation guide.
- You can require users to assign access codes when they create new cases, documents, and contacts. To do this, specify relevant access codes in the `AccessCodesAffectRequiredFields` element and assign them to the users.

WorkZone PDF

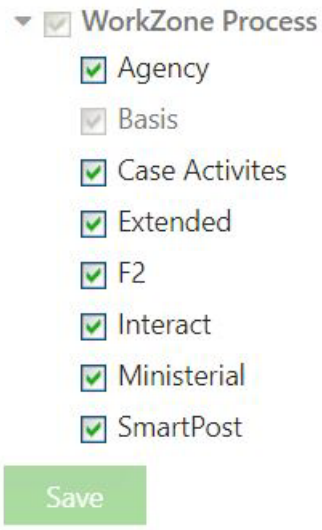
- WorkZone PDF Administrator's guide has been partially moved to the Installation guide. In particular, installation, updating, uninstallation, and configuration sections.
- Web application name is now used to get configuration from the database. Target name in Web.config is no longer used for this purpose. This improvement simplifies configuration process.

WorkZone Process

Selection of process packages is now done in WorkZone Configurator

Selection of which packages to use has been moved to WorkZone Configurator from the WorkZone Process Configurator wizard. The **Package selection** page has been removed

from the wizard. All standard process packages are installed but only the Basis process package is by default activated for use. You can activate other packages on the **Feature settings** page in WorkZone Configurator



See Activate process packages.

You can also display customized process packages.

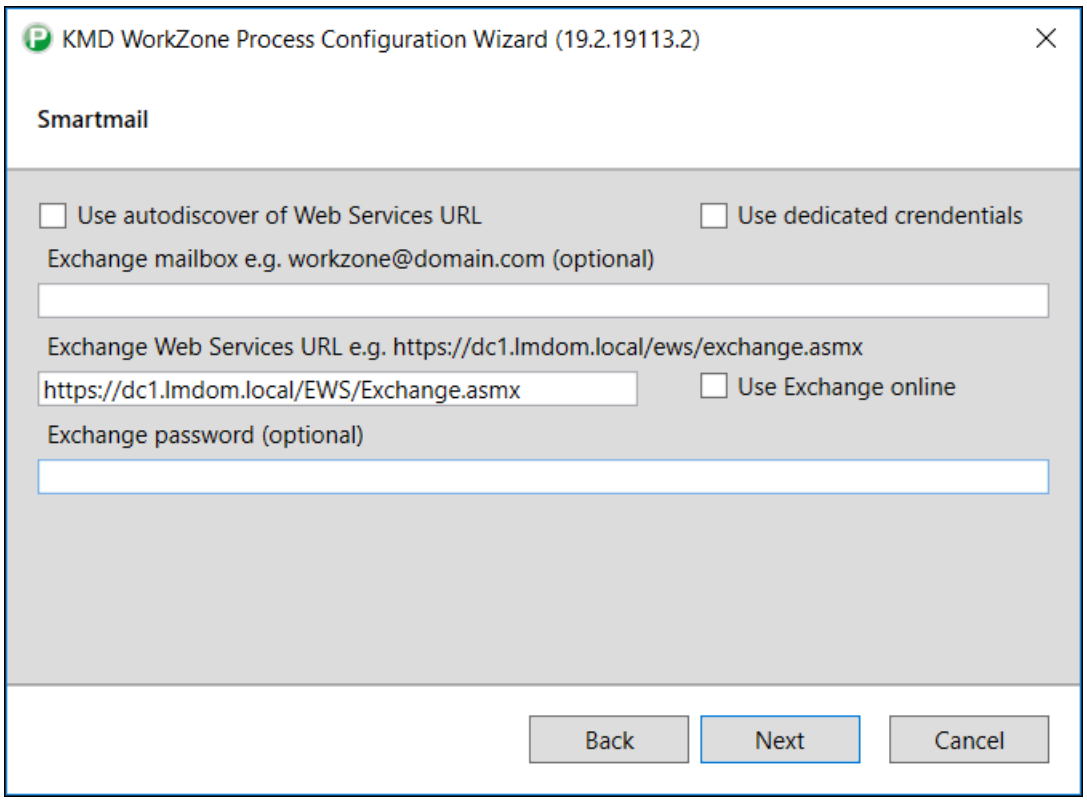
See Display customized process packages in WorkZone Configurator.

Alignment of Exchange configuration parameters

The configuration of Exchange On-Premises and Exchange Online has been aligned. It is possible to

- Use Autodiscover when using Exchange On-Premises
- Configure the URL manually when using Exchange Online.

The **Smartmail** page of the WorkZone Process Configurator wizard has been modified to reflect this alignment.



See revised instructions in step 5 in Configure WorkZone Process

If you use command line configuration, two new parameters have been added.

- AutoDiscover
- ExchangeServerVersion

See revised parameter descriptions and examples in Command line configuration.

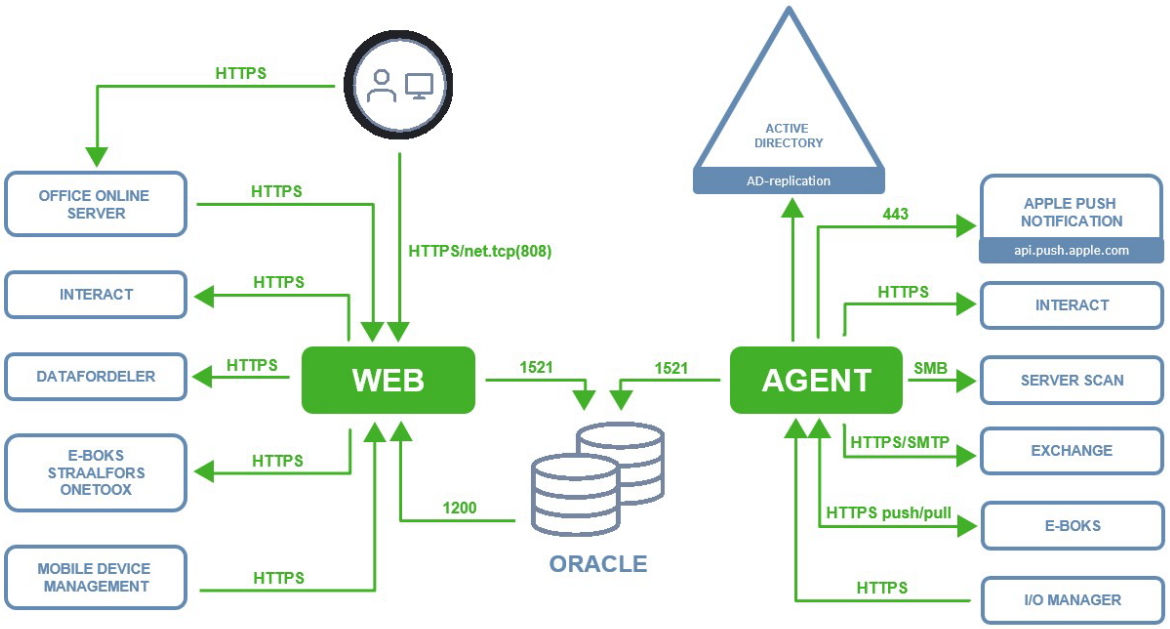
The WorkZone architecture

In this section you can get an overview of the WorkZone infrastructure, where the different WorkZone components are installed, and 3rd party releases supported by WorkZone.

Infrastructure

A typical WorkZone implementation consists of a database server, one or more web servers, an agent server, and a number of client machines.

The diagram below shows the WorkZone infrastructure by web and agent roles.



The Web server

The web server runs web services and other web elements used by WorkZone. Services restarted on the Web server will impact users and cause running applications to close, requiring restart in order to resume ordinary operations.

Multiple web servers can be deployed in your WorkZone infrastructure.

The Agent server

The agent server runs background services such as mail agents and messaging services. Services restarted on the Agent server will normally not impact users directly and will not normally cause applications to close. Instead, restarted services will be queued and started/restarted according to internal WorkZone procedures. Additionally, restart procedures with regards to interoperability and dependencies between services are managed by WorkZone.

Only one agent server can be deployed for each database in your WorkZone infrastructure.

Firewall directions and network ports

The arrows in the diagram illustrate the firewall direction and the ports indicated must be opened for traffic in order for WorkZone to operate correctly.

Special note regarding TCP port 1200

The network TCP port 1200 (configurable) is required to be open for incoming traffic on the Web server in order to receive chat notifications from the Oracle database to the new Notifications web application. If the Windows firewall is enabled on the Web server, it will be opened automatically when installing WorkZone Content Server using Olympus.

If the port is not open, the chat feature will not receive notifications regarding changes to chats. If another firewall is configured between Oracle and the Web server, the TCP port 1200 (configurable) must be opened there as well.

If another TCP port number is preferred, the port used can be changed in the “appsettings.json” file (section OracleAQNotificationPort) located in “C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\Notifications\bin” on all Web servers.

Where are WorkZone components installed?

In this section you can get an overview of where WorkZone components installed by WorkZone product.

WorkZone Content Server

Web server

All common web services, Microsoft Office services and collaboration services required by WorkZone.

Agent server

All agents and services required by WorkZone not included Web server program features.

WorkZone Process

Agent role

Component	Description
Mail agent	The mail agent is a Windows service responsible for sending out e-mails with smarttasks.
Push notification agent	The push notification agent is a Windows service responsible for sending notifications.

Web role

Component	Description
Process packages	Installs all process packages. See About process packages.
WorkZone Process Configurator	The WorkZone Process Configurator wizard allows you to configure WorkZone Process components.
Package loader	The Package loader is a utility that is used for deployment of customized Process packages. See Install and activate customized process packages.

Component	Description
Processes overview	The Processes overview is a web page that allows you to view the status of all processes and tasks, and perform actions.
Process module in WorkZone Configuration Management	The Process module in WorkZone Configuration Management. You do most configuration of WorkZone Process in WorkZone Configurator but a few configurations must be done WorkZone Configuration Management. For example, configuration of process logging and the Process monitor service workflow. See Monitoring WorkZone processes.

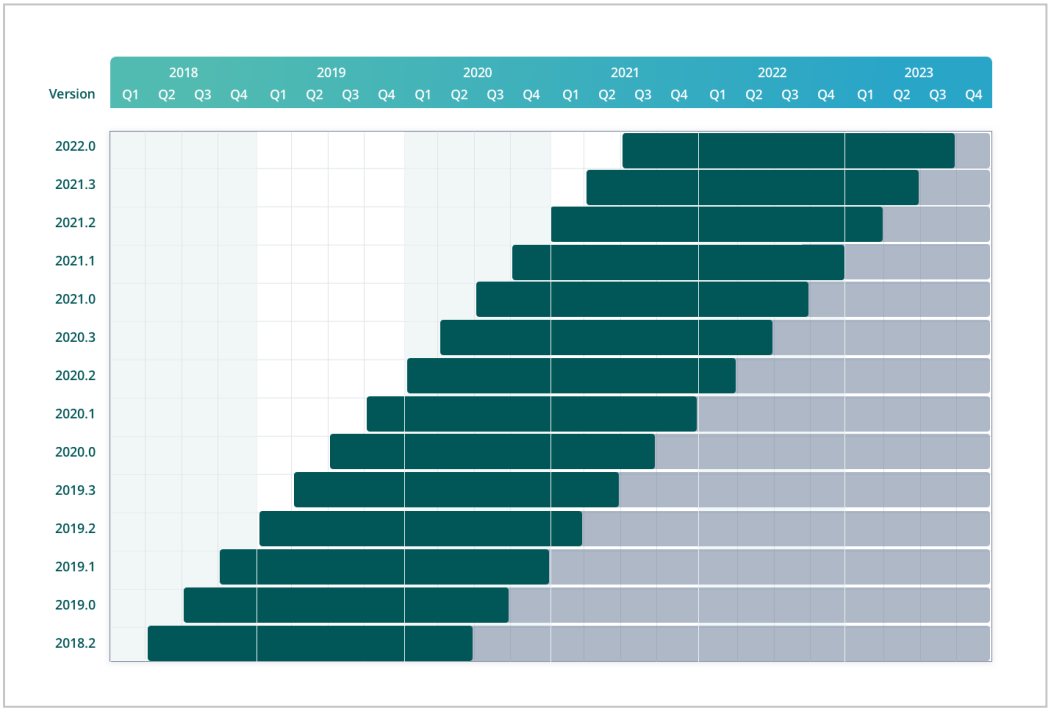
Note: If you are running two identical web servers, an agent server and a web server, the full WorkZone Process package must be installed on the agent server.

Supported versions and 3rd party products

This section contains overviews of the 3rd party product releases that specific WorkZone releases support.

Supported WorkZone versions

The diagram below provides an overview of the support status of current versions of WorkZone.



- Green: The version is supported.
- Grey: The version is no longer supported.

The WorkZone 2018.2 row in the diagram also includes the versions 2018.2 SP1 and 2018.2 SP2.

Older versions of WorkZone not displayed in the diagram (WorkZone 2018.1, WorkZone 2018.0, WorkZone 2017.0 (including 2017 SP1) and WorkZone 2016 R2 are no longer supported.

The support period

A released version of WorkZone will be fully supported during the two years following the release after which it will no longer be supported.

What does "Supported" mean?

Supported WorkZone versions are eligible for program updates (including security and privacy updates) that fix reported errors based on a subjective appraisal of the consequences of the errors.

Program updates are usually delivered in the form of hot fixes that can be downloaded and applied to the version in question.

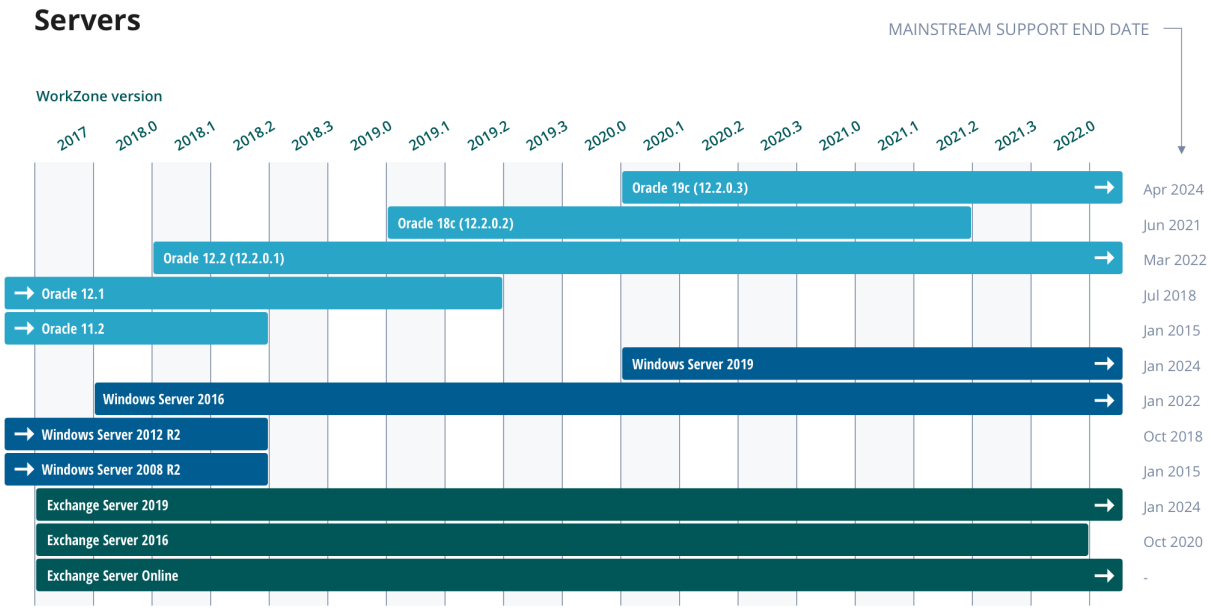
Unsupported versions

WorkZone versions that are no longer supported are not eligible for (and will not receive) program updates of any kind, including security and privacy updates. Unsupported versions still retain all program features and functionality and can still be used for daily operations. Embedded links to internal and external sites, for example the WorkZone documentation site may no longer function.

> **Important:** If your version of WorkZone is unsupported, it is recommended to upgrade to a supported WorkZone version to help ensure continued program stability, security and protection of privacy, as well as to receive new functionality and improvements to program functionality and performance.

Windows Server, Exchange Server, and Oracle

The diagram below provides an overview of which releases of Microsoft Windows Server, Exchange Server, and Oracle are supported by a specific WorkZone release. WorkZone supports the 3rd party products during their mainstream support period (that is, until the 3rd party product enters into the extended support period. Mainstream end support dates are shown to the right.



> **Important:** Provided information about the 3rd party main support end dates is subject to change. Refer to the Windows Server Product Lifecycle and Oracle Lifetime Support Policies for the most up-to-date information about Microsoft and Oracle products support.

See also:

- WorkZone Support matrix (on premises)
- WorkZone Support matrix (Cloud Edition)

Windows, macOS, and Office

The diagram below provides an overview of which Microsoft Windows, macOS, and Microsoft Office releases a specific WorkZone release supports. Mainstream end support date of these

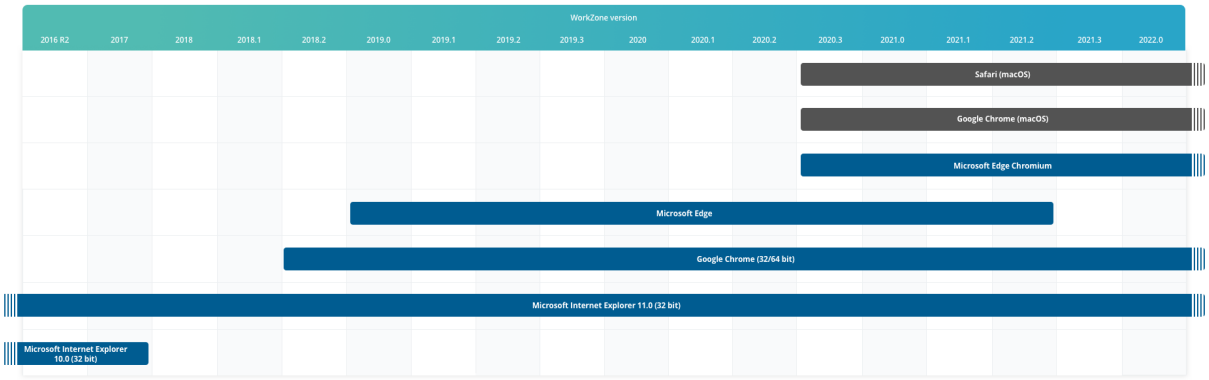
products is shown to the right.

See also:

- WorkZone Support matrix (on premises)
- WorkZone Support matrix (Cloud Edition)

Internet browsers

The diagram below provides an overview of which browsers a specific WorkZone release supports.



Note: Internet Explorer 10 has an end date January 2020. See Internet Explorer 10 Product Lifecycle.

See also:

- WorkZone Support matrix (on-premises)
- WorkZone Support matrix (Cloud Edition)

Product dependencies

The table below displays the mandatory and optional requirements for selected WorkZone 2022.0 products. Locate the column for your WorkZone product and see which other WorkZone products are required and which are optional.

x: Required products are WorkZone products that must be activated for other WorkZone products to run or function at all.

(x): Optional products are WorkZone products that are not an absolute requirement for the selected WorkZone product to run or function. Optional products may contain functionality or feature sets that can be considered important, but as long as the optional product itself is not required to actually run the selected WorkZone product, it is considered optional.

2022.0	Client	Configurator	365	for Office	Mobile[1]	PDF	Process
Client	-	(x)	(x)	(x)		(x)	x
Configurator	x	-		(x)		(x)	x
Content Server	x	x	x	x	x	(x)	x
Configuration Management	(x)			(x)			
for Office	(x)	(x)		-			(x)
PDF	(x)	(x)	(x)		x	-	x
Process	(x)	(x)		(x)	x		

x: Required: This is a prerequisite for the WorkZone product to run.

(x): Optional: Some, but not all features, will require this product.

WorkZone Client

This table provides an overview of dependencies between WorkZone functionality and other WorkZone applications and modules.

Functionality	Required products
• Sending a case in an email • Sending a document as a link or as	WorkZone for Office

Functionality	Required products
an attached file • Exporting a list to Excel (the WorkZone for Excel add-in required)	
• Working with WorkZone meetings • Configuration of a meeting search detail page	WorkZone 365
• Opening a case in Windows explorer	WorkZone Explorer
• Working with processes • Working with case activities • Working with delegates	WorkZone Process
• Creating PDF files to print case documents and case notes • Using reports	WorkZone PDF Engine
• Working with notes	The Notes module

WorkZone Process

It is highly recommended to activate WorkZone for Office to benefit from the full functionality of WorkZone Process.

WorkZone Content Mobility

- If you do not activate WorkZone PDF Crawler, documents will open in Quick Look.
- If the organization uses the Meeting module and runs on WorkZone Content Server 2017, you need to replace an OData dll file on all web servers in order to load all

meeting data correctly. Copy and replace the `Scanjour.Services.OData.dll` file to the folder `C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\OData\Bin`

Hardware recommendations

Server recommendations

KMD strongly recommends you obtain guidance from experienced hardware architects for professional advice and recommendations with regards to necessary hardware requirements. This is to ensure optimized everyday operations that respect the architectural hardware and software restrictions inherent to your organization.

The reasons for this recommendation are that organizations work differently, have specialized customizations, and have varied legal, procedural and historic requirements for daily and long-term operations, security, communication and interoperability as well as utilize different 3rd party applications.

Additionally, WorkZone has dependencies to, for example, Microsoft Active Directory, Microsoft Exchange, firewall setup, internet connectivity and stability, internet bandwidth and speed, storage size and accessibility as well as being dependent on Oracle for storing current and archived data. The server capacity and configuration also depends on how your organization uses WorkZone, meaning whether WorkZone is the primary application or is used as an archive.

As a rule of thumb, the hardware requirements should as a minimum fulfill the requirements of the software listed in the WorkZone Support matrix (operating system, database, Microsoft Office applications to mention a few).

Memory requirement

A minimum of 16 GB RAM is required on WorkZone servers but hardware architects should be consulted to analyze memory requirements based on your organization's usage patterns and user loads. For example, if you expect to do large report loads regularly, have intensive loads on service workflows, have large user loads, or run integrations, you should get your setup analyzed.

Client PC recommendations

WorkZone runs either as an add-in to Microsoft Office or in an Internet browser and therefore, KMD follows Office and browser requirements and recommendations with regards to PC configuration. It is expected that customers also take these recommendations into consideration.

System requirements

For Office 2016, 2019, and 365, see System requirements for Office.

In general, these Office requirements are the minimum configurations that WorkZone can run on.

Note that Microsoft does not take other 3rd party software such as anti-virus programs and other specialized systems (fagsystemer) into consideration. Therefore, it is recommended to consider both performance and requirements across Office and its 3rd party dependencies.

Cached Exchange Mode recommendations

It is strongly recommended that Cached Mode is enabled in Microsoft Outlook.

Microsoft recommendations:

See Plan and configure Cached Exchange Mode in Outlook 2016 for Windows

KMD WorkZone recommendations:

See Microsoft exchange server and cached exchange mode in the WorkZone Installation Guide.

Summary of KMD Client PC recommendations

KMD recommends customers analyze the applications they run on their PCs and set any appropriate requirements.

The minimum WorkZone system requirements are as defined by Microsoft:

- **Computer and processor**: 1.6 gigahertz (GHz) or faster, 2-core.
- **Office Professional Plus**: 2.0 GHz or greater recommended for Skype for Business.
- **Memory**: 4 GB RAM; 2 GB RAM (32-bit).
- **Hard disk**: 4.0 GB of available disk space.

Source: System requirements for Office

In addition, it is strongly recommended to run Outlook in Cached Mode because it gives a better user experience when running WorkZone in interaction with Outlook.

See also

WorkZone support matrix

Prerequisites

Before installing WorkZone, a list of requirements and prerequisites must be met. Use this section to check the full list of prerequisites starting from basic and finishing with product specific ones.

See also Support matrix.

Basic

HTTPS

Running with https is strongly recommended.

SMTP mail service

If you plan to use Agent SUB and WorkZone Content Server Imaging, you must install SMTP mail service on the agent server, where Agent SUB and WorkZone Content Server Imaging are running. You add the **SMTP Server** feature in Server Manager.

Default configuration

WorkZone has been tested on servers that use the default configuration that has been set by the supplier, for example, Microsoft or Oracle. Therefore support cannot be guaranteed if these settings are changed. Examples of changed settings can be changes to the system rights concerning objects, keys in the registration database, files, reconfiguration of the system, as well as removal of features and files.

Execution of VBS files

VBScripts are used for creating the WorkZone database. Therefore the server must be able to execute.VBS files when creating and upgrading the system.

Active Directory services tools - optional

You may need to check and verify the Active Directory (AD) in connection with error handling. To make this easier, you can install AD DS and AD LDS tools as features under remote server administration.

WorkZone Content Server database

- Installation of an empty Oracle database version with Intermediate Text. See supported Oracle versions in the Support matrix.

ODBC acess

- The database must be accessible through 32 bit ODBC.

Microsoft Active Directory

Installed/accessible

Windows requirements

Requirements for Windows

> Important: If you have installed the Microsoft update kb2918614, make sure that you also install the Microsoft update kb3008627. If you have installed update kb2918614 but not kb3008627, the WorkZone installation will fail.

.NET Framework 4.8 features are installed as part of the WorkZone installation.

Windows Server Roles and Features

The WorkZone installation requires that the following Windows roles and features are enabled.

Note: You can run the WZCS.ps1 script located in the **DSC** folder, which will enable the required roles and features. See the WZCS.ps1 script for comments.

Windows Server roles

Select Web server (IIS)

Expand **Web Server** and select the following roles

Web Server	Roles
Common HTTP Features	• Default Document • Directory Browsing • HTTP Errors • Static content
Performance	• Static Content Compression • Dynamic Content Compression
Security	• Basic Authentication • Windows Authentication
Application Development	.NET Extensibility ASP.NET ASP ISAPI Extensions ISAPI Filters. Version 4.0 (2008 R2) or 4.5 (2012).

Expand Management Tools and select the following roles

Management Tools	Roles
IIS Man-agement Con-	

Management Tools	Roles
sole	
IIS 6 Management Compatibility	IIS 6 Metabase Compatibility IIS 6 Management Console IIS 6 Scripting Tools IIS 6 WMI Compatibility.
IIS Application Initialization (only for IIS 8.0 or later)	It makes WorkZone application up and running right after installation. If the Application Initialization element is not installed, the WorkZone PDF Engine installation will fail. If the WorkZone PDF Engine installation procedure detects an ISS 7.0 or IIS 7.5 during installation, the Application Initialization element requirement will be waived and the installation will proceed as usually but the start up speed of a WorkZone PDF Engine application will not be improved.

Note: If WorkZone PDF cannot access IIS via `https://localhost` or `https://<server name>` but only through a common HLB/NLB name, you need to install WorkZone PDF on all servers that are distributed from HLB/NLB.

IIS URL rewrite

If you want to apply URL rewrite rules, you need to install IIS URL Rewrite 2.0 on the web server(s). This is required to ensure that URL paths are redirected to the new paths used since the 2014 release. See Add URL rewrite rule.

Note: When running https, you must bind the Default Web Site in Internet Information Services (IIS) Manager.

Microsoft Web Deploy 3.5

- You can install Microsoft Web Deploy program from the **Prerequisite software** folder in the WorkZone installation package, or you can download from here.

Windows Server features

- Enable the following.NET Framework 4.8 Advanced Services:
  - **WCF Services**
    - HTTP Activation
    - TCP Activation
    - TCP Port Sharing

  Office Services require that the WCF Services features are enabled.

ISAPI and CGI Restrictions:

- In **Service (IIS) Manager**, set ASP.NETv.4 (32 bit) to **Allowed**.

  The ASP.NETv.4 (32 bit) is located in the **Framework** folder as opposed to ASP.NETv.4 (64 bit), which is located in the **Framework64** folder. If you, by accident, set ASP.NETv.4 (64 bit) to **Allowed** instead of ASP.NETv.4 (32 bit), you will not be able to start the installation.

For more information, see the Support matrix.

Exchange prerequisites

If you use WorkZone Process, you need to specifically configure Exchange.

You must create an Exchange Account and set it up to:

- Send smartmails.
- Send email notifications.
- Monitor mailboxes.

You can set up the account on an Exchange On-Premises server or in Exchange Online.

Send on behalf

You can use an email account different from the email account of the SOMESERVICEUSERNAME to send smartmails. Thus allowing a user friendly sender to be seen as sender on smartmails. To do this, you will need to configure an email account that grants SOMESERVICEUSERNAME the right to send on behalf of the configured mail account.

Microsoft documentation links

To make SOMESERVICEUSERNAME able to send messages on behalf of a MailAgent user, make the configurations described here: http://technet.microsoft.com/en-us/library/aa998291(EXCHG.80).aspx

For more information about setting up Send As permission, see:

- Exchange On-Premises; Recipient permission
- Exchange Online: Shared mailboxes in Exchange Online

> **Example**: A mailbox which allows SOMESERVICEUSERNAME to send on behalf of someone could be `MailAgent@lmdom.local`.

See Configure WorkZone Process.

Exchange Autodiscover service

You can automate the configuration of how you want to send smartmails by configuring the Autodiscover service on the Exchange Server. The Exchange autodiscover service finds the endpoint for the Exchange service automatically when you configure how to send smartmails in WorkZone Process Configurator. See Configure WorkZone Process and the `ExchangeWebServicesUri` and `UseAutoDiscover` parameters in the Exchange configurations using EWS (Exchange Web Services) section, if you use command line configuration.

See also Autodiscover for Exchange in the Microsoft documentation.

Verify access to Exchange server and oData

Verify that the following is in place:

On the agent server

- Verify access to the Exchange EWS web service:

    1. Open Internet Explorer as the user who is sending e-mails.
    2. Go to `https://<Exchange Server Name>/EWS/Exchange.asmx`.

        This should return XML.

- Verify access to oData with SOMESERVICEUSERNAME:

    1. Open Internet Explorer as SOMESERVICEUSERNAME.
    2. Click **Tools** > **Internet options** > **Content**.
    3. Under **Feeds and web slices**, click **Settings**.
    4. Under **Advanced**, deselect the **Turn on feed reading view** check box.
    5. Click **OK**, and then go to `https://<hostname>/OData`.

        This should return XML.

On the web servers

Verify access to oData with SOMESERVICEUSERNAME.

1. Open Internet Explorer as SOMESERVICEUSERNAME.
2. Go to `https://<hostname>/OData`.

    This should return XML.

Access rights requirements

Administrator permissions

You must have administrator permissions on the local machine to install and set up the WorkZone Content Server and its component programs.

Run as administrator

You must always run programs, for example WorkZone ScanSQL, as an Administrator with elevated rights.

Exception: The WZSql database tool does not require administrator privileges with elevated rights.

Prerequisites for WorkZone Content Server database

Follow the instructions in About installing WorkZone Content Server before installing the database.

Configuration requirements

Installation of the WorkZone Content Server database requires:

- Installation of an empty Oracle database version with Intermediate Text. See supported Oracle versions in the Support Matrix.
- Installation of WorkZone Content Server where the creation of the WorkZone Content Server database tables and data take place.

WorkZone database templates

In a standard WorkZone Content Server installation, database templates are located in:
`C:\Program Files (x86)\KMD\WorkZone\Program\DBSetup\OracleTemplates`

You can find templates for Oracle, as well as a readme file that explains how to place the template in relation to the Oracle installation.

Requirement for access through ODBC

The database must be accessible through 32-bit ODBC. For more information, see the Configure the ODBC.

Database system administrator requirements

Before you start the installation, the database system administrator must create a SJSYSADM user with the SJ_PASSWORD profile and grants.

A database script from WorkZone can thereafter be applied which will assign the SJSYSADM user with the necessary rights for further installation, setup and maintenance of the database.

Service accounts

WorkZone requires the following service accounts to install WorkZone PDF, WorkZone Process, and WorkZone Mass Dispatch:

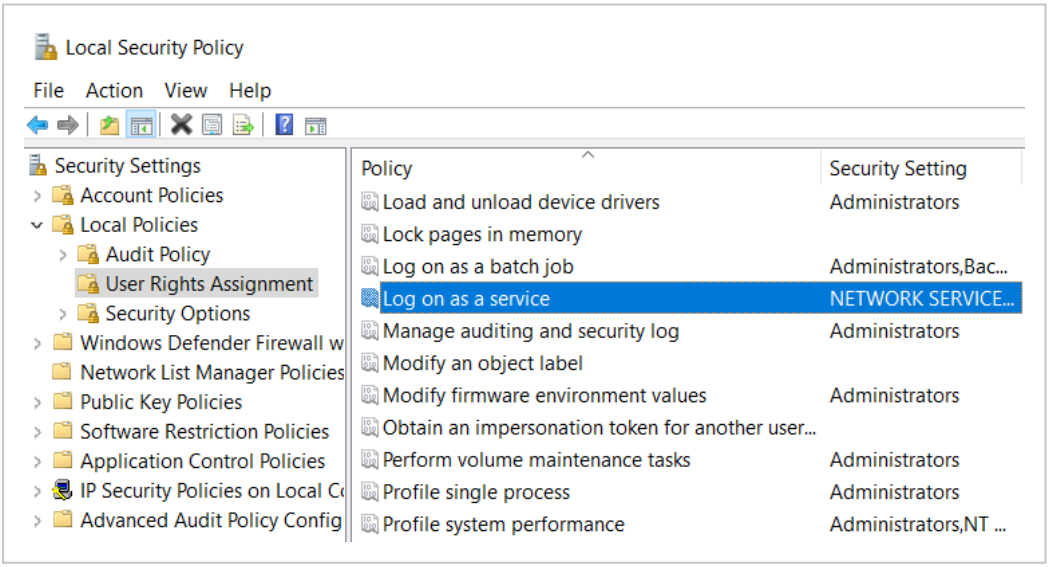
WorkZone PDF

> **Important:** By default, the crawler user is defined as *system*. In this case, the WorkZone PDF service will be executed as a Local System (see Microsoft documentation), and you do not need to follow the steps described below.

To install and run the WorkZone PDF crawler service, you need to grant the "Log on as a service" rights for the crawler user.

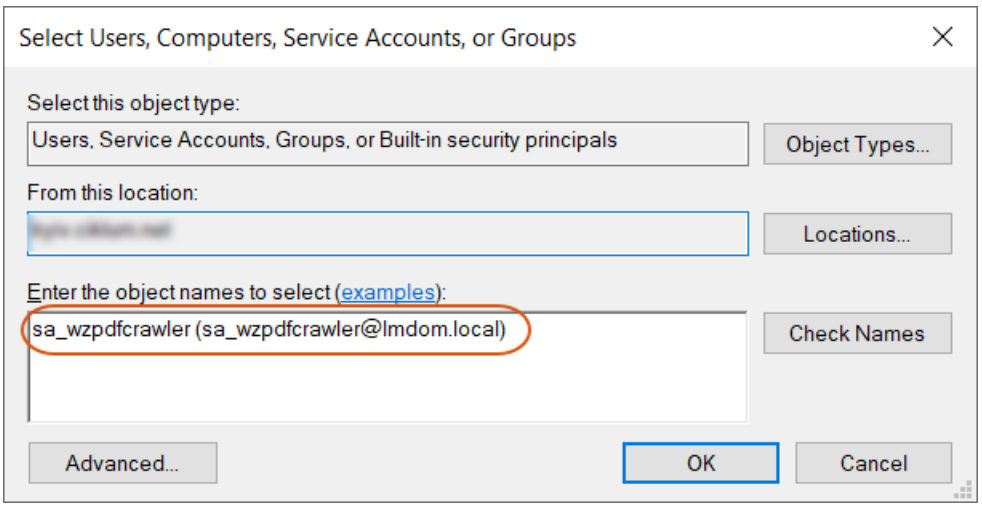
Create WorkZone PDF user with the "Log on as a service" rights

1. Go to **Local Security Policy > Local Policies > User Rights Assignment**.
2. Find *Log on as a service* among listed policies and double-click it.



3. Click **Add User or Group...**

4. Enter the crawler service user:



5. Click **OK**.

WorkZone Process

Before you install WorkZone Process or WorkZone Mass Dispatch, you must create a service user in Active Directory (AD).

Requirements for the service account:

- It can have any name. In the following, the service user is referenced as SOMESERVICEUSERNAME.
- It must be set up with the "Log on as a service" privilege.
- It must not be a member of any WorkZone replication groups, or used for any other WorkZone-related purposes or configurations as the SID of this user will be associated with a specific WorkZone user named SJPROCESSUSER in the WorkZone database.

When you configure WorkZone Process, enter the credentials of service account in the **KMD WorkZone Process Configuration Wizard** on the **Service Account** page. The configurator will take care of the SID association when you click **Next** to move on. See Configure WorkZone Process.

Assign an exchange account to a service account

The service account must have an exchange account to be able to send smartmails or to act as a delegate for another account that sends smartmails. To set up the exchange account for the service account in the Exchange Management Console, create a new mailbox for the existing AD service account.

Create a mailbox in Exchange Management Console

1. Open Microsoft Exchange Management Console.
2. Right-click **Mailbox** under **Recipient Configuration**, and select **New Mailbox**.
3. In the **New Mailbox** wizard, under **Choose mailbox type**, select **User Mailbox**, and click **Next** to proceed.
4. Under **Create mailboxes for**, select **Existing users**.
5. In the **Select User** dialog box, select the service user, and click OK.
6. Complete the wizard by entering a name alias and click **New**.

Service account acting on behalf of an account with an ordinary user name

If you want smartmails that are issued from a service account to appear as if they are sent from a user account with an ordinary user name, the service account must be assigned the permission to act on behalf of this user.

If a permission setup has not been created for a service account, smartmails that are sent from the service account will appear under a user name. To make smartmails from a service account appear as if they are sent from an ordinary email account, the service account must be assigned permissions from the email account that belongs to the ordinary email user.

Assign permissions to a service user to act on behalf of an ordinary mail user

1. Open Microsoft Exchange Management Console.
2. Click **Mailbox** under **Recipient Configuration**.
3. On the list of accounts, right-click the mail account of the user that should appear as the sender of smart tasks that are sent by the service user, and select **Manage Send As Permissions**.

4. In the **Manage Send As Permissions** wizard, click **Add**, and select the service user.
5. Click **Manage**, and complete the wizard.

Network connections

Component	Local Ports	Connects to	Protocol	Notes
AD replicator	N/A	Oracle, DC	N/A	Connected to Oracle when the replication is active. Time depends on the size of the Active Directory.
OCR and FIX agent	N/A	Oracle	N/A	Always connected to the Oracle while the NT Service is running.
SUB/WFM agent	N/A	Oracle, SMTP	N/A	Always connected to the Oracle while the NT Service is running.
Service Channels	N/A	Oracle, File, POP3	N/A	Always connected to the Oracle while the NT Service is running.
Scan Station	N/A	File server or FTP		

Certificates

Overview of WorkZone certificates

Product/Module	Certificate	Certificate name/type	Usage	For more information
WorkZone Process /SmartPost	e-Boks Strålfors	Functional certificate (funktionscertifikat)		e-Boks and Strålfors certificates
WorkZone Pro-	Interact	Functional certificate		Acquire and

Product/Module	Certificate	Certificate name/type	Usage	For more information
cess/Interact		(funktionscertifikat)		install the Interact certificate
WorkZone Process	Push notification certificates	Apple Push Services: dk.kmd.WorkZone Apple Push Services: dk.kmd.workzone.intune	Send notifications from WorkZone Process to WorkZone Mobile The certificates are installed in the certificate store as part of the WorkZone Process installation.	Configure push notification certificates for WorkZone Mobile in the WorkZone Process Administrator's Guide.
WorkZone CVR Integration	FOCES certificate	Functional certificate (funktionscertifikat)	Integration with Det Centrale Virksomhedsregister (CVR)	WorkZone CPR and CVR Integration
WorkZone Content Server	SSL Certificate	SSL Certificate	SSL (Secure Sockets Layer) Certificates must be configured in the Internet Information Server (IIS) as defined by Microsoft.	How to set up SSL on IIS 7 How To Set Up an HTTPS Service in IIS (External link to Microsoft technical documentation)

Important: Running the WorkZone Process modules requires that your certificates are valid. During installation, you can choose to disregard certificate errors and thus allow running the modules in environments with invalid certificates. Note, however, that this is

not a recommended option. In general it should only be possible to run WorkZone Process in environments with valid server certificates.

Other integrations

You can integrate WorkZone with the following third party products.

WorkZone CPR and CVR Integration

CPR

- In WorkZone Configurator > Global > Feature settings, activate WorkZone Content Server CPR integration.
- Contract with the hosting service provider (CSC)
- Application CPR Klient (`CprDirekte_V180.exe`) is configured with the required parameters (user name, and so on) according to the signed contract.

CVR

- In WorkZone Configurator > Global > Feature settings, activate WorkZone Content Server CVR integration.
- Valid FOCES certificate (Funktionscertifikat) from The Agency for Data Supply and Efficiency (Danish: Styrelsen for Dataforsyning og Effektivisering). Use the following URL: Datafordeler to access the agency's website.
- User name and password provided by CVR.
- Grant access to the URL https://s5-certservices.datafordeler.dk.

CPR Batch

- Permissions for accessing the FTP-site at the CPR-Office.
- Path to the format descriptions for the CPR extract.
- Path to the Interim directory.
- Permissions for accessing the database when importing the subscription files.

For more information regarding WorkZone CPR and CVR Integration, see [WorkZone CPR/CVR Integration guide]

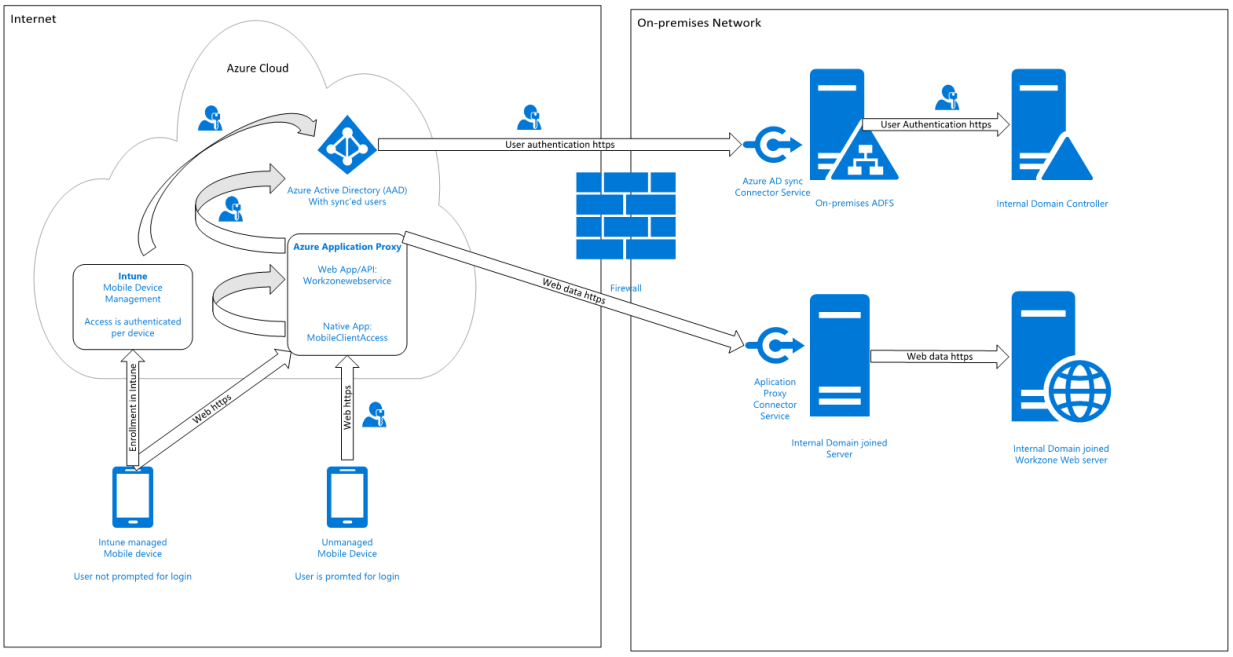
Microsoft Enterprise Mobility Suite (Intune) infrastructure

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 Azure Active Directory

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 Azure Active Directory 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 Azure Active Directory 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 Azure Active Directory, 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 Azure Active Directory, 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.

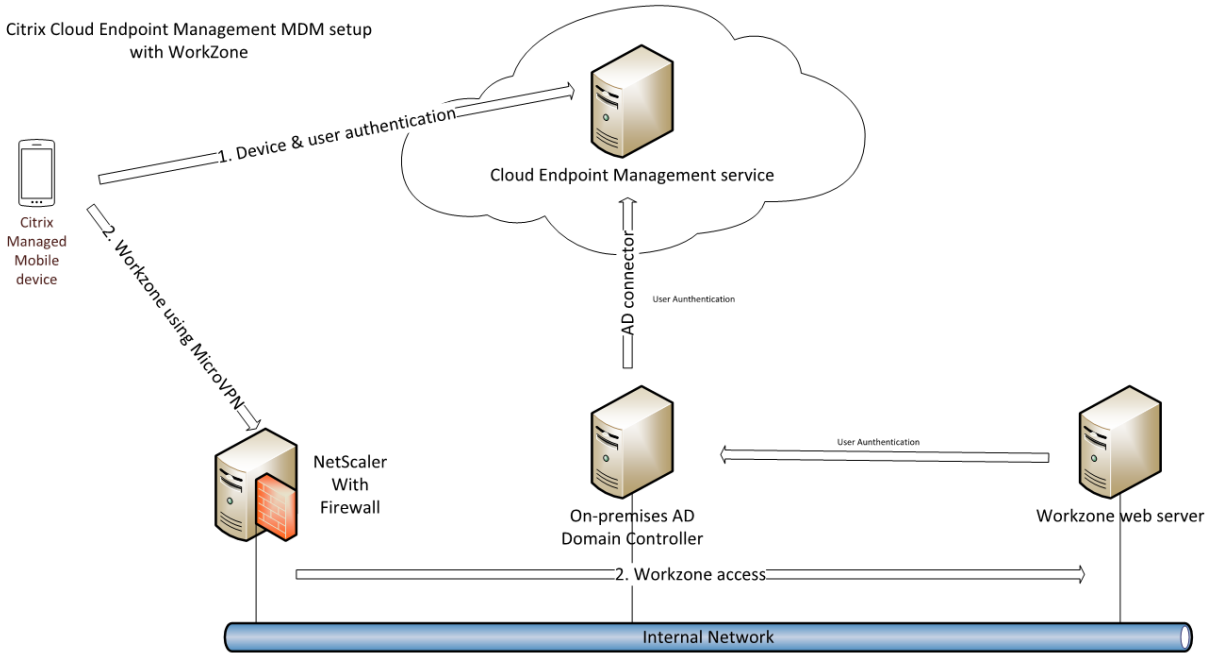
Citrix XenMobile infrastructure

You can deploy WorkZone Mobile using Citrix XenMobile. To allow WorkZone Mobile access to on-premise WorkZone through Citrix XenMobile, some configuration of your organization's infrastructure is required. You need to:

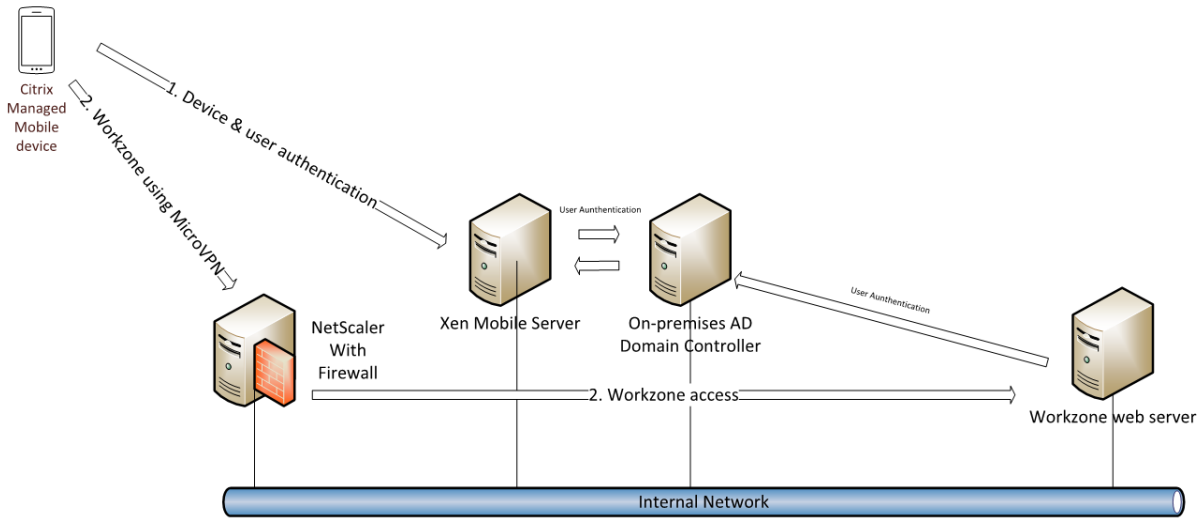
- Set up on-premises Citrix XenMobile server or Citrix Cloud Endpoint Management to manage organization's mobile devices.
- Establish a Citrix NetScaler with MicroVPN to an internal WorkZone web server.
- Make the WorkZone Mobile app available in Citrix Secure Hub.

The diagrams below show a conceptual overview of the components in the infrastructure and how they are set up to support WorkZone Mobile with Citrix XenMobile. The number of real servers, firewalls, load balancers, and so on, varies depending on how the environment is set up for a specific organization.

Cloud solution



On-premises solution



The set-up and configuration process varies depending on how the environment is set up for your organization. See Citrix documentation for relevant steps.

Configure WorkZone Mobile in Citrix XenMobile

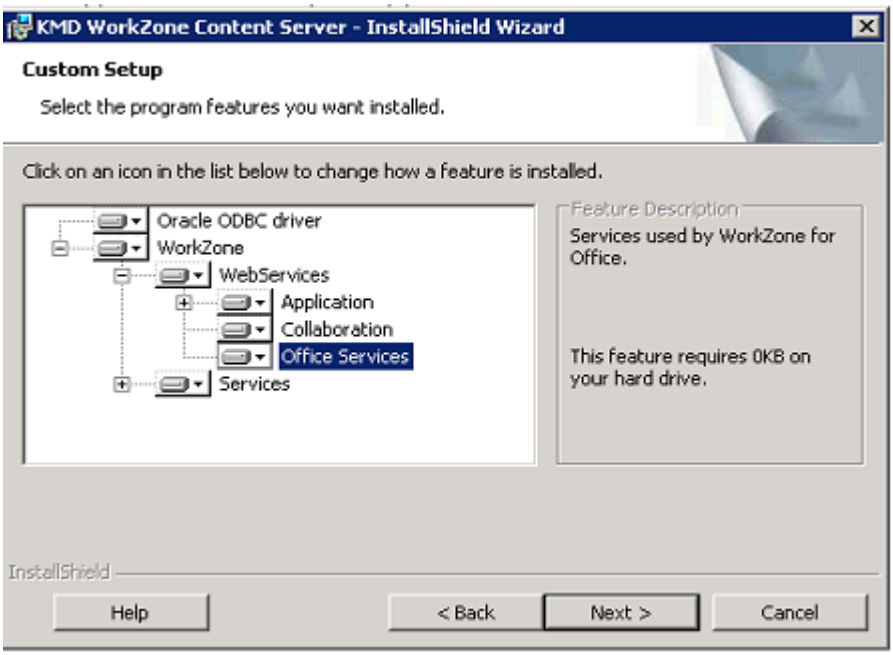
When the requirements to the infrastructure are fulfilled, you can set up and configure WorkZone Mobile in Citrix XenMobile. See Administrator Guide for WorkZone Mobile.

Product specific prerequisites

Apart of the common prerequisites listed in the previous sections, some of the WorkZone products have additional prerequisites. Use this section to take into account the full list of requirements.

WorkZone for Office

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



Required data and default values

For WorkZone 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 server settings.

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

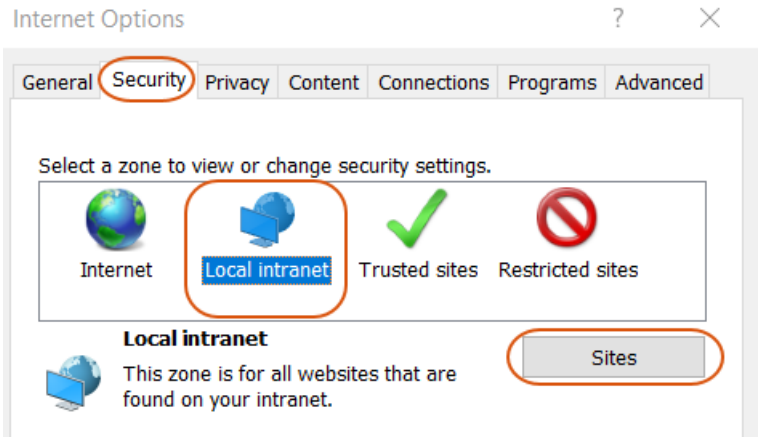
Sent items folder in Microsoft Outlook that has been sent in reply to another saved email. In this special case, there is a slight difference in behavior, since this reference can only be detected when **Cached Exchange Mode** is turned on.

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. Click **Tools** in your browser and select **Internet options**. The **Internet Options** dialog box opens.
2. On the **Security** tab, click **Local intranet** and then **Sites**.



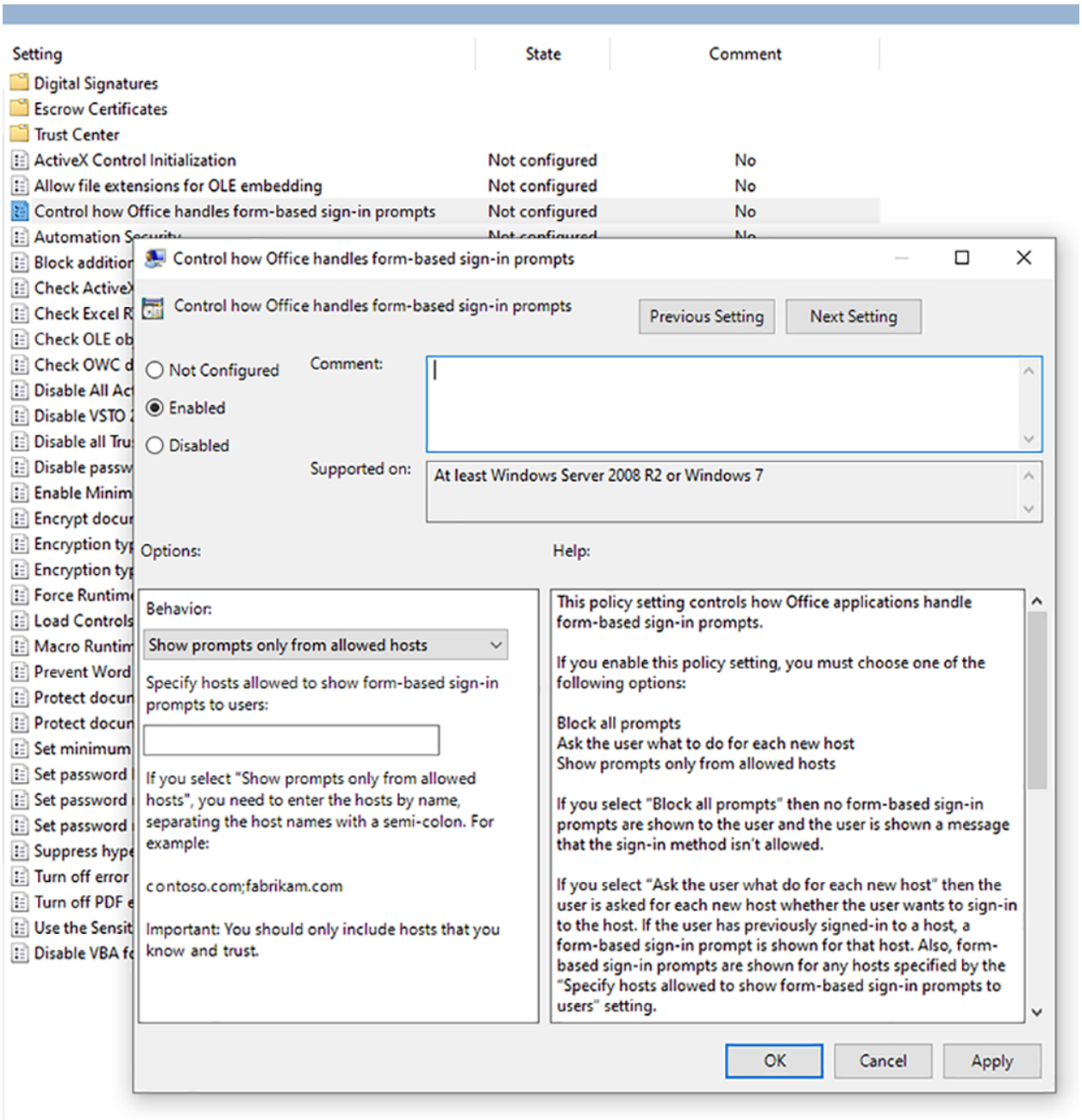
3. Click **Advanced**.
4. Type in your website domain, and click **Add**.

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**.

WorkZone Process

SmartPost

Certificates

e-Boks and Strålfors certificates

If you want to use SmartPost in WorkZone Process you need to acquire certificates for e-Boks and Strålfors.

Local Registration Authority (LRA) - NemID administrator

The NemID administrator is an employee who is authorized to create access to the service providers' administration portals (e-Boks Administration Portal and Strålfors Connect), create and issue employee certificates to other employees, and assign different roles to the employees such administrator, super administrators, and so on. The NemID administrator is often an employee of the IT department in an organization.

The NemID administrator needs to have an LRA certificate, which is a special type of certificate that allows the NemID administrator to manage and issue employee certificates.

Point out an administrator and issue an employee certificate

The LRA administrator assigns an employee as administrator (or super administrator) and issues an employee certificate to this employee. This employee will then be authorized to create dispatch and retrieval systems and to manage the organization's e-Boks and Strålfors configurations.

The typical process is as follows:

1. The employee is requested to order an employee certificate at NemID. See https://www.medarbejdersignatur.dk.
2. The LRA administrator receives an approval message from NemID and approves the NemID.
3. The employee receives a message from NemID with instructions on how to download the certificate.
4. The LRA administrator assigns the employee as administrator or super administrator.

Acquire and use of the certificate (funktionscertifikat)

The LRA administrator needs to acquire a certificate (funktionscertifikat). The SmartPost process will use the certificate as electronic identification in relation to the service providers. The LRA administrator hands over the certificate to the administrator, who will then use the certificate to configure the systems.

The certificate allows a system A to identify itself towards another system B, where system A submits a service.

The certificate can be used in two different ways:

- As dispatcher

  This is system A. System A identifies itself towards another system B. System A will use the certificate to encrypt the communication with the use of a private key.

- As recipient

  This is system B. System B has received the certificate in a form where it only contains a public key that system B can use to decrypt the communication from system A. If the communication does not derive from system A but from a third unknown

system C that pretends to be system A, it will be revealed during the decryption. Only the system with the certificate with the private key can make an encryption that can be decrypted with the public key that system A previously handed over to system B.

The certificate must be stored in the certificate store on the server that runs the SmartPost process.

See Acquire and install the e-Boks Certificate for instructions on the certificate process.

Acquire and install the e-Boks Certificate

The organization needs a certificate from Nets for SmartPost to work as a dispatch system for e-Boks. The steps in the certificate process are:

1. Acquire a certificate (Funktionscertifikat)
2. Import the certificate in to the certificate store
3. Add the private key of the IIS user to the certificate
4. Export the P12 certificate to a CER certificate
5. Upload the certificate to e-Boks
6. Apply the certificate to the e-Boks dispatcher

Acquire a certificate (Funktionscertifikat)

An employee at the organization must order a certificate from Nets. The employee must be a NemID administrator at the organization and have an employee signature to be able to order a certificate. The employee will receive an email from Nets with an installation code to use to get the certificate from Nets and a password, which is connected to the certificate.

The employee starts the certificate process using the Nets link: https://www.nets-danid.dk/produkter/funktionssignatur/bestil_funktionssignatur/ and follow the instructions. When the process has been completed, the employee will receive an email with an installation code and a link to start the installation process. During the installation process, the employee selects the certificate type **PKC#12**, enters the installation code from the email, and creates a password for the certificate. The result of the installation is a certificate file.

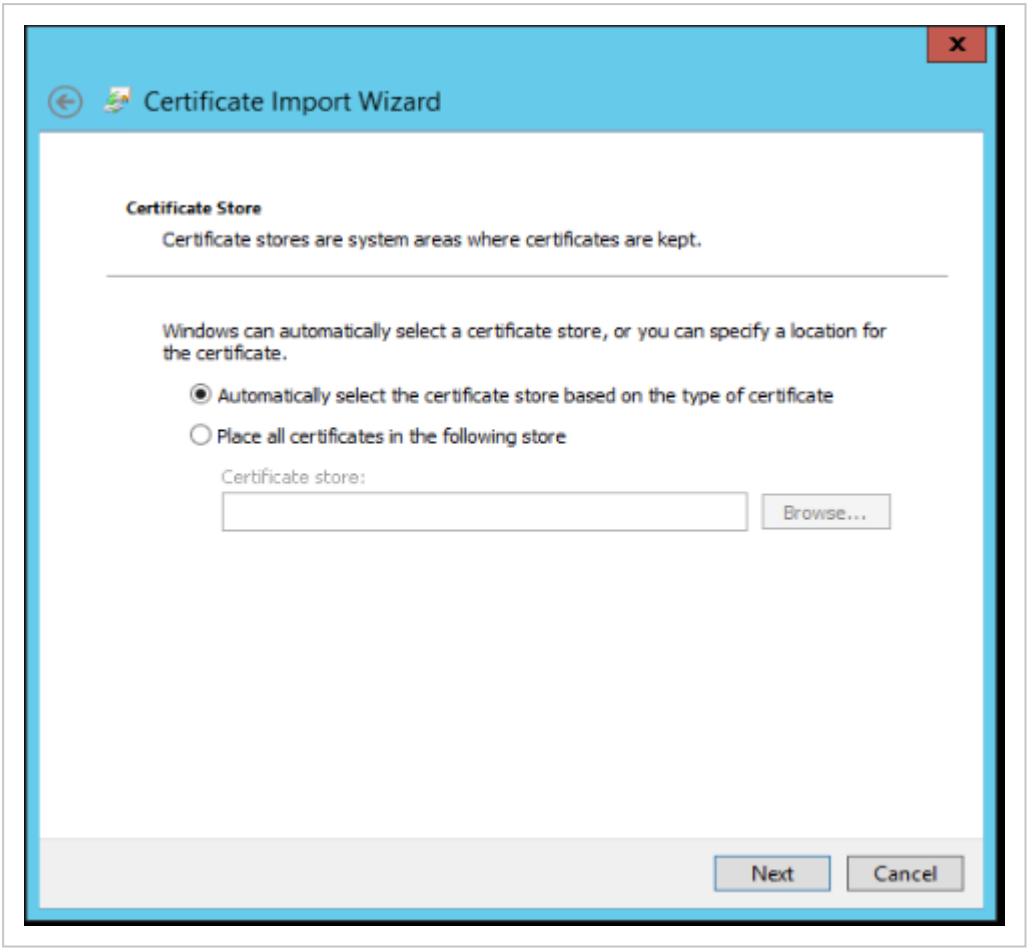
> **Important:** The certificate file and the password are connected and will be used later in the process.

Import the certificate in to the certificate store

You need to import the certificate in to the certificate store on the server that runs the SmartPost process using the **Windows Certificate Import Wizard**.

1. Double-click the certificate to start the **Certificate Import Wizard**.
2. On the Welcome page, click **Local Machine**, and then click **Next**.

3. Click Next until you reach the **Certificate Store** page, and then select **Automatically select the certificate store based on the type of certificate** option.



4. Complete the wizard.

Add the private key of the IIS user to the certificate

You must add the private key of the IIS user that runs the WzpSvc app pool, typically that is **IIS APPPOOL\WzpSvc**, to the SmartPost certificate. This is done in the **Certificate Manager**. See Apply certificates to SmartPost.

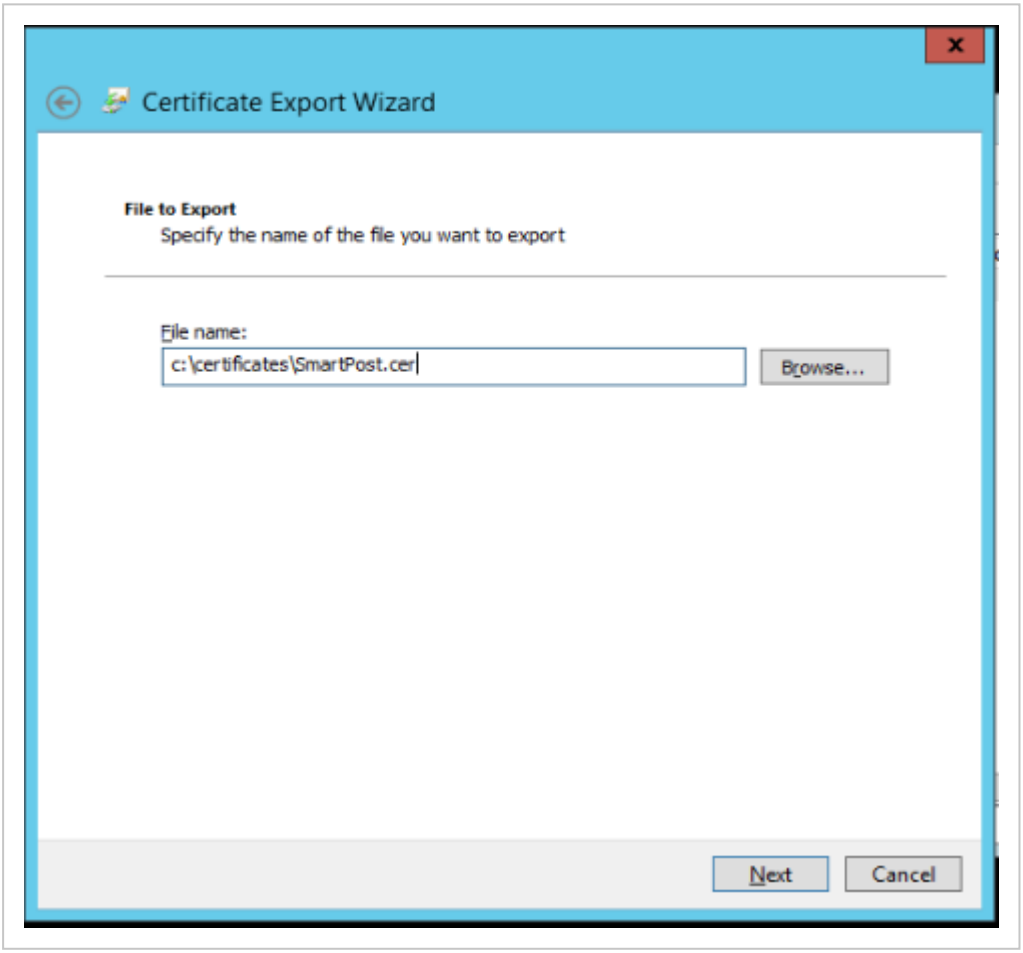
Export the P12 certificate to a CER certificate

The certificate file that is acquired from Nets is a P12 certificate, see the previous section. This certificate will be used by the dispatcher in WorkZone. However, in e-Boks you must register

the certificate in the CER format. Therefor, you need to convert the P12 certificate file to a CER certificate file.

Export certificate

1. Open **Certificates Manager**.
2. Expand **Certificates Local Computer** > **Personal** > **Certificates**.
3. Right-click the SmartPost certificate, and then select **All tasks** > **Manage Private Keys** > **Export**. The **Certificate Export Wizard** starts.
4. Click **Next** until you get to the **Export File Format page**, and then select **BASE-64 encoded X.509 (.CER)**, and then click **Next**.
5. On the **File to Export** page, enter a name of the file to export, and then click **Next**.



6. Complete the wizard.

A CER certificate file is created. The next step is to upload it to e-Boks.

Upload the certificate to e-Boks

You upload the CER certificate file to e-Boks using the e-Boks Administration Portal.

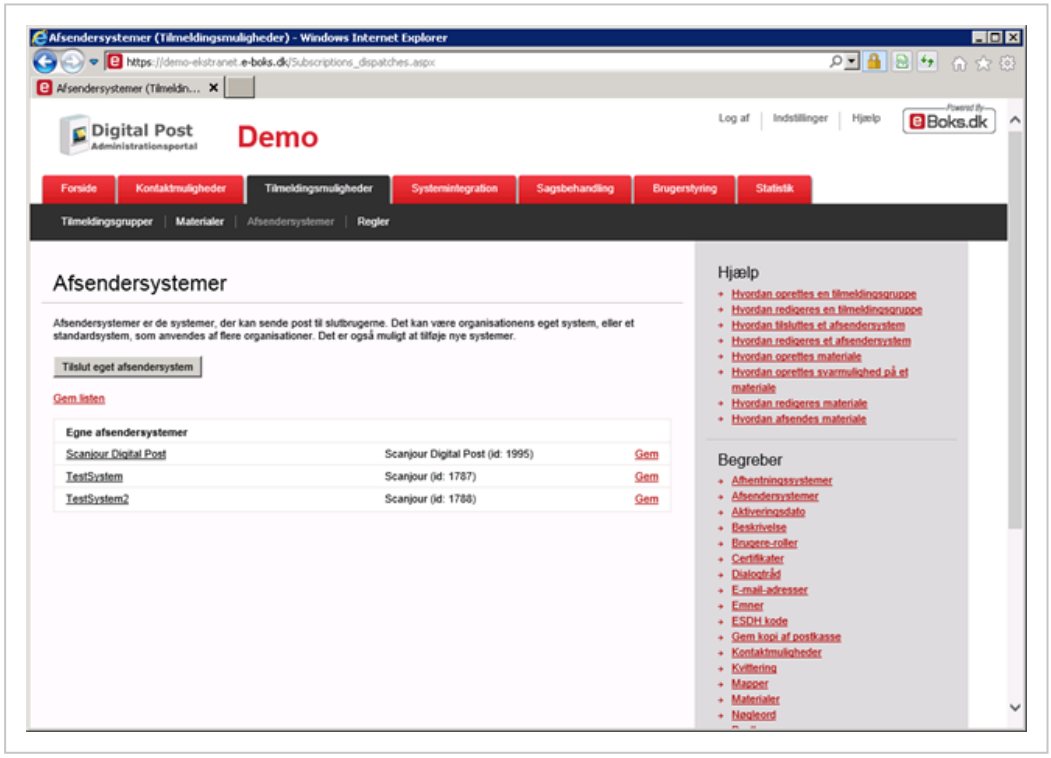
Upload certificate

1. In a browser, open the e-Boks Administration Portal

   Demo: https://demo-ekstranet.e-boks.dk/

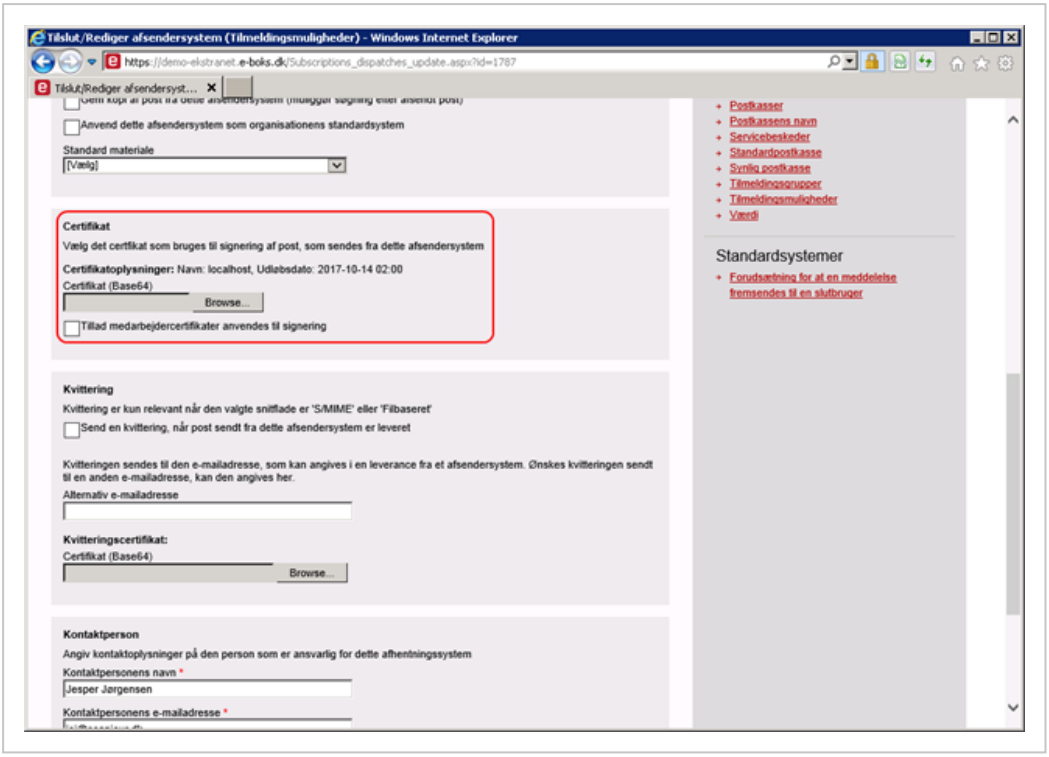
   Production: https://ekstranet.e-boks.dk

2. Log in with your credentials.
3. On the **Welcome** page, select **Tilmeldingsmuligheder** (Registration options).
4. Click **Afsendersystemer** (dispatch systems), and then click the dispatch system, you want to use.



   The **Rediger afsendersystem** (Edit dispatch system) page is shown.

5. On the **Rediger afsendersystem** page, scroll to the **Certifikat** (Certificate) section, and browse to locate the certificate.



6. Click **OK**. The certificate is now registered in e-Boks.

Apply the certificate to the e-Boks dispatcher

You register the e-Boks certificate in WorkZone Configurator.

1. In WorkZone Configurator, click **Process** > **Process dispatchers**.
2. Select the **eBoks** dispatcher.
3. Enter the thumbprint of the certificate in the **EboksCertificateThumbPrint** field.

See also Process dispatcher module in the WorkZone Configurator Installation Guide.

Apply certificates to SmartPost

Once you have received a certificate and imported it to the certificate store, you need to:

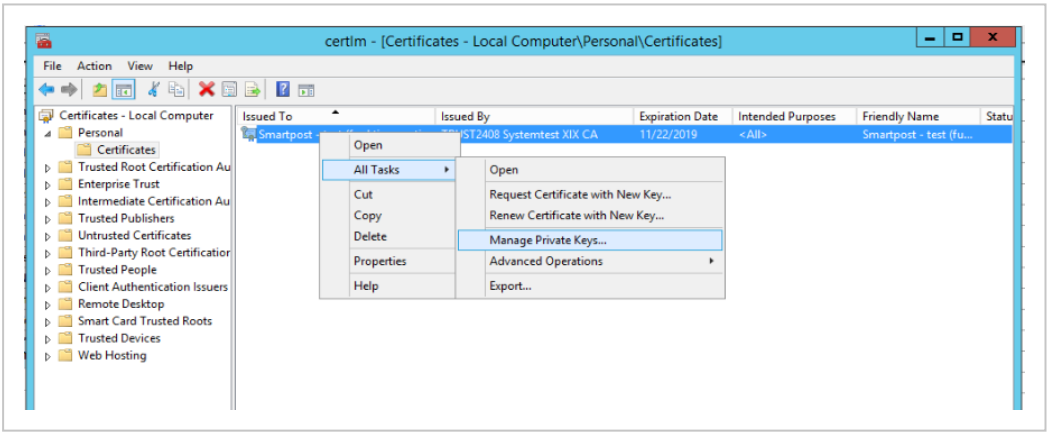
- Add the private key of the IIS user to the dispatcher certificate.
- Apply the certificate to the SmartPost dispatcher.

Add the private key of the IIS user to the dispatcher certificate

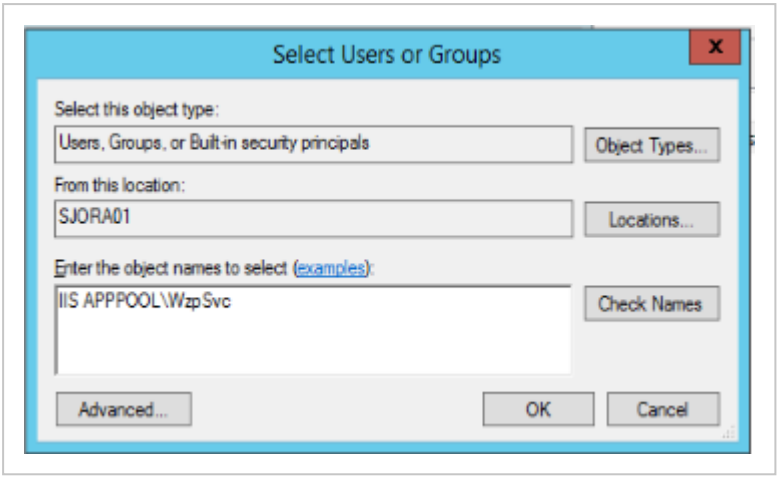
For the dispatchers, such as e-Boks and Strålfors, to work with SmartPost, you must add the private key of the IIS user that runs the WzpSvc app pool to the dispatcher certificates. Typically this is an **IIS APPPOOL\WzpSvc** user. This is done in the **Certificate Manager**. You need to locate the dispatcher certificate and manage its private keys. By default, the dispatcher certificates are located under the current computer account.

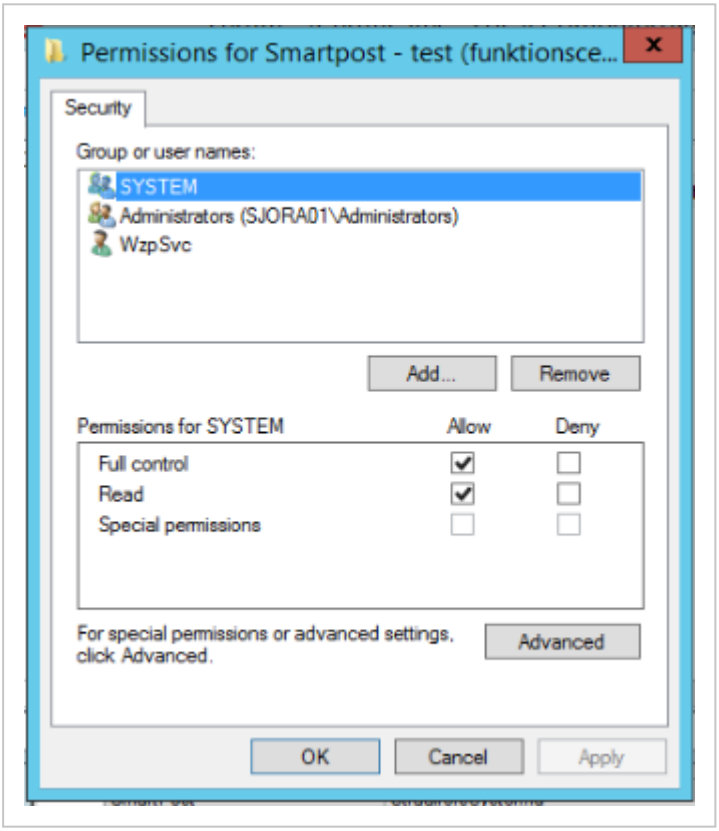
> **Important:** You need to re-add the private key after upgrading WorkZone.

1. Open **Certificates Manager** (mmc.exe).
2. Expand **Certificates Local Computer** > **Personal** > **Certificates**.
3. Right-click the SmartPost certificate and select **All tasks** > **Manage Private Keys**.



4. In the **Permissions** dialog box, click **Add** to add the private key, typically the **IIS APPPOOL\WzpSvc** user.



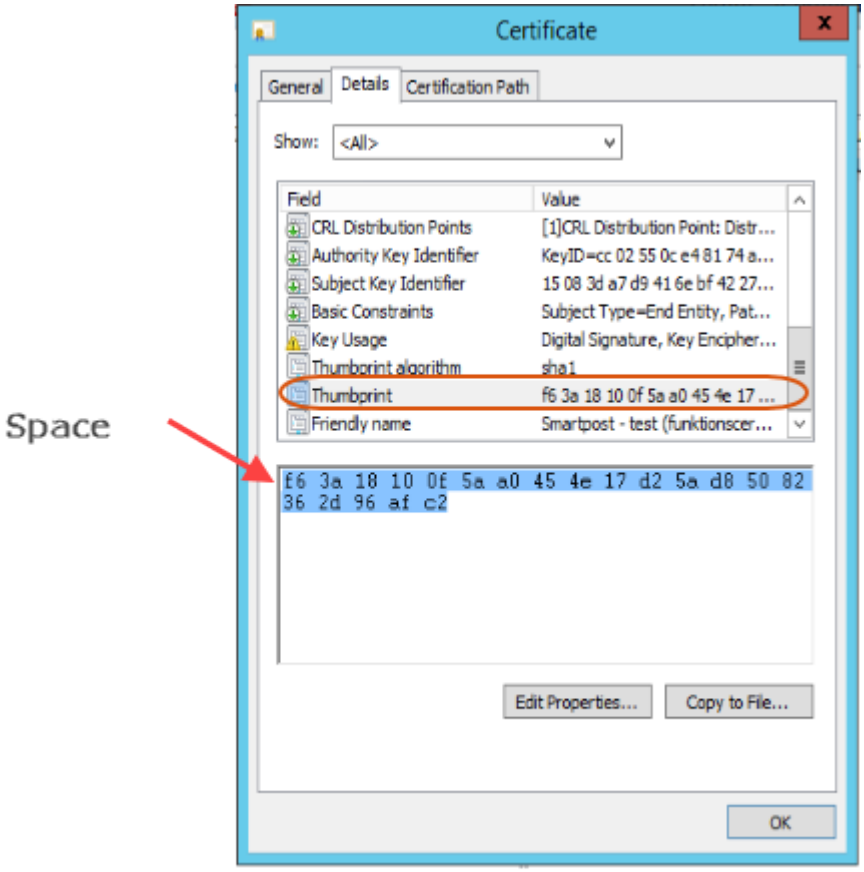


Copy thumbprint and apply the certificate to the dispatcher

You copy the thumbprint of the certificate from the Certificates Manager and paste it into the dispatcher settings in WorkZone Configurator.

1. Open **Certificates Manager** (mmc.exe).
2. Expand **Certificates Local Computer** > **Personal** > **Certificates**.

3. Double-click the SmartPost certificate.
4. In the **Certificates** dialog box, click the **Details** tab.
5. Select **Thumbprint** in the list.
6. Mark the thumbprint without the first space and press Ctrl + C to copy the thumbprint.



For more information about the extra space, please see Microsoft support article Certificate thumbprint displayed in MMC certificate snap-in has extra invisible unicode character.

Apply the certificate to the dispatcher

You register the certificates in WorkZone Configurator.

1. In WorkZone Configurator, click **Process** > **Process dispatchers**.
2. Select a dispatcher, for example **e-Boks** or **Straalfors**.

3. Paste the thumbprint that you just copied into into the **EbooksCertificateThumbPrint** field.

See also Configure dispatchers and Process dispatchers in the WorkZone Configurator Installation Guide.

Dispatchers

Digital mail

e-Boks prerequisites

Remote print

SmartPost supports Strålfors Connect and KMD OneTooX for remote print. Before you can start to configure SmartPost to use OneTooX or Strålfors Connect, the authority or company must make an agreement with KMD Printcenter or Strålfors depending on which print center will be used.

Strålfors prerequisites

OneTooX prerequisites

e-Boks prerequisites

Before you can start using the SmartPost process, you need to complete some configuration tasks for SmartPost to be able to communicate with e-Boks.

1. e-Boks opens for the organization's IP addresses
2. Agreement on provision of NemID services (tilslutningsaftale)
3. Retrieval system
4. Configure e-Boks

e-Boks opens for the organization's IP addresses

A prerequisite for SmartPost to be able to communicate with e-Boks through the REST interface is that e-Boks knows the IP addresses of the systems that use the services of e-Boks. These are typically registered at Digitaliseringsstyrelsen (Danish Agency for Digitisation) from where e-Boks usually gets the information.

> **Important:** If the information about e-Boks addresses is not up-to-date, SmartPost will not be able to contact the services of e-Boks.

The IP address is the IP address(es) that is known from the WAN (typically the Internet).

> **Tip:** From the organization's network, you can determine the IP address by using the website: http://www.myip.dk.

Agreement on provision of NemID services (tilslutningsaftale)

The LRA administrator makes an agreement with e-Boks. See instructions Tilslutning til Digital Post Administrationsportalen from Digitaliseringsstyrelsen.

The agreement must be completed before the configuration of e-Boks can start.

Retrieval system

This sections describes the configuration tasks in connection with setting up a retrieval system in the e-Boks administration portal. The retrieval system allows the SmartPost process to retrieve messages from a mailbox in e-Boks. SmartPost retrieves the messages, such as replies from citizens and organizations to messages in e-Boks and unsolicited messages, and saves them automatically in WorkZone.

Create a retrieval system

Before you start this process, make sure that the organization's IP address is known by e-Boks and that an agreement has been made so that the REST service and the e-Boks administration portal are available. You can verify IP address and the agreement are in place it by logging into the e-Boks administration portal using this link: http://ekstranet.e-boks.dk/. If clicking the link results in a page with a text saying "Kun adgang for myndigheder" (Only accessible for authorities), the organization is either not an authority, or the agreement has not yet been concluded.

See e-Boks opens for the organization's IP addresses and Agreement on provision of NemID services (tilslutningsaftale).

The customer needs to create a retrieval system at e-Boks. This can be done via e-Boks administration portal (http://ekstranet.e-boks.dk/).

The table below describes the values that must be applied to the retrieval system.

Value name	Value	Description
Name	Suggestion: ”KMD SmartPost Retrival”	The name by which the retrieval system can be recognized.
EAN no.	Customer specific	The EAN number of the authority.
Delivery type	Pull	Specifies whether e-Boks needs to “push” messages into the customer’s system, or whether SmartPost needs to request e-Boks’s service in order to retrieve the messages (pull). SmartPost only uses pull.
API Version	v1	Currently, SmartPost only supports v1.
Certificate	Customer specific	The certificate to e-Boks is uploaded here.
Name of contact person	Customer specific	The name of the person at the customer's business who e-Boks must be able to contact in connection with questions and handover of commercial information. This will typically be a manager in the customer’s organization.
Email address of contact person	Customer specific	The email address on which the contact person can be contacted.
Phone number of contact per-	Customer specific	The phone number on which the contact person can be contacted.

Value name	Value	Description
son		

When the values have been entered, and the retrieval system is created, e-Boks automatically assigns an ID to the retrieval system. This ID must be used in connection with the configuration of SmartPost so that SmartPost knows which retrieval system to use.

See Configure SmartPost for receiving messages.

Create mailboxes

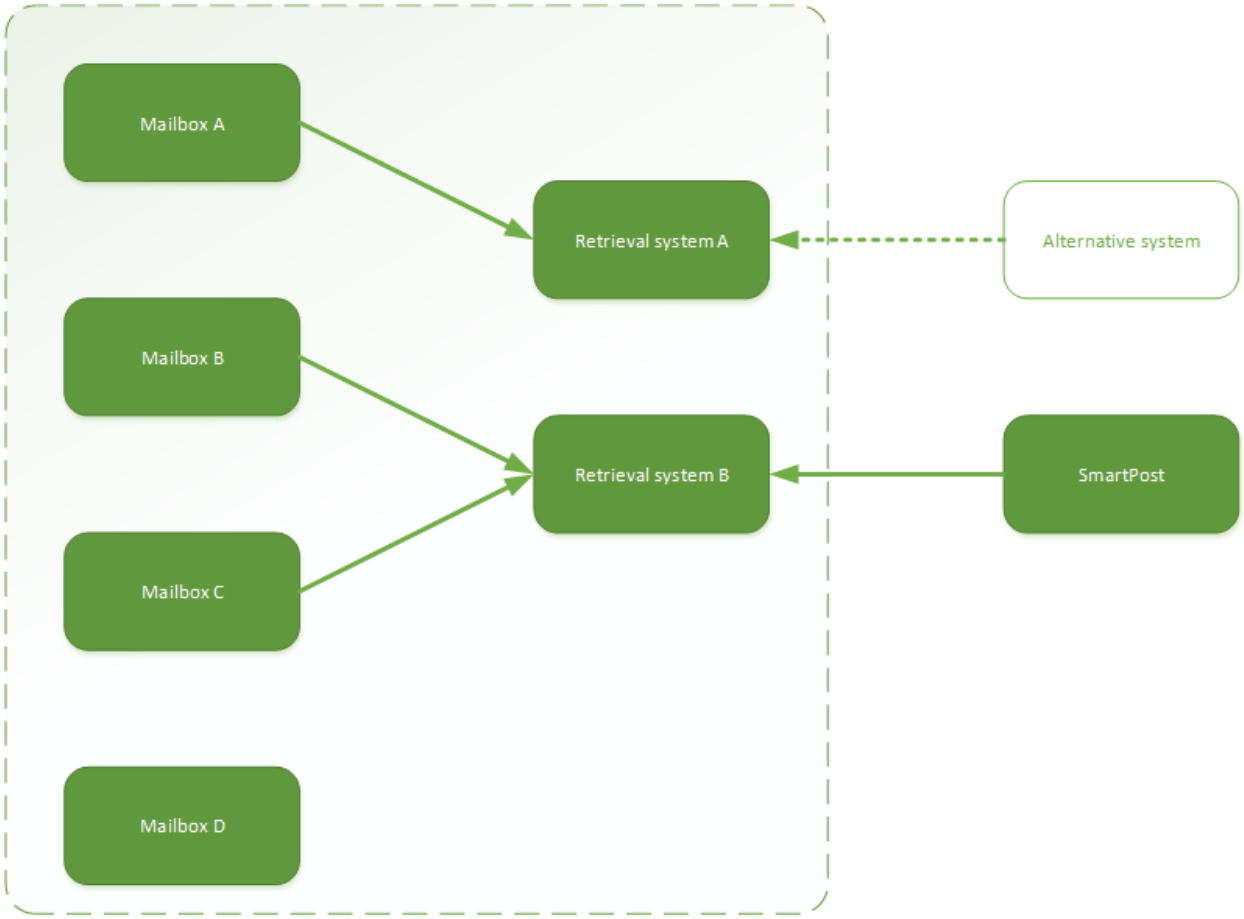
The organization needs to create at least one mailbox at e-Boks in which messages from citizens or an organization can be gathered, before they are collected by the SmartPost retrieval service. Subsequently, the mailbox needs to be connected to the Retrieval system.

Depending on the size of the organization and how it is organized, the organization can decide whether more than one mailbox needs to be configured. As SmartPost applies to a retrieval system and not to a specific mailbox, the customer can decide the number of mailboxes independently of SmartPost. In connection with the configuration of individual mailboxes in e-Boks, the customer can choose if the mailbox should be emptied by a retrieval system and, in that case, by which one. The diagram below shows an example of mailboxes and retrieval systems that are configured in e-boks and SmartPost.

Mailbox A is connected to retrieval system A. If necessary, an alternative system can retrieve messages from Retrieval system A.

Mailbox B and Mailbox C are connected to Retrieval system B. As SmartPost has been configured to retrieve messages from Retrieval system B, Mailbox B and Mailbox C are emptied by SmartPost.

Mailbox D is not connected to any retrieval system. As a result, SmartPost (or an alternative system) cannot retrieve messages from this mailbox via the REST interface.



The table below describes the values with which an e-Boks mailbox can be configured.

Value name	Value	Description
Name	For example: ”Mail for organization”	The name of the mailbox as the end user sees it.
Description	This mailbox is used for replying to messages sent by SmartPost as well as unsolicited messages.	A description of the mailbox for users who later use the administration portal.
Instructions	Send mail to this mailbox if you want to contact the organization.	Description of the mailbox that the end user sees.

Value name	Value	Description
Select folder for placing the mailbox	See notes	In a minimum configuration, there will only be one mailbox, and this mailbox will be the root mailbox. In such a case, the selection must be empty. In cases of more complex configurations with more mailboxes, the selection is based on the planned mailbox hierarchy.
Activation date	Now	Specifies the date where the mailbox will be active, that is visible to the end user.
External code can be used freely by suppliers and is available via system call	Empty	Not used.
This mailbox must be used by default for reception of mail, in cases where the end user makes a direct request	Selected	In the minimum configuration, the same mailbox will be used for both end user requests and unsolicited requests. In this case, the mailbox must be the default mailbox, for which reason the field must be selected. In cases of more complex configurations with more mailboxes, this mailbox is not necessarily selected by default.
The mailbox must be visible to the end user	Selected	In the minimum configuration, the same mailbox will be used for both end user requests and unsolicited requests. In this case, the mailbox must be visible so that the end user can use it for unsolicited requests. In cases of more complex configurations with more mailboxes, this mailbox is not necessarily visible.

Create subject

A minimum of one subject for one of the mailboxes connected to the retrieval system from which SmartPost is to retrieve messages must be configured.

Value name	Value	Description
Subject name	For example: “Contact to organization”	The subject that the end user can choose in connection with sending in an unsolicited message for an authority.
Form	Empty	Not supported by SmartPost.

See also e-Boks and Strålfors certificates

Configure e-Boks

SmartPost uses e-Boks to implement digital mail (Digital Post). For SmartPost to be able to communicate with e-Boks, the organization must make an agreement (tilslutningsaftale) with e-Boks first.

To configure digital mail using e-Boks, you need to complete the following steps.

1. Acquire and install a certificate.
2. Ensure Internet access.
3. Configure the dispatch system.
4. Configure the retrieval system.

You need to complete all steps for both test and production environments.

Certificate

The organization must acquire and install a certificate (funktionscertifikat) with a password. See Acquire and install the e-Boks Certificate.

Apply the certificate to the SmartPost process

You must add the private key of the IIS user that runs the WzpSvc app pool to the e-Boks certificate and set up the e-Boks dispatcher to run with this certificate. See Apply the certificate to the dispatcher.

Internet access

For SmartPost to be able to communicate with e-Boks, it is required that the server that runs SmartPost has Internet access to e-Boks.

Environment	URL	Port
Test	https://demo-rest.e-boks.dk/V1.svc	443
Production	https://rest.e-boks.dk/v1.svc	443

As SmartPost is deployed on the web servers, it is only required to open for access to e-Boks from the web servers.

Configure the dispatch system

When you have uploaded the certificate and configured a dispatch system using the e-Boks Administration portal, you need to configure SmartPost to reflect the configuration of the dispatch system. See Configure SmartPost for sending messages.

Configure the retrieval system

When you have uploaded the certificate, you can start configuring a retrieval system using the e-Boks Administration portal. The minimum configuration of a retrieval system consists of a mailbox and a subject, to which you attach the retrieval system. Next, you need to configure SmartPost to reflect the configuration of the retrieval system. See Configure SmartPost for receiving messages.

Strålfors prerequisites

Before you can start setting up and configuring remote print using Strålfors, you must make an agreement with Strålfors

The following prerequisites must be fulfilled:

- The organization must make an agreement with Strålfors.
- The organization must get a certificate. It is possible to use the same certificate as the one used for e-Boks, but it needs to be clarified with Strålfors.
- Find out which protocol Strålfors uses.

See also e-Boks and Strålfors certificates.

Configure Strålfors

To configure remote print using Strålfors, you need to complete the following steps.

1. The authority or company must make an agreement with Strålfors and install a certificate. See Apply the certificate to the SmartPost process.
2. Set up the test and production systems. See Test and production systems.
3. Configure a Strålfors dispatcher. See Configure dispatchers.
4. Include the Strålfors dispatcher in a dispatch sequence. See Configure dispatch sequences.
5. Configure Strålfors print types. See Configure print types.

You need to complete all steps for both test and production environments.

Certificate

Strålfors will assist with the installation of the certificate and the necessary configurations. When this is in place, you configure SmartPost with system ID, password, and certificate thumbprint.

> **Note:** You can clarify with Strålfors whether you can use the same certificate that you use with e-Boks, or if you need an additional certificate.

This process applies to both test and production.

Apply the certificate to the SmartPost process

You must add the private key of the IIS user that runs the WzpSvc app pool to the Strålfors certificate and set up the Strålfors dispatcher to run with this certificate. See Apply the certificate to the dispatcher.

Test and production systems

For SmartPost to be able to communicate with Strålfors Connect, it is required that the server that runs SmartPost has access to Strålfors Connect via the Internet.

Environment	URL	Port
Test	https://testprint.sconnect.dk/fjernprint/1.0.0	443
Production	https://prodprint.sconnect.dk/fjernprint/1.0.0	443

SmartPost is deployed on the web servers and therefore it is only required to get access to Strålfors from the web servers.

OneTooX prerequisites

Before you can start to use OneTooX and send SmartPost messages to KMD Printcenter for printing, the following prerequisites must be fullfilled:

- The organization must make an agreement with KMD Printcenter.
- The organization must get a OneTooX system key from KMD Printcenter. The system key is a PKE file.
- Document types must be defined and set up by KMD Printcenter. The OneTooX document types contains information about the dispatch of a document, for example if it is A or B mail, the envelope type, single-sided or double sided, and so on.

  OneTooX requires at least one documentation type.

  You need the names of the document types for configuring SmartPost print types.

Configure OneTooX

To configure OneTooX, you need to complete the following steps:

1. The organization must make a OneTooX agreement with KMD Printcenter.
2. Get a system key from KMD Printcenter, and configure it in WorkZone Configurator. See Apply the OneTooX system key to SmartPost.
3. Define document types, which KMD Printcenter will create. Once created, get the names of the document types. You will need the names of the document types to set up print types in WorkZone Configurator. At least one document type must be defined.
4. Set up test and production systems. See Test and production system.
5. Configure a OneTooX dispatcher. See Configure dispatchers.

6. Include the OneTooX dispatcher in a dispatch sequence. See Configure dispatch sequences.
7. Configure OneTooX print types. See Configure print types.

Apply the OneTooX system key to SmartPost

You must specify the system key when setting up a OneTooX dispatcher.

1. Open the PKE file that you have received from KMD Printcenter in a text editor, for example Microsoft Notepad.
2. Select all the text and copy it to clipboard.
3. In WorkZone Configurator, go to **Process** > **Process dispatchers**.
4. Point to next to the OneTooX dispatcher, and click  **Edit parameters**.
5. Paste the system key in plain text into the **Systemkey** field.

Test and production system

For SmartPost to be able to communicate with OneTooX, you need to set up a test and production system.

Environment	URL	Port
Test	https://test.doc2mail.dk/delivery/FileUploader.asmx	443
Production	https://privat.doc2mail.dk/delivery/FileUploader.asmx	443

Interact

Acquire and install the Interact certificate

Before you can start using the Interact connector service workflow, you need to acquire the functional certificate that was used for the Interact installation including the private key. The steps in the certificate process are:

The steps in the certificate process are:

1. Acquire a certificate
2. Import the certificate to the certificate store
3. Add the private key of the IIS user to the certificate
4. Apply the certificate to the Interact service workflow

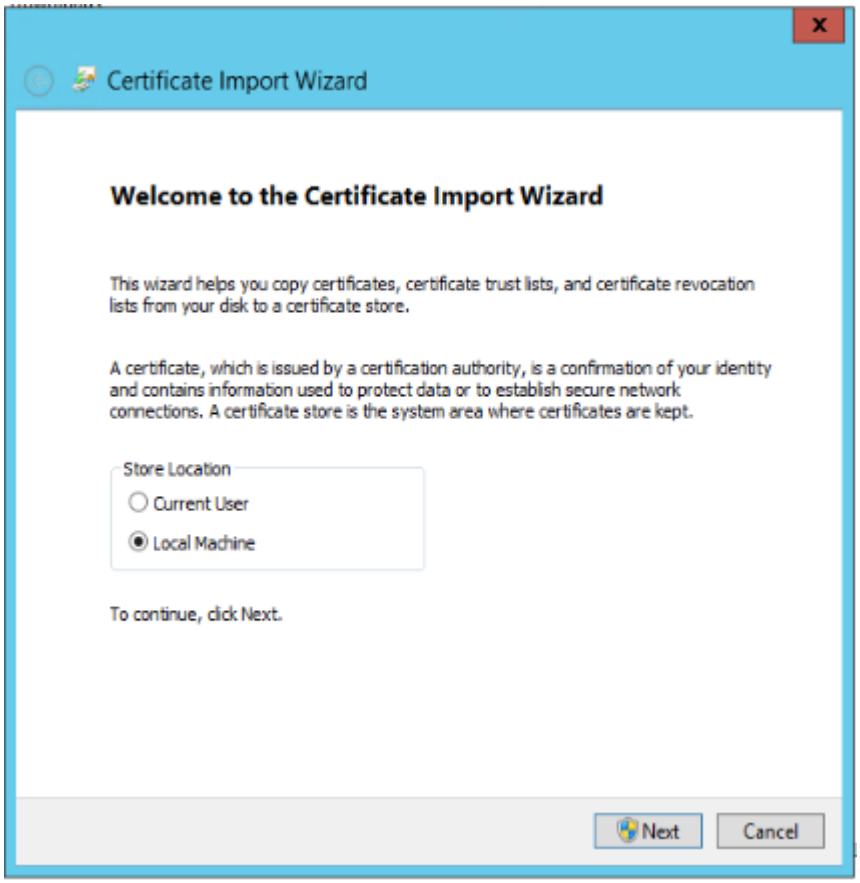
Acquire a certificate

Contact the organization's certificate administrator to get the Interact certificate including the private key that can be used for Interact.

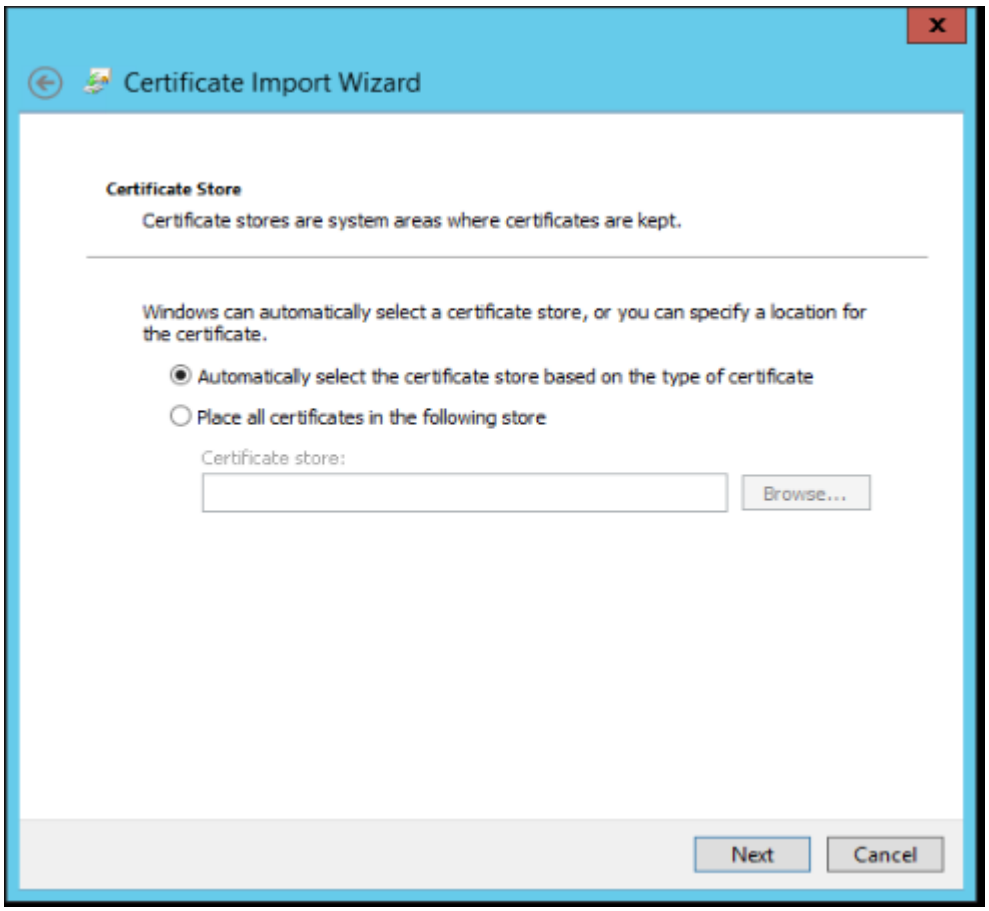
Import the certificate to the certificate store

You need to import the certificate to the certificate store on the WorkZone server that runs the Interact service workflow using the **Windows Certificate Import Wizard**.

1. Double-click the certificate to start the **Certificate Import Wizard**.
2. On the Welcome page, click **Local Machine**, and then click **Next**.



3. Click Next until you reach the **Certificate Store** page, and then select **Automatically select the certificate store based on the type of certificate** option.



4. Complete the wizard.

Add the private key of the IIS user to the certificate

You must add the private key of the IIS user that runs the WzpSvc app pool, typically that is **IIS APPPOOL\WzpSvc**, to the Interact certificate. You do this in the **Certificate Manager** in the same way as for SmartPost. See Apply certificates to SmartPost .

Apply the certificate to the Interact service workflow

You register the Interact certificate in WorkZone Configurator.

1. In WorkZone Configurator, go to **Process** > **Service workflows**.
2. Select the a service workflow of the type **Interact connector**.

3. Enter the thumbprint of the certificate in the **CertificateThumbPrint** field.

See Service workflow in the WorkZone Configurator Installation Guide.

Case activities prerequisites

You can model case activities using DCR (Dynamic Condition Response) Design Portal. DCR Design Portal is a third-party tool.

> **Prerequisite:** In order to use the DCR Design Portal for production, your organization must own a license. You can buy DCR Design Portal licenses from DCR Solutions.

F2 integration

Automatic creation of the SJ-TEMP case type is required for the use of an F2 integration service workflow. For more information about F2 integration, see F2 integration in the WorkZone Process Administrator's Guide

Verify automatic creation setup for SJ-TEMP

1. Open WorkZone Configurator, and go to **Taxonomy**.
2. On the **Taxonomy** page, select the **Classification scheme** tab.
3. Double-click the **SJ-SYSTEM group** case group
4. Point to the **SJ-TEMP** case group, and click  **Edit**.
5. Verify that **Case Creation** is enabled.

Install and configure WorkZone

Before using WorkZone, you must install, activate, and configure each module your organization wants to utilize. The following section contains the installation procedures for all WorkZone modules.

Cross Origin Resource Sharing (CORS)

If WorkZone services are to be requested from web clients executed by a web browser and loaded from other domains (for example WorkZone Client and WorkZone Configurator being hosted on a different host than Process service), you must configure the Cross-Origin Resource Sharing parameters **AllowedCorsOrigins** and **AllowedCorsHeaders** for WorkZone PDF Engine, WorkZone Process and WorkZone OData.

General installation procedure

1. Install each WorkZone module to be used by your organization. All module features and functionality will be installed automatically when the module is installed.
2. WorkZone Content Server must be installed first on the server or servers intended to run WorkZone. The installation of WorkZone Content Server also includes steps where you can install the Oracle database that will contain WorkZone data for your organization.

   The following WorkZone Content Server modules are included in the installation WorkZone Configurator, WorkZone Configuration Management, WorkZone Explorer and CVR Integration/CPR Integration.
3. Once the WorkZone Content Server has been installed, you can install the WorkZone modules your organization wants to utilize, for example WorkZone PDF or WorkZone Process.
4. After the WorkZone modules are installed, you must activate and configure each specific module as you need it. Modules that have not been activated or configured correctly will not function or be available to your users.

You or any other system administrator can activate WorkZone modules and features in **WorkZone Configurator** > **Global** > **Feature settings** and can configure WorkZone modules and features in **WorkZone Configurator** and **WorkZone Configuration Management**.

> **Tip:** Install all WorkZone modules and features (for example WorkZone Client, WorkZone PDF, WorkZone Process) to ensure all modules are present and installed if they are needed at a later time.
> You can install, activate and configure any skipped WorkZone modules if your organization decides to utilize features from these modules at a later time. You can also deactivate any modules your organization no longer intends to utilize. Deactivating modules will not delete or remove existing data, but data will not be added or updated after they have been deactivated.

See Also

About Cross-Origin Resource Sharing

Feature settings in the WorkZone Configurator Administrator Guide.

About Cross-Origin Resource Sharing

Cross-Origin Resource Sharing (CORS) is a mechanism that enables web-browsers or other web-clients to safely request restricted resources from domains outside of the domain that the web page was loaded from.

Often, cross-domain requests are prevented unless the request originates from a requester on the same domain as the service resides (same-origin security policy). This is done to reduce threats from off-site attacks.

CORS defines a way to determine whether requests for these services, when made from a browser with a web page not loaded from the same domain as the server, can be authorized by the server. This authorization allows the cross-origin request to be performed or its data to be passed by the browser to the requesting party to be executed by the requesting browser. This combines the freedom and flexibility of accepting all cross-origin requests with the increased security of same-origin requests by defining which sites may successfully send requests and receive access to services.

WorkZone uses Cross-Origin Resource Sharing to enable web pages to access WorkZone services, such as WorkZone PDF Engine, WorkZone Process and WorkZone OData when these pages are loaded from different domains.

Configure CORS in WorkZone

If WorkZone services are to be requested from web pages with other origins (for example WorkZone Client and WorkZone Configurator applications hosted on a different host than Process service), you must configure the Cross-Origin Resource Sharing parameters **AllowedCorsOrigins** and **AllowedCorsHeaders** for WorkZone PDF Engine, WorkZone Process and WorkZone OData.

See Also

Install WorkZone PDF Engine

Command line configuration

Silent installation

Pre-installation checklists

Use the pre-installation checklists to ensure that all preliminary steps were completed.

WorkZone PDF pre-installation checklist

Complete the installation checklist below before installing WorkZone PDF. Completing the checklist prior to installation will help ensure a successful installation.

> **Note:** When you install your test and production environments, you will need to provide values for each environment. The values listed in this checklist are just examples. You must enter the values that apply to your system.

☐	To be verified	Comments and examples
☐	A client reference PC and a user is available for verification purposes.	The client reference PC is to be used for verification and troubleshooting purposes. In general, the installation and configuration process does not depend on the existence of a client reference PC.
☐	A service user is created with the "Log on as a service" rights	For more information about the service account user, see Service accounts > WorkZone PDF.

To be verified	Comments and examples
You know the service user credentials	**Example**: Service user credentials: - DOMAIN: lmdom.local - LOGIN: SomeServiceUserName - PASSWORD: 123
You know the database credentials	**Example**: Database credentials: - ODBC data source name: db01 - Database user name: sjsysadm - Database password: sjsysadm
You know the URL for WorkZone Content Server	**Example**: https://db01
The service user has access to OData.	**Example**: https://db01/OData
In a load-balanced environment, verify that the global Domain Name System (DNS) is mapped to the local host.	To verify, check the mappings of IP addresses to host names in the hosts file located under C:\Windows\System32\drivers\etc\hosts. **Example**: db01.lmdom.local > 127.0.0.1
Verify that the setup in the registry database allows loopbacks on all	To verify, open the Registry Editor, and add a multi-string named BackConnectionHostNames to 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_

	To be verified	Comments and examples
		0’. Then add the hostnames.
	web servers.	**Example**: host name db01.lmdom.local
☐	Ensure that Microsoft IIS role Application Initialization is enabled.	See Step by Step Instruction.
☐	Ensure that Microsoft Web Deploy 3.6 or later is installed.	To verify, look into **Programs and Features**. If it is not installed yet, you can install it from the Prerequisite software folder in the WorkZone installation package, or you can download from here.

WorkZone Process pre-installation checklist

Complete the installation checklist below before installing WorkZone Process. Completing the checklist prior to installation will help ensure a successful installation.

Note: When you install your test and production environments, you will need to provide values for each environment. The values listed in this checklist are just examples. You must enter the values that apply to your system.

☐	To be verified	Comments and examples
☐	A client reference PC and a domain user is available for verification purposes.	The client reference PC is to be used for verification and troubleshooting purposes. In general, the installation and configuration process does not depend on the existence of a client reference PC.
☐	A service user is created	For more information about the service account user, see Assign an exchange account to a service account.

	To be verified	Comments and examples
☐	You know the service user credentials	Service user credentials: - DOMAIN: lmdom.local - LOGIN: SomeServiceUserName - PASSWORD: 123
☐	You know the database credentials	Database credentials: - ODBC data source name: db01 - Database user name: sjsysadm - Database password: sjsysadm
☐	You know the URL for WorkZone Content Server	https://db01
☐	You know the URL for Exchange Web Services **Note:** Only applies to the on-premises Exchange server configuration.	https://dc1.lmdom.local/ews/exchange.asmx
☐	The service user is able to access Exchange Web Services **Note:** Only applies to the on-premises Exchange server configuration.	https://dc1.lmdom.local/ews/exchange.asmx
☐	Verify the email address of the user that you will use to access Exchange Online.	Go to login.microsoftonline.com and log in with this user.

	To be verified	Comments and examples
☐	Verify that the service user is an Active Directory user with a valid mailbox.	
☐	Optionally, in Active Directory, verify that the service user has the rights to send emails on behalf of another mail user.	Before the installation, you must consider if it will be necessary to send smart mails from WorkZone on behalf of a mail user different from the service user. You might want the sender of smart mails to appear with a name such as Mail agent rather than a name such as sjserviceagentuser4.
☐	Verify that the service user has the Logon as service privilege on the server(s) where you install WorkZone.	To verify, open **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignment**. Then right-click **Log On As Service**, and select **Properties**.
☐	The service user has access to OData.	https://db01/OData
☐	Verify that all agent servers have AgentCOM installed together with WorkZone Content Server.	To verify, identify agentCOM.exe under C:\Program Files (x86)\KMD\WorkZone\Program.
☐	Verify that the ports 1801, 2103, and 2105 are open from the web server to the agent server, if you run on separate web and agent servers.	See Install the notification agent on a separate server.

	To be verified	Comments and examples
	Make sure to open ports that can be used for the push and mail notification agents, if you run on separate web and agent servers. Default ports are 8080 and 8081.	
☐	From the WorkZone server, verify that WorkZone PDF is installed.	https://db01/Render should show a PDF index page.
☐	If WorkZone Mobile is to be installed, verify that the server that hosts the notification is allowed to communicate on port 2195 in the firewall.	
☐	In a load-balanced environment, verify that the global Domain Name System (DNS) is mapped to the local host.	To verify, check the mappings of IP addresses to host names in the hosts file located under C:\Windows\System32\drivers\etc\hosts. db01.lmdom.local > 127.0.0.1
☐	Verify that the setup in the registry database allows loopbacks on all web servers.	To verify, open the Registry Editor, and add a multi-string named BackConnectionHostNames to 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0'. Then add the hostnames. host name

	To be verified	Comments and examples
		db01.lmdom.local
☐	If the F2 Integration is used, automatic creation of the SJ-TEMP case type is required.	To verify, open WorkZone Configurator, and go to **Taxonomy** > **Classification scheme**. Verify that **Case Creation** is enabled for the **SJ-SYSTEM group** case group.
☐	If SmartPost is used, make sure that certificates are installed.	
☐	If the Interact integration is used, make sure that the interact certificate is installed.	

WorkZone Content Server

About installing WorkZone Content Server

WorkZone Content Server uses an installation program for automatic standard installation.

The installation program also includes installation of WorkZone Services.

The installation program installs the WorkZone Content Server together with the web system and scripts required for configuration of the WorkZone Content Server database.

Optionally verify successful download of files

After you have downloaded WorkZone Content Server and before you begin the installation process, you can use the MD5.xml file, located in the setup folder, to check that all files have been downloaded correctly. Use a third party tool, for example fciv, to verify that the checksum of the downloaded files is the same as the checksum listed in the MD5.xml file in the

installation package. If this is not the case, try to download the files again. Firewalls and anti-virus software can damage the files.

Database name

You must specify the ODBC DSN name of the database when installing WorkZone Content Server. This is also the name of the web site https://<database name>/<webservices>. You can specify additional database names during the installation to set up more systems at the same time.

Create an A host for WorkZone Content Server

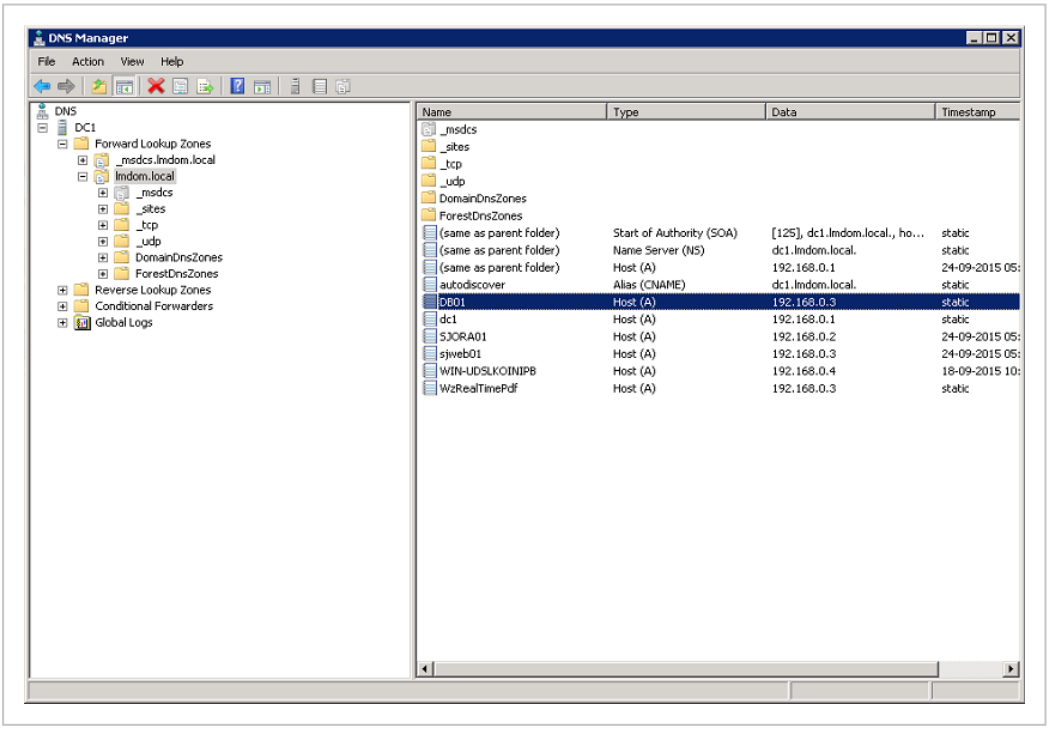
It is a prerequisite for the installation to create an A host name for WorkZone Content Server.

A host naming

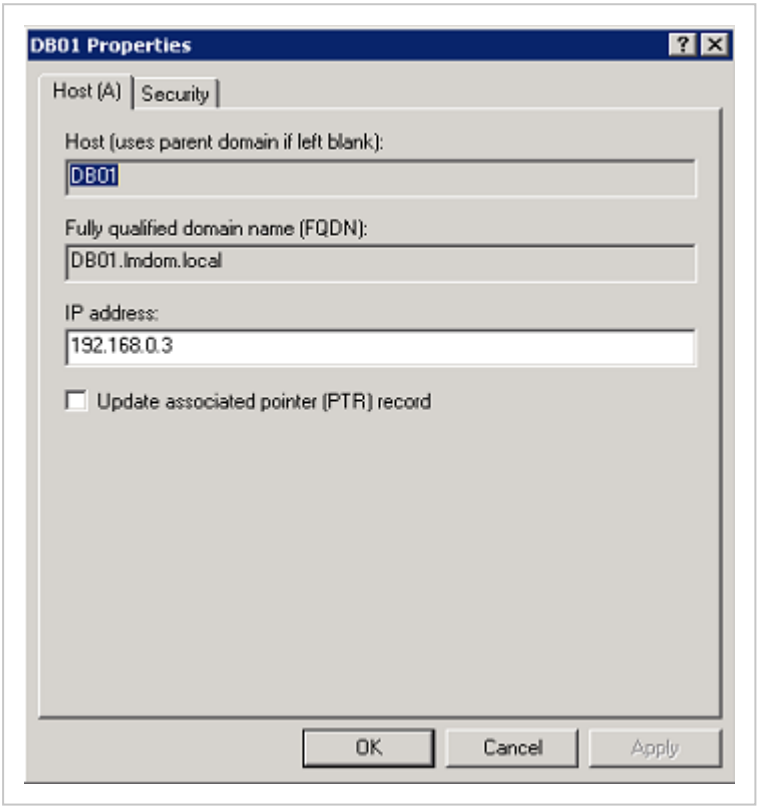
The A host name that you define must contain the ODBC data source name (DSN) as the first part of the A host name. For example, if you have a DSN called DB01 and your web server is called SJWEB01, you must define an A host name for SJWEB01 called DB01.

Create the A host

1. Log on to the Domain Name Server (DNS), open **DNS Manager**.



2. Expand **Forward Lookup Zones** and then right-click on a domain, in this example lmdom.local, and then select **New Host (A or AAAA)**.
3. Enter the name of the database in the **Name** field. The database name must be the same as the one you will select later during installation of WorkZone Content Server.
4. In the **IP address** field, enter the IP address of the web server.



Note: If you run NLB (Network Load Balancing), enter the IP address of the NLB.

Install WorkZone Content Server

This procedure describes how to install WorkZone Content Server.

- It is not possible to access clients or services directly from the web server. For information on how to enable access from the web server, see Microsoft article 896861.
- If you want to run WorkZone Explorer from Windows Explorer on a Windows Server operating system, you must enable the Windows **Desktop Experience**.

Install WorkZone Content Server

> **Prerequisite:** You must create an A host for the WorkZone Content Server before you start the installation, see Create an A host for WorkZone Content Server.

1. Start **setup.exe** and click **OK** to install the prerequisite packages. It may take a few minutes.

   If restart is required, click **OK** to restart.

   The **KMD WorkZone Content Server Installer Information** dialog closes and the **KMD WorkZone Content Server InstallShield Wizard** opens.

2. Click **Next** to display the **License Agreement** page. Read the license agreement and select the **I accept the terms in the license agreement** check box.
3. Click **Next** to open the **Custom Setup** page and select the program feature (Oracle client, Web server or Agent server) you want to install and clear the features you do not want to install.

   - Program features
     - **Oracle Client:** Installs the Oracle client in the path specified in the **Install To** field. The **Oracle ODBC driver** feature is installed by default.
     - **Web server:** Installs all common web services, Microsoft Office services and collaboration services required by WorkZone in the path specified in the **Install To** field.
     - **Agent server:** Installs all agents and services required by WorkZone not included Web server program features in the path specified in the **Install To** field.
   - Notes
     - The Microsoft.NET framework is installed as part of the WorkZone installation if it is not already installed on the server.
     - WorkZone Configuration Management, OData, WorkZone Configurator, and WorkZone Explorer are installed by default.

- The OAuth2 authentication framework (for WorkZone Mobile App user authentication) is automatically installed and activated during installation.

4. Click **Next** to open the **Authentication type** page and select the authentication type used by WorkZone to authenticate users.

   - **Windows:** Use Windows Domain authentication to verify and authenticate users in an on-premise installation. On -premise software is installed, maintained and run at the physical location of the organization and consists of the well-known Server-Client set up.
   - **OAuth2:** Use the OAuth2 framework for user verification and authentication. OAuth2 can be used for off-premise installations. Off-premise software is installed, maintained and run at a location other than the physical location of the organization, either in the cloud or at a service-provider.
     If you select **OAuth2**, you must configure the OAuth2 connection settings by defining the **Tenant ID**, **Client ID** and **Client Secret** in the following page of the wizard.

5. Click **Next** to open the **WorkZone Content Server Prerequisites Checker** page. The **WorkZone Content Server Prerequisites Checker** page displays the status of all components necessary for the correct installation WorkZone Content Server. When the **Status** field is green and **Passed**, click **Close**.
6. Click **Next** to display the **Database(s)** page and fill in the fields:

Database(s) to use with WorkZone Content Server

Enter the ODBC DSN name(s) of the database(s) to use with WorkZone Content Server. If you enter multiple names, they must be separated by semicolons.

- Only the characters a-z and A-Z are allowed in the database names.
- The only allowed special character is _ (underscore).
- Period is allowed.
- Numbers are allowed.

- Spaces, forward and backward slashes are not allowed.
- The length of the database name must not exceed 32 characters.

Add URL rewrite rule

If you upgrade from releases before the 2014 release of WorkZone Content Server, you can select the **Add URL rewrite rule** check box to ensure that existing URL paths are automatically redirected to the new paths used as from the 2014 release.

If you run https, you need to bind the Default Web Site in Internet Information Services (IIS) Manager.

> **Important:** URL rewrite requires that IIS URL Rewrite 2.0 is installed on the web server(s).

Stateless Connection Pool

Minimum Pool Size

The default value is 2. Accept the default value or enter the minimum pool size for web connections.

The minimum pool size specifies how many WorkZone Content Server sessions are kept alive when the system is idle.

Do not set this value to zero since the first session needs to load the configuration. Specifying a value greater than zero ensures that the configuration is kept in memory so that the first request after an idle period is served at once.

Do not specify a value too high or near the maximum pool size, as the pool will take up unnecessary resources.

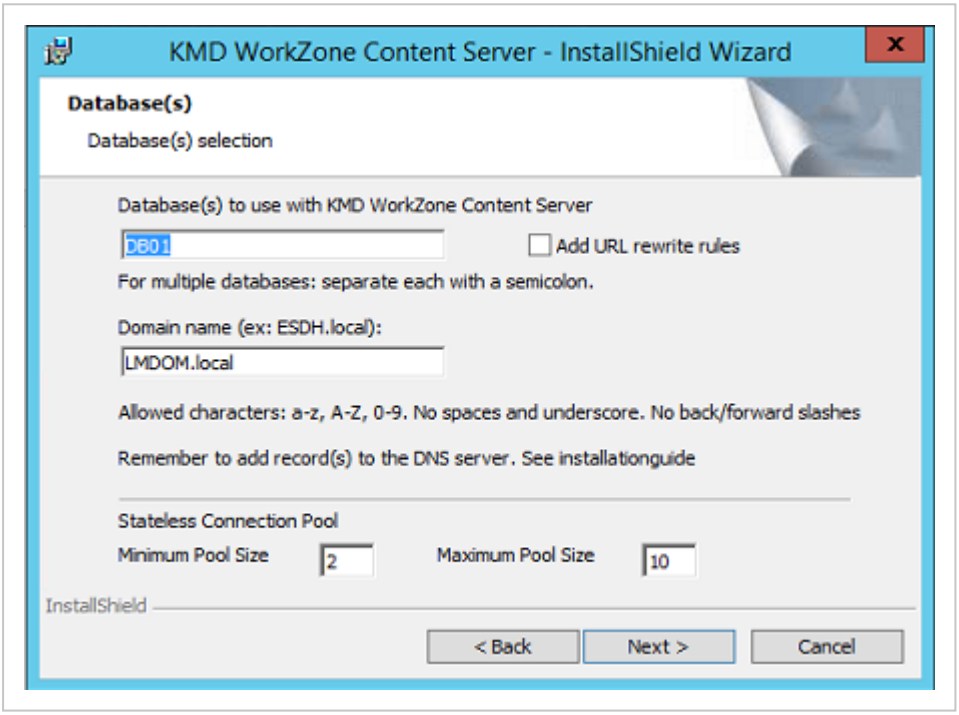
Maximum Pool Size

The default value is 10. Accept the default value or enter the maximum pool size for web connections.

The recommended maximum pool size depends on the number of system users, their type of work and the performance of the hardware, network and Oracle.

If the value is set too low, requests will be queued up and served when a pooled session is available, resulting in slow performance. Setting the value too high could result in the server running low on available RAM.

The configured component is activated in process, which means that every IIS worker process (application pool) will have its own runtime pool. Sessions are not shared between processes. You cannot configure the pool sizes independently for different processes, so the WorkZone Content Server application pool will share the same settings as the WebService pool, but they will not share the same sessions. For example, if you specify a minimum pool size of 2, every process will have 2 sessions available to them.



Click **Next** to display the **Ready to Install the Program** page and click **Install**. The **KMD WorkZone Content Server Installer Information** dialog is displayed and the installation will start.

When the installation is complete, the **InstallShield Wizard Completed** page is displayed.

Click **Finish** to close the **KMD WorkZone Content Server InstallShield Wizard**.You must restart your machine for the installation to take effect.

Upgrade WorkZone database following the instructions in the Content Server Database.

Silent installation

To install all WorkZone features with default settings, execute the following command:

```
msiexec /i "KMD WorkZone Content Server.msi" ADDLOCAL=ALL SJDSN-
N=<Database(s)> HOSTHEADER=<HostHeader>/q
```

Where:

- `<SJDSN>` is the name of the Oracle database(s). Separate each database with a semi-colon.
- `<HostHeader>` is the host header of the website.
- `ADDLOCAL=ALL` installs all features with default settings.

Example with all features installed, multiple databases and defined website host header.

```
msiexec /i "KMD WorkZone Content Server.msi" ADDLOCAL=ALL SJDSN-
N=”DB01;db02” HOSTHEADER=”lmdom.local” /q
```

Optional Parameters

- `CORSORIGINS` define which web client applications executed in a browser hosted on other domains will be able to perform CORS requests to the WorkZone Content Server, for example to access WorkZone OData.
  If the CORSORIGINS is not specified, the default value will be wild card (*). Note most browsers will prevent passing credentials or tokens to the service when the wild card (*) is used as the origin.
  Multiple origins must be separated by semi-colons (;)

CORSORIGINS example

```
msiexec /i "KMD WorkZone Content Server.msi" ADDLOCAL=ALL SJDSN-
N="DB01" HOSTHEADER="lmdom.local" CORSORIGINS-
S="https://db01;https://db02" /q
```

Installation process log file

If errors occur during the installation process, they are registered in the log file `WZCS.log`. The log file is placed in the user file folder `%temp%`.

> **Note:** When using RDP, the %temp% folder may be deleted at logoff.

See also

Install and set up URL Rewrite

The OAuth2 framework

The OAuth2 framework

OAuth2 has been introduced as an authorization framework for WorkZone Content Server. The OAuth2 framework is an open standard authorization framework that allows users to grant applications temporary and limited access to their user account information on other websites without distributing sensitive information such as passwords.

The OAuth2 framework delegates user authentication to the service that hosts the user account, and authorizes third-party applications to access the user account, with the most known usages by internet-based companies to enable users to share information with third party applications or websites.

OAuth2 and WorkZone

The OAuth2 framework can be used in WorkZone to improve security and facilitate delegation of authorization between the WorkZone Content Server and external components or systems such as mobile devices or WorkZone Client without exposing passwords or using "on-behalf-of" features.

The OAuth2 authentication framework is automatically installed and activated during WorkZone Content Server installation but the OAuth2 connection settings must be configured correctly before the framework can be utilized.

A system administrator can create, set up and maintain OAuth2 connections in WorkZone Configurator > **Global** > **OAuth2 settings**.

> **Note:** Performing case and document searches directly from File Explorer is not supported in a cloud setup as OAuth2 authentication is not supported by Windows Federated Search. See Supported Authentication Protocols (External link)

Examples of access to clients and services

The table below shows examples of how to access clients and services.

Client/Service	Address
WorkZone Client	https://<database name>/App/Client/
WorkZone Explorer	https://<database name>/Explorer
WorkZone Configuration Management installation	https://<database name>/Configuration manager/Client/
OData	https://<database name>/OData/
Office Services	https://<database name>/Office/

General errors

General errors in Microsoft Windows installation

If general errors occur in the Microsoft Windows Installation, check the following:

- Do you have the necessary privileges to make changes in the file system and in the Windows registry?
- A firewall or other security systems can block the installation process.
- Verify MD5.xml file. For more information, see About installing WorkZone Content Server.

Errors in the verification of certificates

When you install agents and web services, errors might occur during installation because you are dealing with.NET components. During the installation of the.NET components, the installation program will try to access the internet in order to verify the certificates.

This will cause issues if you install on a web server without connection to the internet. This is often the case if the server exclusively services an intranet.

You can solve this issue in two ways:

- Provide the server access to the internet.

- Follow the instructions provided in the Microsoft article **KB936707**.

  If you are dealing with, for instance, the XDI-gate, the program is named `Scanjour.Services.Service.exe`, and the config file must be named `Scanjour.Services.Service.exe.config`.

> **Prerequisite:** Always place the config file in the same folder as the exe file.

Configure WorkZone Content Server

After you have installed the WorkZone Content Server, you must

1. Install Oracle client drivers to be able to access the Oracle database.
   The Oracle Client driver is installed by default as part of the WorkZone installation but if you have deselected the feature during installation, you can find the installation files for the Oracle Client driver on the Oracle website.
2. Configure the ODBC connection to your Oracle database.
3. Install or upgrade the WorkZone Content Server database.
4. Set up user replication between WorkZone and Microsoft Active Directory.
5. Configure an agent to handle up to 6 different queues in order to be able to handle data sent to a certain agent in batch without interfering with the daily production data.

See also:

Install Oracle Client driver

Configure the ODBC

Install or upgrade the WorkZone Content Server database

AD replication

Working with multiple agent queues

Install Oracle Client driver

To access the Oracle database, the Oracle Client driver must be installed on the WorkZone. The Oracle Client driver is installed by default as part of the WorkZone installation but if you have deselected the feature during installation, you can find the installation files for the Oracle Client driver on the Oracle website.

1. Download:

   Oracle Database Client (12.1.01) for Microsoft Windows (32-bit).

2. Install according to the Oracle instructions.

   As a minimum, select the following product components:

   - SQL *Plus
   - Oracle Net
   - Oracle ODBC Driver

Configure the ODBC

This procedure describes how to configure the ODBC for a 32 or 64 bit environment.

> **Prerequisite:** Make sure that you have a working SQL Net connection to the database when configuring ODBC.

Configure the ODBC

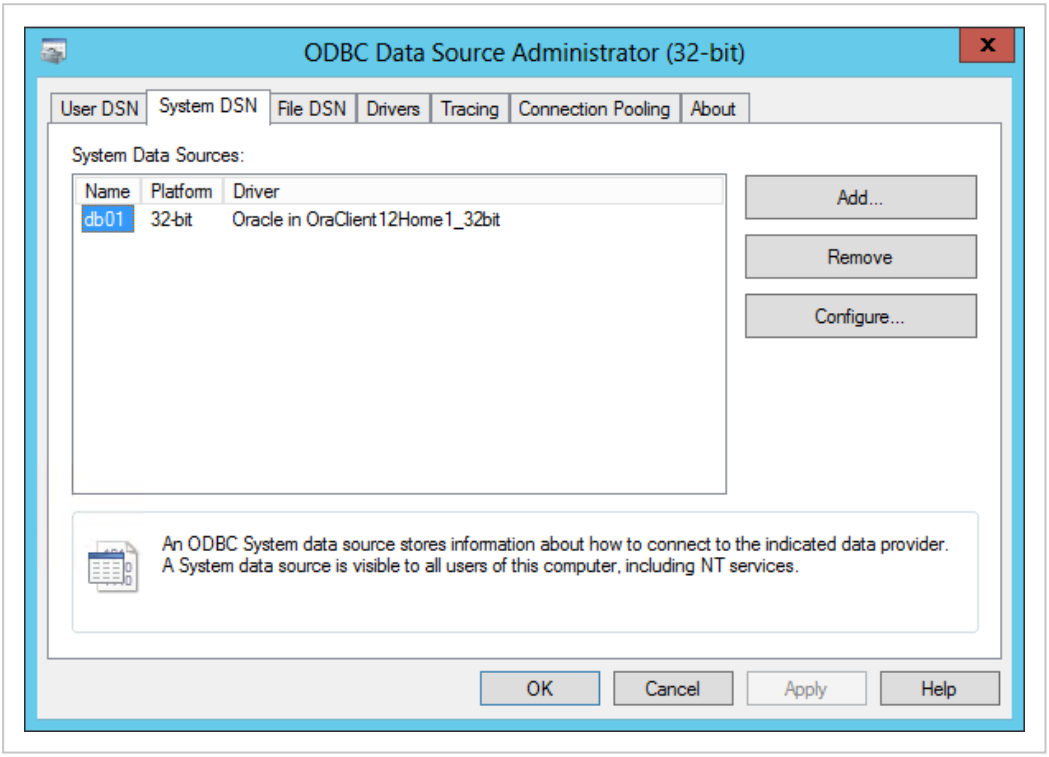
1. On a 64-bit environment:

   1. Open Windows Explorer.
   2. Open the folder **Windows** > **syswow64**.
   3. Double-click the `odbcad32.exe` file. The **ODBC Data Source Administrator window** opens.

   On a 32-bit environment:

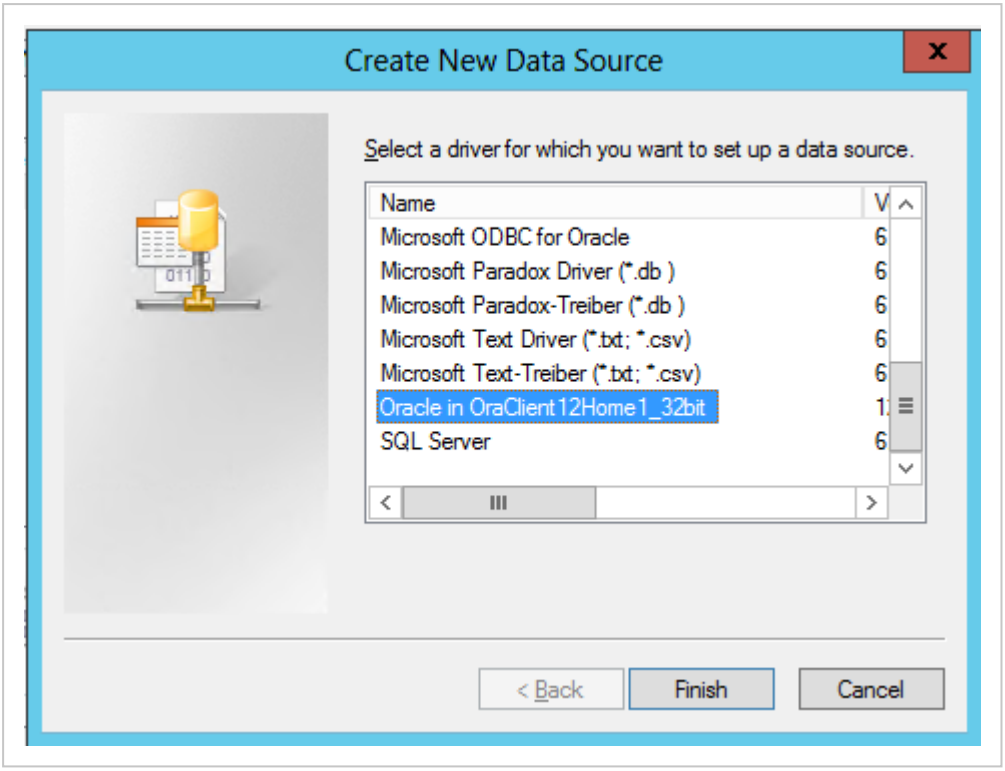
1. Select **Start** > **Settings** > **Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Data Sources (ODBC)**. The ODBC Data Source Administrator window opens.

2. Click the **System DSN** tab. The **System Data Sources** list appears.

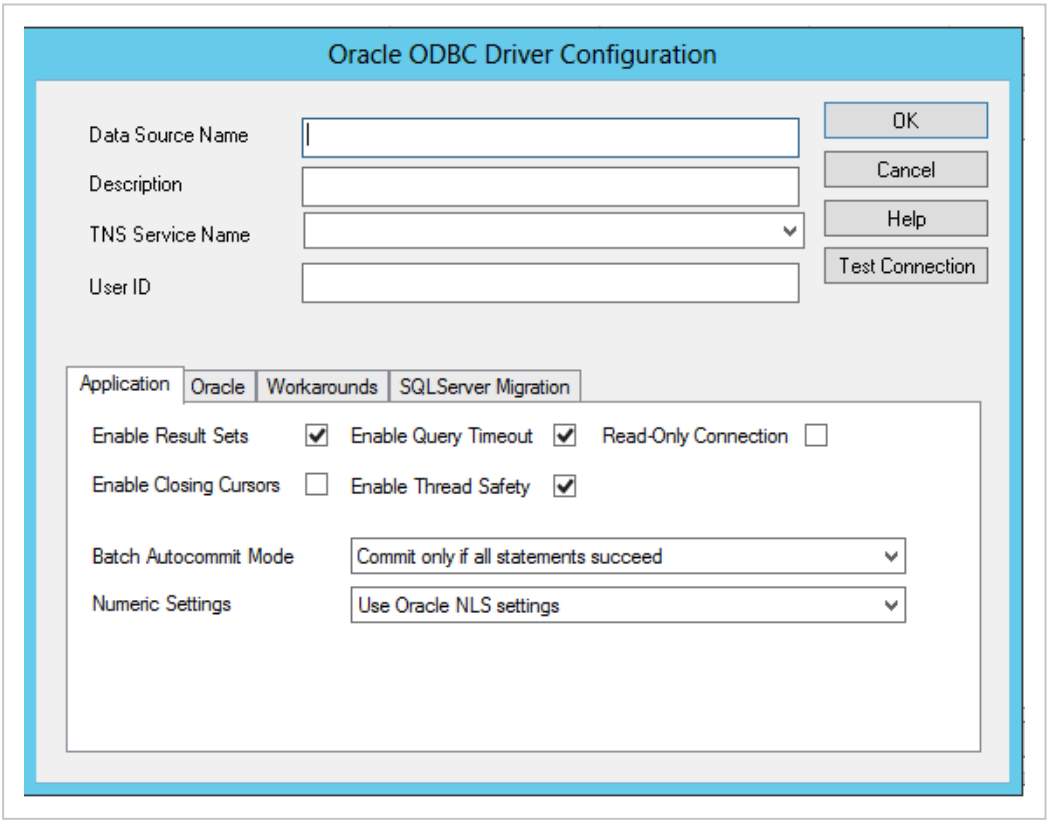


If a database already exists, you can skip the steps 4-9. If not, proceed with step 4.

3. Click **Add**.
4. In the **Create New Data Source window**, select the **Oracle in Ora11g** driver from the list.



5. Click **Finish**. The **Create New Data Source** window closes, and the **Oracle ODBC Driver Configuration** window appears.



6. Enter the name of the database in the **Data Source Name** field and the name of the TNS service in the **TNS Service Name** field.

   Optionally, enter a description, which identifies the database, in the **Description** field.

7. Click **OK** to close the window and return to the **ODBC Data Source Administrator** window.
8. Click **OK** to close the window. The configuration of the ODBC is complete.

Install or upgrade the WorkZone Content Server database

Now you must install or upgrade the WorkZone Content Server database.

For more information, see Content Server Database

AD replication

You must make an AD replication before you can start WorkZone Client.

For more information Active Directory

Working with multiple agent queues

FIX agent handles up to six queues

In WorkZone and subsequent versions, you can configure an agent, for example, the FIX agent, to handle up to 6 different queues.

The purpose of this feature is to handle data sent to a certain agent in batch without interfering with the daily production data. In this way, data sent in batch does not disturb ongoing production.

If, for example, a lot of addressees are automatically updated and created each night, free text indexing these addressees can be handled in another queue than the normal service_queue.

Parameters

To support this feature, the following parameters have been added to the procedure concerning installation of a service agent.

Parameter	Value	Description
/queue	1, 2, 3, 4 or 5	The queue that feeds the agent. If /queue is not used, the default service_queue is used.
/orderby	Valid orderby sql to service_queue, for example, "at_time"	Here you can change the way the records in the queue are selected. If you write the value "NULL", the records are not sorted. You should use "NULL" when dealing with batch updating/inserting handled by queue 1-5 because execution then is faster. If you do not enter any /orderby, default is "key".
/limitation	Valid where clause to service_queue, for example, "key > 3"	Here you can change which records in the queue are chosen. If you enter "NULL", all records belonging to the given agent type are selected. If you do not write /limitation, default is "at_time <= {fn now()}".

Install an agentFIX for handling data in batches

Example - how to install an agentFIX for handling data in batches

```
agentFIX /install /db=SJP /queue=1 /limitation=NULL /orderby=NULL
```

In this example, the FIX agent is installed to work with queue number one and there are no limitations or sorting involved in the selection of the records in the queue, which are sent on to be free text indexed.

How does data end in queue 1 to 5 for AgentFIX

Disabling triggers per session

The normal queue receives its data via triggers on different tables. If you, for example, update an addressee, a trigger on the name table will create a record in service_queue.

To prevent data from landing in the normal queue, you must disable these triggers per session. This is accomplished by means of the Oracle procedure sjp_fix.disable.

Correspondingly, the Oracle procedure named sjp_fix.enable will enable normal behavior.

Below is an example of a batch job called “Insert/update names 2009.01.01”, which inserts or updates a row of names that are to be handled in queue 1:

```
SQL> execute sjp_fix.disable
SQL> insert/update names
SQL> execute sjp_fix. Tilfritekst('CONTACT',<namekey>,'
'Insert/update names 2009.01.01',1);
SQL> commit;
SQL > exit
```

sjp_fix.Tilfritekst

Parameters for `sjp_fix.Tilfritekst`:

Parameter	Description
1	Tablename (CONTACT, ADDRESS, FILE, RECORD).
2	Internal key for the record in a given table. For example, for CONTACT the internal key is name_key in name.
3	Explanatory text, for example, which batch job has inserted the record.
Queue number	Null, 1, 2, 3 4 or 5.

Configure WorkZone Content Server service framework

The WorkZone Content Server service framework consists of NT services used for regular monitoring of a number of channels. For each channel, a number of plug-ins can be defined to make it possible for the channel to perform a given task – for instance, to monitor a folder to see when the new files are placed in the folder, or to monitor an e-mail account to see when the new e-mails are received. The number of plug-ins in a channel can be from 1 to 4.

> **Prerequisite:** WorkZone Configuration Management must be installed before you can start configuring the service framework. For more information on installing WorkZone Configuration Management, see the WorkZone Configuration Management Installation Guide.

Plug-ins

Each plug-in performs a well-defined task which can be used by different channels. A plug-in is a.NET class in an assembly. The following plug-ins exist:

- **Monitoring plug-in**
  This plug-in monitors incoming new items. The type of items depends on what is monitored (for example, an e-mail account, a folder, and so on).
- **Data plug-in**
  This plug-in provides data for the other plug-ins, and transforms the data so it can be used by the other plug-ins.
- **Metadata plug-in**
  This plug-in delivers metadata (in the correct format) based on the received input data.
- **Data transfer plug-in**
  This plug-in transfers data to the WorkZone Content Server database.

Channels

A channel only works if it is equipped with a monitoring plug-in. The other types of plug-ins are not always necessary to make the channel work. If a channel contains more plug-ins, the output from one plug-in is delivered as input to the next plug-in, and so on. The plug-ins defined for a channel are called by the NT service in the following order: monitoring plug-in, data plug-in, metadata plug-in, data transfer plug-in.

Predefined plug-ins

As a standard, WorkZone has a number of predefined plug-ins, which are automatically imported to WorkZone Configuration Management when it is installed. You can immediately configure and install the channels which are used in the predefined plug-ins.

See also:

- Import customer specific plug-in assemblies
- Install XDI service for WorkZone Content Server Imaging

- Install service for importing emails
- Install service for importing files without fesdPacket.xml file

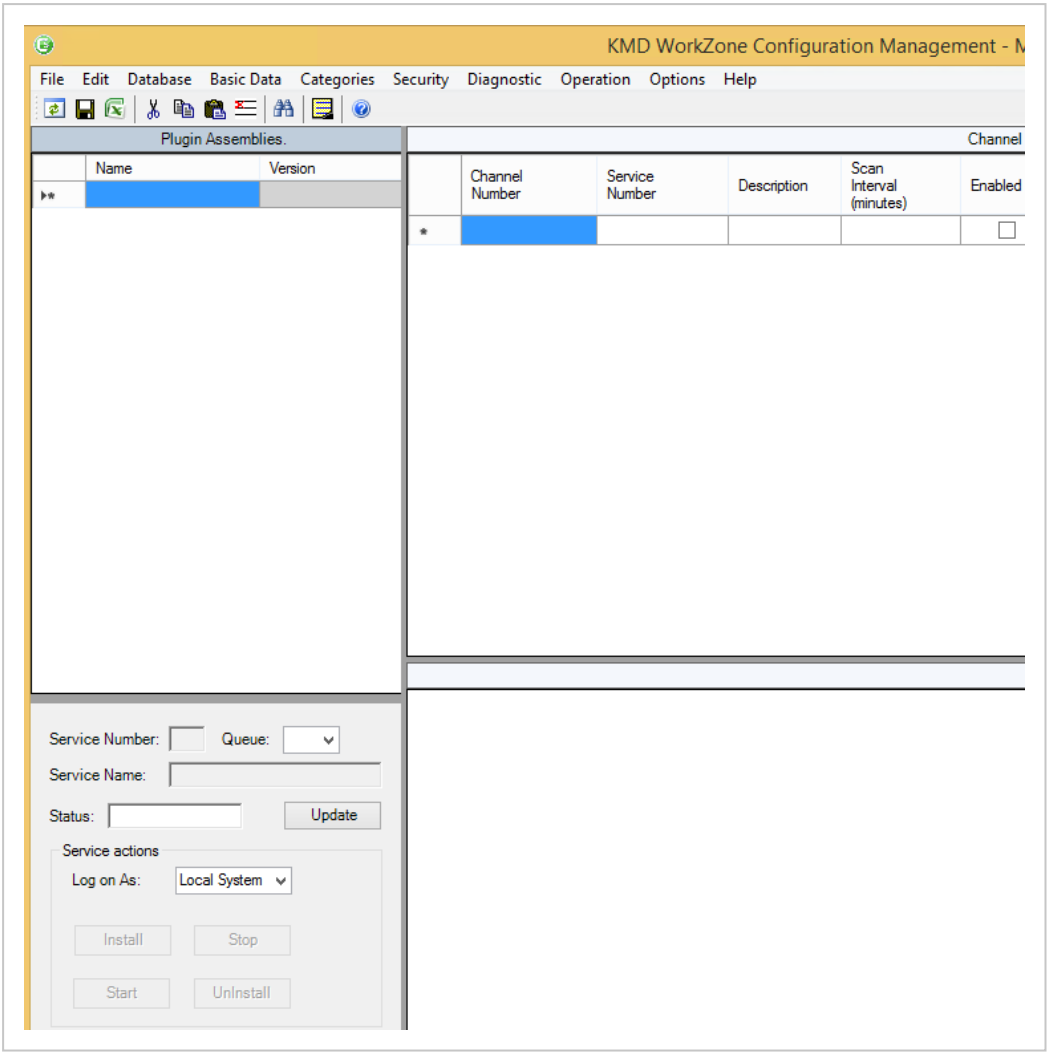
Import customer specific plug-in assemblies

This procedure describes how to import assemblies, which are made for a specific customer and not part of standard WorkZone Content Server). The import must take place on the computer, where WorkZone Content Server is installed.

The import of the customer specific plug-in assemblies is done in WorkZone Configuration Management. To use WorkZone Configuration Management, you must have access to WorkZone Content Server, and you must have the relevant access codes.

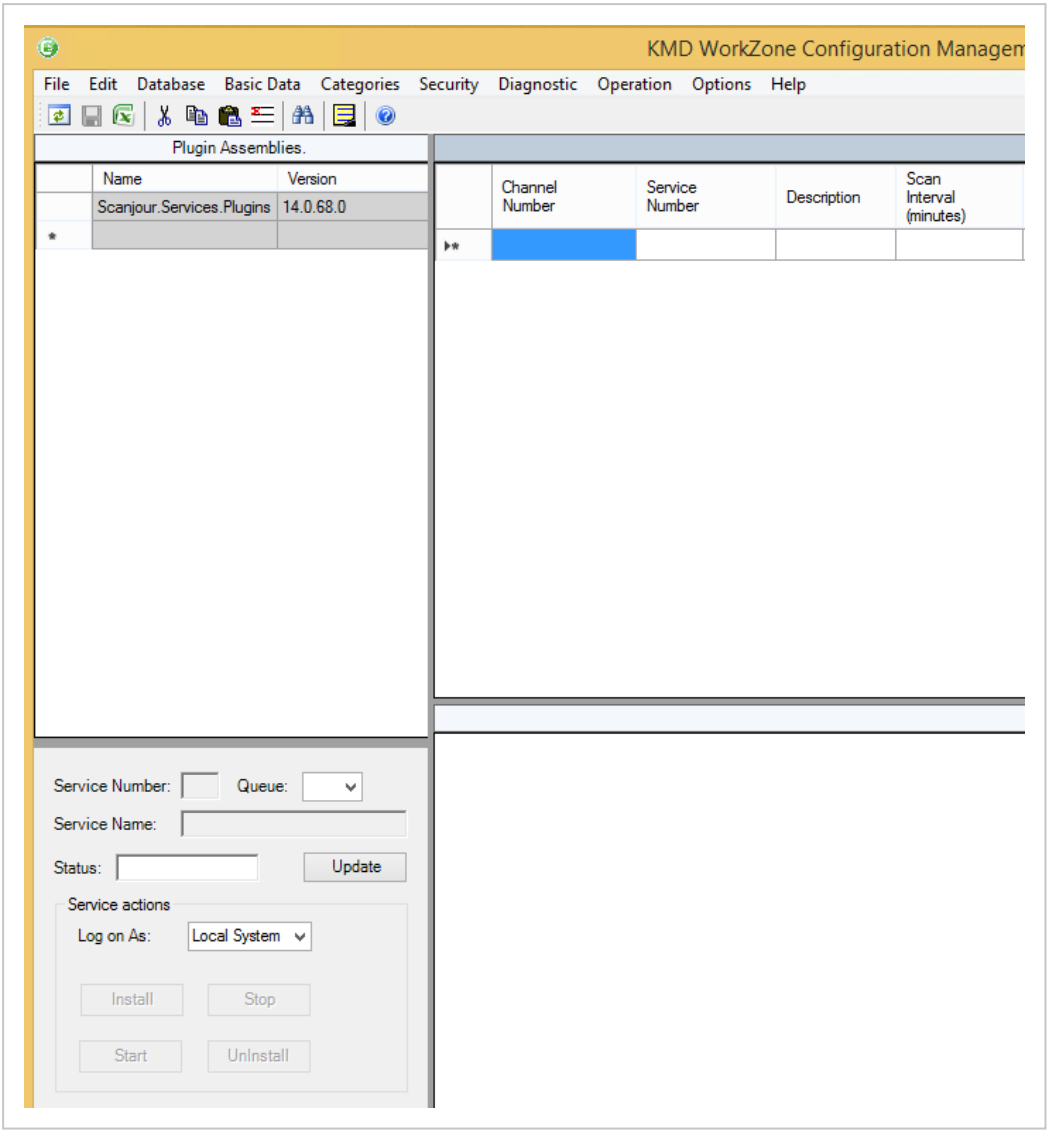
For more information, see Active Directory

1. Select **Start** > **Programs** > **KMD** > **WorkZone Configuration Management** to open WorkZone Configuration Management.
2. Select **Operation** > **Service Channels**. The WorkZone Configuration Management - **Modules: Service Channels** window opens.



3. Select **File** > **Import**.
4. In the **Open** dialog box, find the folder in which you have placed the customer specific plug-in assembly, and select the relevant plug-in assembly.

   The selected plug-in assembly is shown in the **File name** list.
5. Click **Open**. The **Open** window closes, and the imported plug-in assembly is shown in the **Plugin Assemblies** list in the WorkZone Configuration Management - **Modules: Service Channels** window.



6. Repeat steps 3 to 4 for each plug-in assembly that you want to import.
7. Click the **Refresh** button to reload the definitions of the imported plug-in assemblies. Now you can continue configuring and installing the channels which use the customer specific plug-ins.

Install service for importing emails

This procedure describes how you configure a channel and install a service for importing emails. The configuration and installation is done in WorkZone Configuration Management. To be able to use WorkZone Configuration Management, you must have access to WorkZone Content Server, and you must have the relevant access codes.

For more information, see Active Directory

1. Select **Start** > **Programs** > **KMD** > **WorkZone Configuration Management** to open WorkZone Configuration Management.
2. Select **Operation** > **Service Channels**. The **KMD** WorkZone Configuration Management - **Modules: Service Channels** window opens.
3. In an empty row in the **Channel definitions for WorkZone Services** list, do as follows:

    - In the **Channel Number** column, enter the value 4.
    - In the **Service Number** column, enter the value 3.
    - In the **Description** column, enter a description which you can use to identify the purpose of the channel.
    - In the **Scan Interval (minutes)** column, enter the value 5.
    - In the **Enabled** column, select the check box.
    - In the list in the **Watch Class** column, select the value `Scanjour.Services.MailPop3Watch`.
    - In the list in the **Data Provider Class** column, select the value `Scanjour.Services.MailDataProvider`.
    - In the list in the **MetaData Provider Class** column, select the value `Scanjour.Services.MailMetaDataProvider`.
    - In the list in the **Data Consumer Class** column, select the value `Scanjour.Services.XdiDataConsumer`.
    - In the **Error Path** column, enter the entire path to the folder, in which errors will be logged, for example, `C:\ServiceError\Channel 4`.
4. Click **Database** > **Save**.
5. In the **Channel definitions for WorkZone Services** list, click the row where channel 4 is defined. The row is selected, and information on the plug-in parameters is shown in **Plugin settings for channel 4**.
6. In Plugin settings for channel 4, do the following:

    - In the **MailPop3Watch – Mail server name** column, enter the name of the mail server, which is to be monitored by the channel.
    - In the **MailPop3Watch – Server port** column, enter the value 110.
    - **Port 110** is the default pop3 port.

- In the **MailPop3Watch – *User name** column, enter the user name of the email account, which must be monitored. The user name must be entered in the format `<user name>@<domain name>`
- In the **MailPop3Watch – *User password** column, enter the password of the email account
  * The name of the column depends on the language chosen as current language.
- In the **MailPop3Watch – Mail folder** column, enter the path to the folder, in which extracted emails must be placed, for example: `C:\ServerMail`
- In the **MailDataProvider – Mail** folder column, enter the path to the folder, in which emails must be unwrapped, for example: `C\ServerMail\Mail`
- In the **MailMetaDataProvider – MetaData XML template** column, enter the path and file name of the xml-template. By default the path and file-name is `C:\Program Files\KMD\WorkZone\Program\XDIData\sjFesdPacket.xml`
- In the **MailMetaDataProvider – Responsible Unit** column, enter the name of the organizational unit, which is responsible for the imported email.
- Optional: In the **MailMetaDataProvider – Document type** column, enter the document type, which the imported email will have in WorkZone Content Server database.
- Optional: In the **MailMetaDataProvider – Document group** column, enter the document group, to which the imported email will belong inWorkZone Content Server database.
- In the **MailMetaDataProvider – Access code** column, enter the access code, which will be attached to the imported email.
- In the **XdiDataConsumer - Schema directory** column, enter the path to the xml schemas. By default the XML schemas are located in the folder `C:\Program Files\KMD\WorkZone\Program\XdiData`.

7. Click **Database** > **Save**.
8. In the **Channel definitions for WorkZone Services** list, click the row where channel 4 is defined. The row is selected, and the **Service Id** and **Service Name** fields in the left part of the window are filled in.

9. In the **Log on As** list, select **Local System**. The communication with SOM now will be handled through the user sjserviceagentuser.
10. Click **Install**. When the installation is complete, the **Install log** window appears informing whether the installation has been successful.
11. Click **OK**. The **Install log** window closes. Now the monitoring of the configured channel must be initiated. For more information, see Start and Stop the Services in the WorkZone Content Server Service Framework.

Install service for importing files without fesdPacket.xml file

This procedure describes how you configure a channel and install a service for importing files without an enclosed fesdPacket.xml file. The configuration and installation is done in the WorkZone Configuration Managementt. To be able to use the WorkZone Configuration Management, you must have access to WorkZone Content Server, and you must have the relevant access codes.

For more information, see Active Directory

1. Log on to the computer on which the service for importing files will run.
2. Select **Start** > **Programs** > **KMD** > **WorkZone Configuration Management** to open WorkZone Configuration Management.
3. Select **Operation** > **Service Channels**. The WorkZone Configuration Management - **Modules: Service Channels** window opens.
4. In an empty row in the **Channel definitions for WorkZone Services** list, do the following:
    - In the **Channel Number** column, enter the value 5.
    - In the **Service Number** column, enter the value 4.
    - In the **Description** column, enter a description, which you can use to identify the purpose of the channel.
    - In the **Scan Interval (minutes)** column, enter the value 5.
    - In the **Enabled** column, select the check box. In the list in the **Watch Class** column, select the value `Scanjour.Services.DirectoryWatch`.

- In the list in the **MetaData Provider Class** column, select the value `Scanjour.Services.FileMetaDataProvider`.
- In the list in the **Data Consumer Class** column, select the value `Scanjour.Services.XdiDataConsumer`.
- In the **Error Path** column, enter the entire path to the folder, in which errors will be logged, for instance, `C:\ServiceError\Channel 5`.

5. Click **Database** > **Save**.
6. In the **Channel definitions for WorkZone Services** list, click the row where channel 5 is defined. The row is selected, and information on the plug-in parameters is shown in **Plugin settings for channel 5**.
7. In **Plugin settings for channel 5**, do the following:

   - In the **DirectoryWatch - Watch directory** column, enter the path to the folder, which is to be monitored by the channel, for example: `C:\FileImport`.
   - In the **DirectoryWatch - The directory wildcard** column, enter the name of the folder, in which the imported files will be placed, for example: `*.imp`.
   - In the **FileMetaDataProvider - Metadata XML template** column, enter the path and filename of the xml-template. By default the path and filename is `C:\Program Files\KMD\WorkZone\Program\XDIData\sjFesdPacket.xml`.
   - In the list in the **FileMetaDataProvider - Origin** column, select the origin of the file.
   - In the **FileMetaDataProvider - Responsible Unit column**, enter the name of the organizational unit, which is responsible for the imported file
   - Optional: In the **FileMetaDataProvider - Document type** column, enter the document type which the imported file must have in the WorkZone database.
   - Optional: In the **FileMetaDataProvider - Document group** column, enter the document group, which the imported file must belong to in the WorkZone database.
   - In the **FileMetaDataProvider - Access code** column, enter the access code which will be attached to the imported file.

- In the **XdiDataConsumer - Schema directory** column, enter the path to the xml schemas. By default the XML schemas are placed in the folder `C:\Program Files\KMD\WorkZone\Program\XdiData`.

8. Click **Database** > **Save**.
9. In the **Channel definitions for WorkZone Services** list, click the row where channel 5 is defined. The row is selected, and the **Service Id** and **Service Name** fields in the left part of the window are filled in.
10. In the **Log on As** list, select **Local System**. The communication with SOM now will be handled through the user sjserviceagentuser.
11. Click **Install**. When the installation is complete, the **Install log** window appears, informing whether the installation has been successful.
12. Click **OK**. The **Install log** window closes. Now the monitoring of the configured channel must be initiated. For more information, see section Start and Stop the Services in the WorkZone Content Server Service Framework.

Install XDI service for WorkZone Content Server Imaging

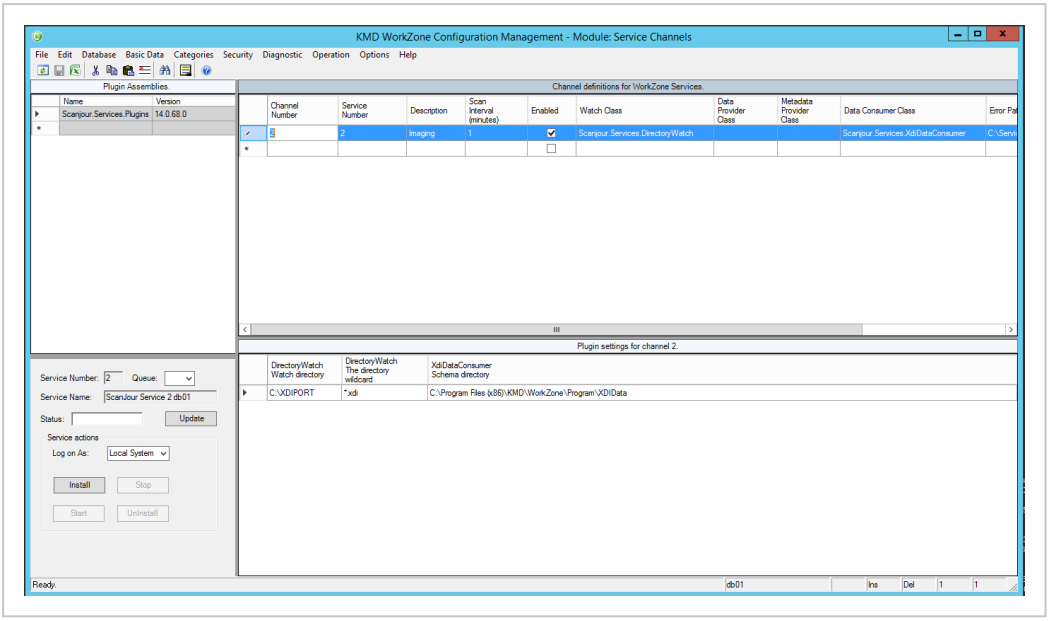
This procedure describes how you configure a channel and install a service for monitoring and fetching files with scanned documents from WorkZone Content Server Imaging. The configuration and installation is done in WorkZone Configuration Management, see the WorkZone Configuration Management online help.

Prerequisite:

- To use the WorkZone Configuration Management, you must have access to WorkZone, and you must have the relevant access codes. For more information, see the Active Directory.
- You must open WorkZone Configuration Management as a system administrator to be able to install the XDI service.
- The XDI service uses WorkZone Content Server for saving documents. Therefore WorkZone Content Server must be installed on the computer where you install the XDI service.

Install the XDI service

1. Log on to the computer on which the service for monitoring and fetching files with scanned documents from WorkZone Content Server Imaging will run.
2. Select **Start** > **Programs** > **KMD** and then right-click on **WorkZone Configuration Management** and select **Run as administrator** to open WorkZone Configuration Management.
3. Select **Operation** > **Service Channels**. The WorkZone Configuration Management - **Modules: Service Channels** window opens.
4. In an empty row in the **Channel definitions for WorkZone Content Server Services** list, do the following:
    - In the **Channel Number** column, enter the value 2.
    - In the **Service Number** column, enter the value 2.
    - In the **Description** column, enter a description which you can use to identify the purpose of the channel.
    - In the **Scan Interval (minutes)** column, enter the value 1.
    - In the **Enabled** column, select the check box to enable.
    - In the list in the **Watch Class** column, select the value `Scanjour.Services.DirectoryWatch`.
    - In the list in the **Data Consumer** column, select the value `Scanjour.Services.XdiDataConsumer`.
    - In the **Error Path** column, enter the entire path to the folder, in which errors must be logged, for example, `C:\ServiceError\Channel 2`.
5. Click **Database** > **Save**.



6. In the **Channel definitions for WorkZone Services** list, click the row where channel 2 is defined. The row is selected, and information on the plug-in parameters is shown in **Plugin settings for channel 2**.
7. In **Plugin settings for channel 2**, do the following:
    - In the **DirectoryWatch - Watch directory** column, enter the path to the folder, in which the service will fetch the files from WorkZone Content Server Imaging, for instance, `C:\XDIPORT`.
    - In the **DirectoryWatch - The directory wildcard** column, enter `*.xdi`.
    - In the **XdiDataConsumer - Schema directory** column, enter the path to the xml schemas. By default the XML schemas are located in the folder `C:\Program Files\KMD\WorkZone\Program\XdiData`.
8. Click **Database** > **Save**.
9. In the **Channel definitions for WorkZone Content Server Services** list, click the row where channel 2 is defined. The row is selected, and the **Service Id** and **Service Name** fields in the left part of the window are filled in.
10. In the **Log on As** list, select **Local System**. The communication with SOM now will be handled through the **sjserviceagentuser** user.
11. Click **Install**. When the installation is complete, the **Install log** window appears informing whether the installation has been successful.

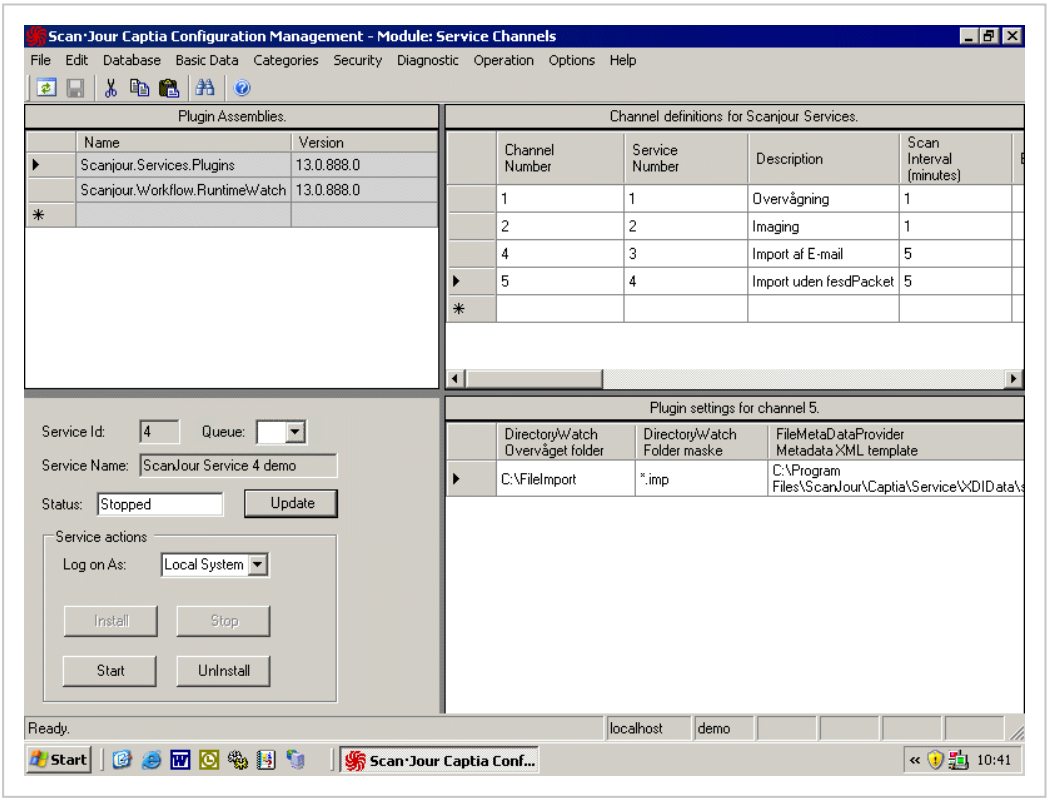
12. Click **OK**. The **Install log** window closes. Now the monitoring of the configured channel must be initiated. For more information, see Start and stop WorkZone Content Server services in service framework.

Start and stop services in WorkZone service framework

The procedure below describes how you start and stop the services which are monitoring channels. This is done in WorkZone Configuration Management. To be able to use WorkZone Configuration Management, you must have access to WorkZone Content Server, and you must have the relevant access codes.

For more information, see Active Directory

1. Log on to the computer on which the **KMD Service Framework** runs.
2. Select **Start** > **Programs** > **KMD** > **WorkZone Configuration Management** to open WorkZone Configuration Management.
3. Select **Operation** > **Service Channels**. The WorkZone Configuration Management - **Modules: Service Channels** window opens.



4. In the **Channel definitions for WorkZone Content Server Services** list, click the row where the relevant channel is defined.

   The row is selected, and the information on the selected channel is shown. For example, you can read the **Status** field to see whether monitoring of the channel is running or has stopped.

5. Perform step 6 to start the monitoring and step 7 to stop the monitoring.
6. Click **Start** to start the monitoring, if the value in the **Status** field is Stopped.

   Click **Update** in the **Status** field to update the value. This way you can check that the monitoring starts (the value in the **Status** field changes to Running).
7. Click **Stop** to stop the monitoring, if the value in the **Status** field is Running.

   Click **Update** in the **Status** field to update the value. This way you can check that the monitoring stops (the value in the **Status** field changes to Stopped).

Start and stop the services from the Control Panel

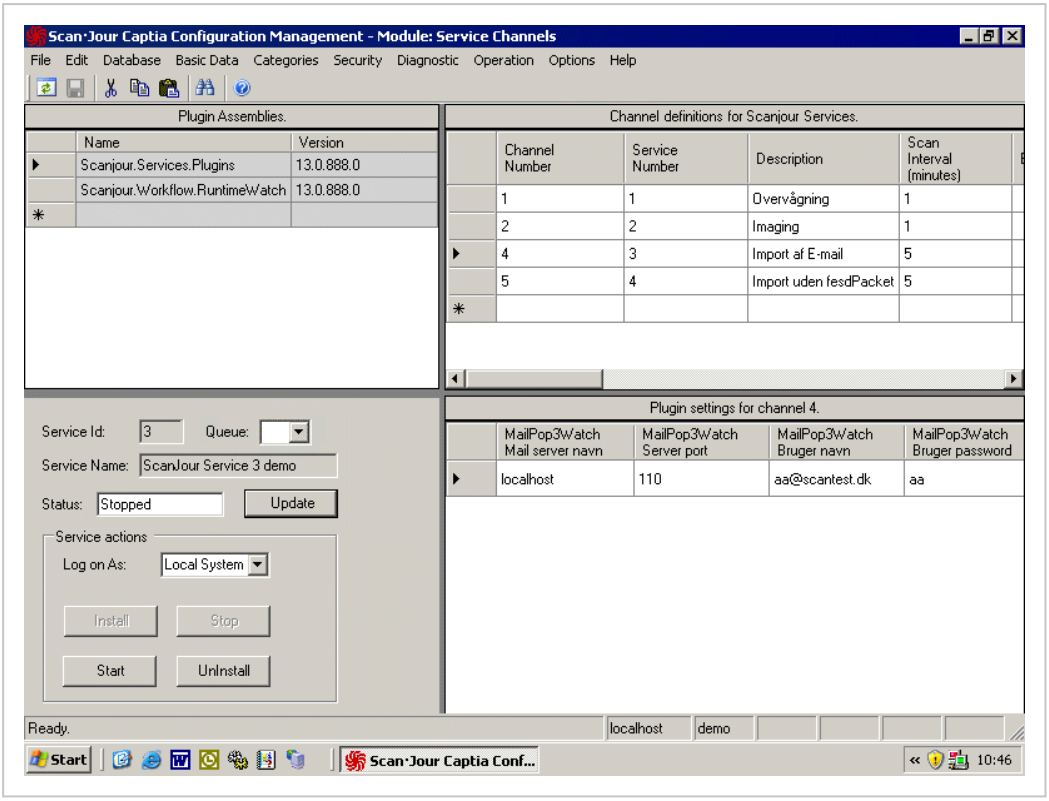
Because WorkZone Content Server Service Framework is implemented as NT services, you can also start and stop the services from the **Control Panel** > **Administrative Tools** > **Services** window.

Uninstall services in the WorkZone Content Server service framework

The procedure below describes how you uninstall the services in the WorkZone Content Server Service Framework. This is done in WorkZone Configuration Management. To be able to use WorkZone Configuration Management, you must have access to WorkZone Content Server, and you must have the relevant access codes.

For more information, see Active Directory

1. Log on to the computer on which the service for importing files runs.
2. Select **Start** > **Programs** > **KMD** > **WorkZone Configuration Management** to open WorkZone Configuration Management.
3. Select **Operation** > **Service Channels**. The WorkZone Configuration Management - **Modules: Service Channels** window opens.



4. In the **Channel definitions for WorkZone Content Server Services** list, click the row where the relevant channel is defined.

   The row is selected, and the information on the selected channel is shown. For example, you can read the **Status** field to see whether monitoring of the channel is running or has stopped.

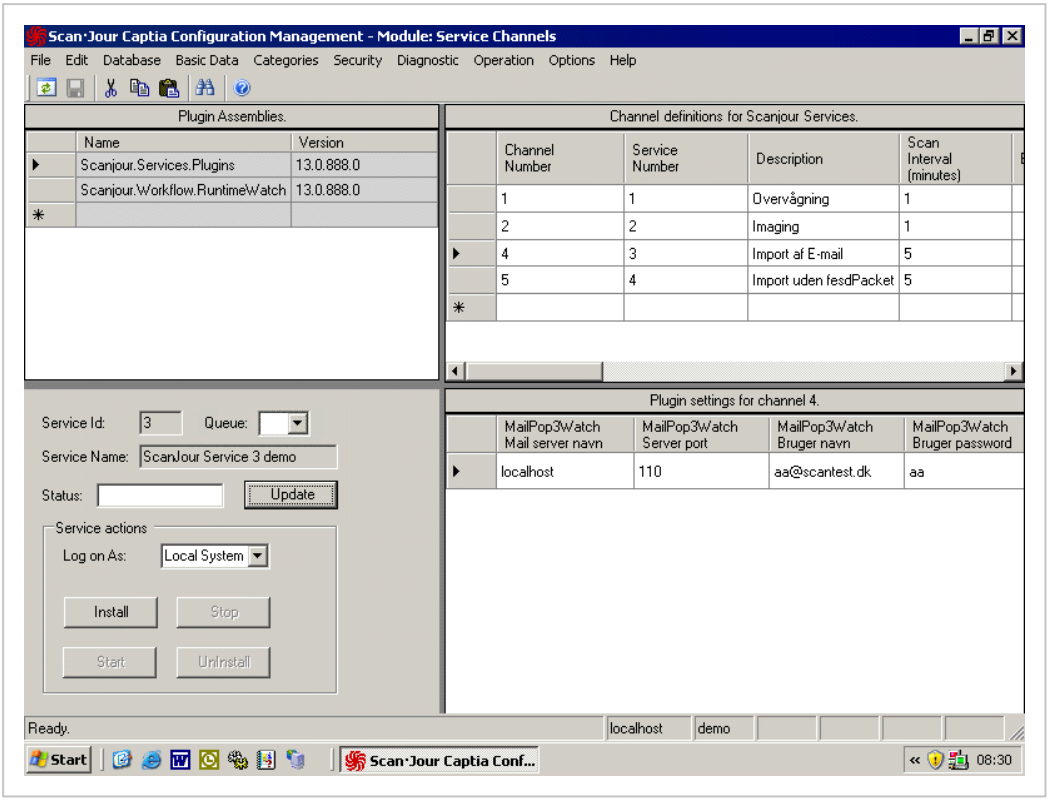
5. In the **Service actions** group box, click **Stop**.

   In the **Status** field, the state changes to **Stopped**.

6. Click **Uninstall**.

   When the uninstallation is complete, the **Uninstall log** window appears, informing whether the uninstallation has been successful.

7. Click **OK** to close the **Uninstall log**.



Configure Office Service to run https

If WorkZone is set up to run HTTPS (Secure Server), you need to configure Office Service to run with HTTPS. This is done by using a web.config file that includes the HTTPS configurations.

WorkZone is installed with two versions of the web.config file:

- `Web.config` - HTTP configurations
- `Web.config.https` - HTTPS configurations

By default WorkZone runs HTTP and uses the web.config file. To configure Office Service to run with HTTPS, rename the `web.config.https` file to `web.config`.

The location of the web.config files is:

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

See also:

- Certificates
- How To Set Up an HTTPS Service in IIS (External link to Microsoft technical documentation)

Install and set up URL Rewrite

If you are operating on a WorkZone installation that contains HTTP references after having converted the installation to run in an HTTPS environment, you can install and configure the URL Rewrite extension to the Microsoft Internet Information Server (IIS).

The URL Rewrite extension enables you to replace the HTTP protocol part of a URL with its HTTPS equivalents – for example changing SmartTask references in WorkZone Client still containing HTTP to their HTTPS equivalents without having to locate and update all links and references.

The URL Rewrite detects the URL request containing the HTTP request and rewrites the URL, replacing the HTTP protocol part of the URL with HTTPS before it is processed by the WorkZone server.

This is a bit different than a URL redirect operation as a URL redirect operation sends information back to the client requesting an incorrect URL (or at least the URL which is to be redirected). The information enables the client to then request the correct URL and display the results. A redirect is a client-side request that redirects the web browser to access another predefined URL.

A URL rewrite is processed on the server and “rewrites” or updates the requested URL to another predefined URL. The requesting client does not receive any information regarding the new URL from the server. The only indication that the new URL is used is the new URL displayed in the address bar. A URL rewrite is a server-side edit of a URL before it is processed by the IIS.

Note:

- Disable URL rewriting of requests generated through the WZ Client, Internet Proxy, the firewall and the Net Load Balancer.

- Clear the cache of the client machine's web browser to remove any URL Rewrite rules from the cache.

Download and install the URL Rewrite extension

The URL Rewrite extension is not installed by default on IIS servers and must be downloaded and installed separately.

Download and run the **rewrite_amd64_en-US.msi** installer from the Microsoft homepage to install the URL Rewrite extension.

To check if the URL Rewrite extension has been correctly installed, open the **Internet Information Services (IIS) Manager** form for the WorkZone site. The **URL Rewrite** extension is displayed in the **IIS** section on the information (right) pane for the WorkZone site.

If the **Internet Information Services (IIS) Manager** form was open during the installation, the URL Rewrite extension may not be displayed as the form needs to be updated.

Close and reload the form to display the **URL Rewrite** extension for the WorkZone site. In some cases, you may have to reboot the IIS server for the changes to take effect.

Set up URL Rewrite

After the **URL Rewrite** extension is installed, you must clear the **Require SSL** check box to accept HTTP calls for the WorkZone site.

In the **Internet Information Services (IIS) Manager** form, WorkZone site, click **SSL Settings** in the **IIS** section on the information (right) pane for the WorkZone site and clear the **Require SSL** check box.

If the **Require SSL** check box is selected, any URL requests containing HTTP will be rejected before the **URL Rewrite** extension can access the HTTP request to rewrite the request.

Create, edit, enable and disable URL Rewrite rules

Once you have correctly set up the URL Rewrite settings, you can create new URL rewrite rules.

> **Tip:** Remember to create a backup copy of the web.config file before creating new URL rewrite rules through the IIS Manager.

In the **Internet Information Services (IIS) Manager** form, WorkZone site, double-click **URL Rewrite** in the **IIS** section on the information (right) pane for the WorkZone site to open the **URL Rewrite** panel.

In the **URL Rewrite** pane, you can add new URL rewrite rules, edit existing rules, enable and disable rules as well as test the URL rewrite rules.

Each rule must be created manually. You cannot import or export rules in the **URL Rewrite** pane.

The IIS settings are stored in the web.config file for the selected site. If you need to mass-create or mass-update URL rewrite rules, you can edit the web.config file instead, copy-pasting the relevant lines to and from web.config files.

All URL rewrite rules in the web-config file are displayed in the **URL Rewrite** panel.

Use the Web.config file to create URL rewrite rules

You can use the web.config file on the IIS server to manually create and edit URL rewrite rules. The web.config file is an XML-based configuration file used by IIS to manage various settings used to configure a website hosted on IIS. The web.config file can be edited in any text-editor and in this way you can control a website's configuration without editing the server's configuration.

The default path to the web.config file is C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone.

> **Tip:** Remember to create a backup copy of the web.config file before manually editing the file.

To create URL rewrite rules in a web-config file, you must add the following rules:

```
<rule name="httpsRedirect" enabled="true" stopProcessing="true">
    <match url="(.*)" />
    <conditions>
        <add input="{HTTPS}" pattern="^OFF$" />
```

```
        </conditions>
        <action type="Redirect" url="https://{HTTP_HOST}{REQUEST_
    URI}" appendQueryString="false" redirectType="Temporary" />
    </rule>
    <rule name="assetRootRedirect" enabled="true" stopPro-
    cessing="true">
        <match url="(.*)" />
        <conditions trackAllCaptures="true">
            <add input="{HTTPS}" pattern="^ON$" />
            <add input="{QUERY_STRING}" pattern="^(.*)as-
    setRoot=http://(.*)$" />
            <add input="{QUERY_STRING}" pat-
    tern="^.*assetRoot=https://.*$" negate="true" />
        </conditions>
        <action type="Redirect" url="https://{HTTP_HOST}{URL}?
    {C:1}assetRoot=https://{C:2}" appendQueryString="false" redir-
    ectType="Temporary" />
    </rule>
```

The `httpsRedirect` rule rewrites the first part of the URL to HTTPS while the `assetRootRedirect` rewrites the internal HTTP URL. For example for WorkZone SmartMail which employs an imbedded URL in the URL.

See also:

URL Rewrite (External link to IIS.net)

The Microsoft Office Online Server

The Microsoft Office Online Server is a server-based application that can be installed locally on a company's servers and made available for users on the company network only. This enables users to utilize the browser-based web service programs for Word, Excel, Powerpoint and OneNote internally instead of using the internet-based versions. Using the Office Online Server, an organization can reduce the number of locally installed office installations as users can create, read, edit and save their documents online through the company's local intranet.

The Office Online Server also enables users to concurrently edit a document and all users can see what each other is adding to the document as it happens.

Simply put, the Office Online Server allows multiple users access to Office Online products concurrently without exposing their network to the external internet.

The browser-based web-service programs are basic versions compared to the fully-featured locally installed Microsoft Office programs, but sufficient features and functionality to satisfy most users working on typical day-to-day tasks. For example, Word Online does not have the References and Mailings features compared to the Word program in the Office 365 Suite.

The Office Online Server also contains a free version which allows uses to view the documents but not make changes to them. If users want to create, edit and save the documents, a full license is required.

The Office Online Server replaces the Office Web Apps Server 2013 and be integrated with Microsoft Exchange 2016, Microsoft SharePoint Server 2016 and Microsoft Skype for Business 2015. If you intend to integrate Office Online Server with Microsoft Skype for Business 2015, the Office Online Server must be installed on a single or multiple server farm using HTTPS. Microsoft Skype for Business 2015 is not compatible with an Office Online Server installed on a single server farm using HTTP.

Office Online Server also can be integrated with Microsoft SharePoint Server 2013, Lync server 2013 with Office Web Apps Server 2013 installed and in some situations with Microsoft Exchange Server 2013.

Tip:

- Assume Office Online Server hardware requirements are identical to MS SharePoint Server 2016
- Do not install on web servers or servers that contain applications that use ports 80, 443 or 809
- Do not install any Office applications on the Office Online Server
- The Office Online Server should be installed on its own dedicate server instances. Do not run the Office Online Server on servers that are also performing the following functions:

    - Domain control
    - Exchange server
    - SharePoint Server
    - Skype for Business server
- The Office Online Server supports Internet Explorer 11 as well as the latest versions of Firefox, Google Chrome, Microsoft Edge and Safari OS x (10.8 or later).

Important: While WorkZone supports Internet Explorer 11, Microsoft Edge and Google Chrome, Firefox and Safari are not officially supported. Using these unsupported browsers may result in unexpected results, inconsistencies and potential errors.

Installing Office Online Server

You must first install the Office Online Server and then configure WorkZone to integrate with the Office Online Server.

Prerequisite: The Office Online Server must be installed on its own dedicated server.

Installation information

For information on how to install Office Online Server, see the installation instructions found online here: Install an Office Online server (external link):

Installation tips

- **Set up the server:** After you have installed the Office Online Server, you must set up your server farm. The Office Online Server installation does not create a running server on the machine.

- **Disable automatic Windows updates:** On the Office Online Server machine, disable automatic Windows Updates. Some updates may conflict with your existing set up and require additional configuration after an update.
  You should test any updates on a separate environment first in order to determine if there are any consequences that need mitigating before an update is applied to your live production environment.

Common errors

Be aware of these potential errors that can occur during Office Online Server installation or setup.

Office Online Server URL address

The URL address to the Office Online Server defined in WorkZone Configurator > **Office** > **Office Online Server** > **Office Online Server URL** field, is used by WorkZone Content Serverto interact with Office Online Server. The address must therefore be able to access the Office Online Server internally on the network. This address can an IP address, the FQDN or even the hostname.

-InternalURL must be FQDN

The **-InternalURL** setting contains the address provided when the Office Online Server farm is created and is used from the client machine. The **-InternalURL** setting must be FQDN in order to prevent name resolution issues.

Internal / external server URLs

Even though Office Online Server supports distinguishing between internal and external server URLs (correspondingly for intranet and extranet usage), WorkZone Content Server does not. Only internal server URLs should be used.

Configure Office Online Server

After you have installed the Office Online Server, you must configure your WorkZone installation to integrate with the Office Online Server.

To configure WorkZone for Office Online Server integration

> **Prerequisite:** You must be assigned the CONFIGADM access code in order to configure the Office Online Server settings.

1. Open the WorkZone Configuratorand select **Office** > **Office Online Server** to open the **Office Online Server** tab
2. In the **Office Online Server** tab
    1. Select the **Allow usage of Office Online Server** toggle key to enable integration with the Office Online Server.
    2. In the **Office Online Server URL** field, enter the internal URL to the Office Online Server.

- The Microsoft Office Online Server
- Installing Office Online Server
- Test the Office Online Server connection
- Common Office Online Server integration errors

Test the Office Online Server connection

You can test if the specified address points to a valid Office Online Server by opening the <OOS_Server_URL>/hosting/discovery page where <OOS_Server_URL> is the URL specified in the **Office Online Server URL** field

When the discovery page is opened in Internet Explorer, an XML file will be opened containing multiple XML tags.

Locate the **urlsrc** attributes in the XML and investigate if the urlsrc attributes all point to the same Office Online Server URL. These urls are used when WZC interacts with the Office Online Server. The Office Online Server URL address defined in the WorkZone Configurator is used by WorkZone Content Server to obtain the Office Online Server discovery XML information.

Common Office Online Server integration errors

Be aware of these potential errors that might occur during configuration or installation of the Office Online Server.

Incorrect Office Online Server URL address in the Office Online Server URL field

If the Office Online Server URL address in the **Office Online Server URL** field is incorrect, <oos_server_url>/hosting/discovery XML will be unavailable and WorkZone Clientwill not be able to access the Office Online Server.

Invalid -Internal URL setting

If the Office Online Server was originally set up with an invalid -InternalURL setting, the <oos_server_url>/hosting/discovery XML will be available but WorkZone Client will not be able to access the Office Online Server.

Testing integration from WorkZone Client to the Office Online Server

You can test the integration from WorkZone Clientto the Office Online Server by previewing and editing all three main Office Online file types (Word, Excel and PowerPoint) from WorkZone Client.

Installing reports

This section describes how to install reports.

Prerequisites

WorkZone includes a number of standard reports that must be installed manually. In addition to this, special reports can be developed for specific customers.

Before you install the standard reports, you need to:

- Install and configure WorkZone.
- Make sure that no reports are installed beforehand. If you install reports on already existing reports, they will not work. In this case you need to remove all reports and install them again, see Uninstall standard reports.

- Create SYSADM as a contact in Active Directory with the name type M (employee). The user SYSADM is not allowed to have an NT account as this can cause issues in connection with the logon with Reportupload.
- Edit the web.config file for the WorkZone/App application. The default location of the web.config file is:

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

.

Locate the setting with `name="CrystalRenderSite"` and specify the address of the default web site.

Example:

<setting name="CrystalRenderSite" serializeAs="String">

<value>https://sjweb01.lmdom.local</value>

</setting>

Note: If you run Net-Load Balancing, you must make this change to the `web.config` file on all servers in order for the servers to point to the same Chrystal Report server.

Install standard reports

The components of a report

Each report consists of three files with the same file name, but with different file types:

- Binary file containing the design definition: `<file name>.rpt`.
- XML file containing the data definitions for the data extract: `<file name>.sjr.xml`.
- ini-file containing the display- and register information for the report: `<file name>.ini`.

This construction is used both for the standard reports and for any customer specific reports.

Location of reports and installation program

The installation program `Reportupload.exe` and all the reports are located in the folder:

`\Extra\Standard_rapporter`

Install standard reports

This procedure describes how you install the standard reports on the WorkZone server.

1. Copy the **standard_rapporter** catalog from the **Extra** folder to the WorkZone install directory.

   Copy any custom reports to the folder above.
2. Start `Reportupload.exe`. A logon window is displayed.
3. Log on as user **SJSYSADM** and enter the name of the database.

   The report files of types `.rpt and.sjr.xml` are inserted as documents in the archive database. The documents are inserted with the record type `RAPDEF` and the record contact `SYSADM`, and with the title and register information as given in the corresponding ini-file for each report.

   Check that the path to the reports is correct

   All files from the folder are automatically inserted as documents in the archive database, if named ini-files exist for the files. As a result, if the files have been inserted beforehand, they will now occur twice.
4. Click **OK**. The reports are now installed.

Access codes

Documents with the record type `RAPDEF` must not be provided with access codes, neither on the main, nor on the appendix documents. This also applies to access codes to which the user has access.

Troubleshooting reports

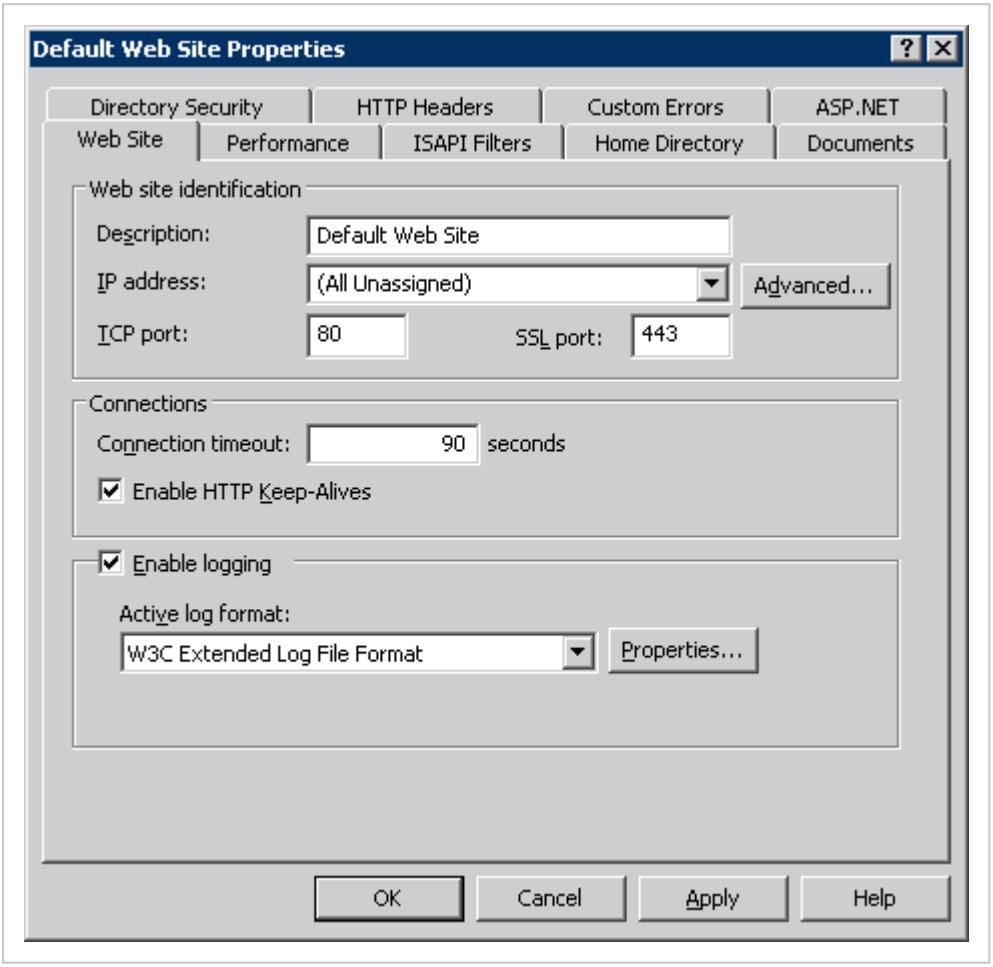
Click an issue below to see the solution or workaround.

Reports with calculations

Some reports containing calculations cannot be generated without showing an error message, if there is no data to be calculated.

Script timed out

The error messages **Script timed** out are by default activated after 90 seconds.



You can change this time period for the Internet Information Server:

1. Right-click **.../Web Sites/Default Web Site and select Properties** > **Web Site**.
2. In the **Connection timeout** field, change the timeout value.

Note: Statistical calculations can require a large amount of time, sometimes many hours.

File size

IIS can only upload files limited to 4 MB. It can be increased by adding the following line to `web.config` in Crystal directory :

```
    <httpRuntime maxRequestLength="32768" />
```

Note: You must perform an **iisreset** after changing the file `web.config`.

Missing write permissions to the Data folder

If the error message “access to path …\Data\..XML…is denied.” is displayed, the possible reason is that the user does not have write permissions to the **Data** folder of **sjCrystalRender**. You can change the setting in the following way:

1. Find the **Data** folder on the server.
2. Open the context menu and select **Properties**.
3. Click the **Security** tab.
4. Find or add the user **<local machine>\Network Service**.
5. Set **Modify** and **Write** permissions for this user..

Missing icons

If the icons are missing in the display window of reports, the possible reason is that the crystalreportviewer site has been deleted, for instance, because of a re-installation of IIS.

During re-installation of WorkZone, the crystalreport viewer site will be re-established.

Missing display of reports

If the reports are not displayed, check whether **SYSADM** is a contact on all records of type RAPDEF, and add it if it is not already a contact.

"ShowReport error: The underlying connection was closed: An unexpected error occurred on a send"

If you run https and try to open a report, you may get the error message:

"ShowReport error: The underlying connection was closed: An unexpected error occurred on a send"

and you cannot open the report. You solve this issue by inserting:

```
<serverRuntime uploadReadAheadSize="2147483647" />
```

into the applicationHost.config file, which is located here:

```
C:\Windows\System32\inetsrv\config\applicationHost.config
```

.

Example:

```
<location path="Default Web Site/SJCrystalRender">
  <system.webServer>
      <serverRuntime uploadReadAheadSize="2147483647" />
```

Uninstall standard reports

If you need to remove all reports to prepare for a re-installation, you can issue an update command from an SQL prompt.

Remove all reports

You can remove all existing reports at the same time:

```
UPDATE record set record_type='XXX' where record_type='RAPDEF'
```

When this command has been executed, you can make a re-installation from the **Reports** folder.

Remove one report

You can also remove one report at a time:

```
UPDATE record set record_type='XXX' WHERE record_type='RAPDEF'
and title='<report title>';
```

Change WorkZone Content Server

This procedure describes how you add and/or remove modules in a WorkZone Content Server installation.

1. Select **Start** > **Control Panel**.
2. Double-click **Programs and Features**.
3. In the **Programs and Features** window, select WorkZone Content Server in the **Currently installed programs** list.
4. Click **Change** and then click **OK**. The WorkZone Content Server installation wizard starts.[1]
5. Click **Next**.
6. On the **Program Maintenance** page, click **Modify** and then click **Next**.
7. The **Custom Setup** page is displayed.
8. The procedure of changing the installation is identical to the actual installation procedure. To change the installation, follow the instructions from step 3 in Install WorkZone Content Server.

[1]If you run WorkZone Content Server on Windows Server 2012 R2, you will get the message: "This setup requires elevated rights." This means that you need to run `setup.exe` as administrator to start the WorkZone Content Server installation wizard with elevated rights.

File locations

This section describes the location of WorkZone Content Server files.

Location of WorkZone Content Server files

By default the installation program places the files in the locations listed in the table below. You need to select the default values when install the system.

Description	Location on 64 bit server
Program files and ini files of WorkZone Content Server.	`C:\Program Files(x86)\KMD\WorkZone\Program`

Description	Location on 64 bit server
fedpacket.xml, sjFesdPacket.xml and web.config files only	`C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\APP\Captia`
Data dictionary. Data dictionary is created not during the installation, but when you log on for the first time. In connection with the first log on, SOM moves Data dictionary from the WorkZone Content Server database to this folder.	`C:\ProgramData\ScanJour\DataDict\<database name>`
Documentation.	The WorkZone Content Server documentation is located on KMD WorkZone Documentation.

Permissions on the Data folder

When you install WorkZone Content Server on a Windows 2008 (R2) server, the user `<local machine>\Network Service` must have **Modify** and **Write** permissions.

Troubleshooting

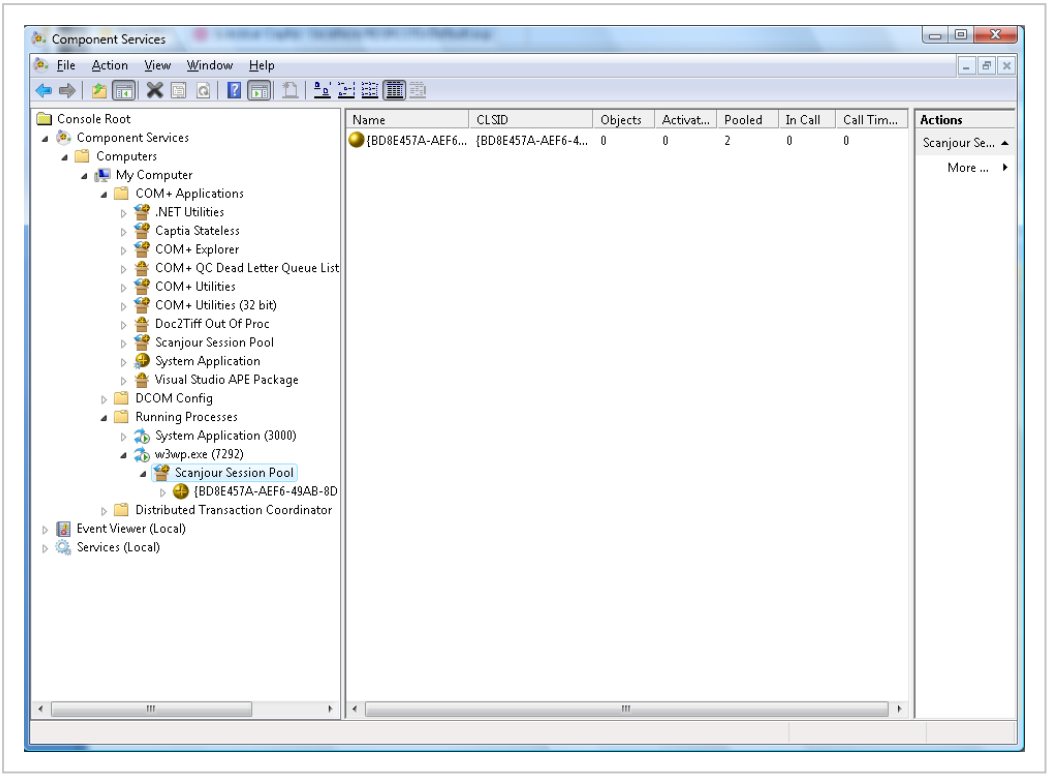
Click an issue below to see the solution or workaround.

Maximum pool size is too low

To find out if the maximum pool size is configured too low, you can monitor the actual pool sizes from the Component Services snap in.

1. Navigate to **Running Processes**.
2. Find the W3Wp process of interest and expand it.
3. Click the **Scanjour.SessionPool** package.
4. Switch to details view by clicking the details icon on the tool bar. A window like the

one below is displayed.



The number in the **Pooled** column indicates the number of objects in the pool for that process.

The number in the **Activated** column specifies how many of these are currently handling requests from users.

If the number of objects activated (the **Activated** column and the **Pooled** column) at any given time is equal to the maximum pool size, it could make sense to increase the maximum pool size (if the web server has enough RAM to accommodate this).

The **Call Time** column specifies how much time the current activated objects have spent processing their requests. Large values in that column is often due to complex searches or large amounts of data (up/downloading of large documents or large search results (for example crystal reports)) that Oracle is currently handling.

Stability issues and the IIS worker processes

IIS reset or application pool/worker process recycle

> **Note:** This description is based on a 64-bit Windows Server 2008 R2.

Depending on which version of IIS you are running, the following might differ slightly.

The Session Pool is hosted in the IIS worker process. Performing IIS reset or performing an application pool/worker process recycle will destroy the pool and all sessions contained within it.

How to solve stability issues

> **Important:** Do not perform the IIS resets on a regular basis to solve stability issues. The IIS worker process model has automatic configurable recycling build into it to handle stability issues.

Recycling the worker processes (application pools) shut down and start up is done in a more controlled manner than the brutal IIS reset. Recycling the worker processes allows currently handled request to finish before the process is terminated. The user will not experience errors during application pool recycling, but they will experience errors during an IIS reset if they had a request handled by the server.

Oracle error when running scansql

If you get the following error when running scansql:

ORA-12154: TNS: could not resolve the identifier specified

It means that there is an error in the SQL Net connection to the database. Check your `tnsnames.ora` file.

Content Server Database

About the database

This section describes tablespaces in WorkZone and the character set that can be used.

Tablespaces in WorkZone Content Server

Character sets in WorkZone Content Server database

Using Oracle proxy users

Tablespaces in WorkZone Content Server

Physical and logical tablespaces

A WorkZone Content Server database consists of a number of logical tablespaces. The logical tablespaces must be mapped to one or more physical tablespaces.

If you want to use the database for test purposes, you only need a few physical tablespaces, but if you want to use it for production including a large amount of data, it is recommended that each logical tablespace is mapped to its own physical tablespace.

To use different configurations of the logical tablespaces, depending on the type of data to be saved in the tablespaces, a number of logical tablespaces are used. This makes it possible to optimize Oracle resources.

As a minimum you must create one physical tablespace.

Logical tablespaces in the WorkZone Content Server database

The table shows the logical tablespaces in the WorkZone Content Server database.

Logical name	Physical default name	Description
TS_STAM_DATA	SJ_STAM_DATA	Used for tables with a few rows, that is, metadata such as postal codes, countries, classification scheme and help registers.
TS_DATA	SJ_DATA	Used for tables with many rows, such as cases and documents, that is, data produced every day.
TS_STAM_INDEX	SJ_STAM_INDEX	Used for indexes with a few rows and thus for indexes on tables in the logical tablespace TS_STAM_DATA.
TS_INDEX	SJ_INDEX	Used for indexes with many rows and thus for indexes on tables in the logical tablespace TS_DATA.
TS_DATA_LOB	SJ_DATA_LOB	Used for ”LOB” segments, especially for the free text table register_text ”LOB”. ”LOB” stands for

Logical name	Physical default name	Description
		”Large objects”. In the free text table all cases, documents, contacts, addresses and tasks are saved as XML in an ”LOB”, and this ”LOB” is free text indexed via Oracles Intermedia Text.
TS_DATA_IMT	SJ_DATA_IMT	Used for Oracle free text index for the WorkZone free text table register_text.
TS_IMPMGR	SJ_IMPMGR	Used for saving data from an external source in the format of the source, for instance data from the CPR register. If you do not use external sources, or if you only need to use very few data from external sources, you can use the logical tablespace TS_DATA instead of using this one.
TS_ARKIV	SJ_ARKIV_CAPTIA	Used for the tables for the archive. The archive is the place where all documents are saved. The documents are saved in binary format and possibly in text format, for instance, if a TIFF document has been OCR processed.
TS_ARKIV_LOB	SJ_ARKIV_CAPTIA_LOB	Used for the ”BLOB” segment of the archive, that is, the document itself.
TS_LOG	SJ_LOG	Used by the use log.
TS_DEBUG	SJ_DEBUG	Used for debug purposes.

All tablespaces must be handled locally and they must be configured to Uniform Size.

Create a tablespace

To create a tablespace, execute the following SQL command:

```
CREATE TABLESPACE “SJ_STAM_DATA” LOGGING DATAFILE

'[SJ_BASE]\oradata\[ORACLE_SID]\sj_stam_data01.dbf' SIZE [TS_
SIZE] AUTOEXTEND ON NEXT [NEXT_SIZE] MAXSIZE UNLIMITED EXTENT
MANAGEMENT LOCAL UNIFORM SIZE [UNI_SIZE];
```

Recommended sizes of tablespaces

The following table shows the recommended sizes of the tablespaces.

> **Note:** The TS_SIZE column only lists a minimum value. The actual size that to use depends on the amount of data that must be saved in the database. It is not required to use autoextend.

Tablespace	Ts_size (minimum)	Next-size	Uni_size
SJ_STAM_DATA	40 MB	10 MB	128 KB
SJ_DATA	300 MB	50 MB	1 MB
SJ_STAM_INDEX	40 MB	10 MB	64 KB
SJ_INDEX	300 MB	50 MB	256 KB
SJ_DATA_LOB	100 MB	50 MB	4 MB
SJ_DATA_IMT	100 MB	10 MB	128 KB
SJ_IMPMGR	50 MB	10 MB	1 MB
SJ_ARKIV_CAPTIA	50 MB	10 MB	128 KB
SJ_ARKIV_CAPTIA_LOB	100 MB	50 MB	4 MB
SJ_LOG	100 MB	10 MB	4 MB
SJ_DEBUG	100 MB	10 MB	1 MB

Character sets in WorkZone Content Server database

WorkZone Content Server is executed under Microsoft Windows, which usually uses the Windows-1252 character set.

Therefore it is recommended that you use the Oracle database character set WE8MSWIN1252 when you create the database (you cannot change this after installation). All the characters that can be used in WorkZone Content Server can be saved in the database.

> **Important:** The Danish State Archives require that structural data is delivered in the character set ”unicode (well-formed UTF8)”, which includes to the Oracle character set WE8MSWIN1252.

If you only want to use one language, you can typically use either “WE8MSWIN1252” or “WE8ISO8859P1’.

If you want to use more than one language, you have to decide between the specific character sets that can cover all the languages or use UTF8.

UTF8

The overhead using UTF8 is about 20%, because some characters are represented by up to 4 bytes.

Converting to UTF8

If you have a database not using UTF8, and you want this database to use UTF8, the most secure method is to export data, and then import the data into a new UTF8 database, and this import have to be done in 4 steps.

- Import all tables
- Convert all columns of type char and varchar2 to use CHAR instead of BYTE in the schemas making up the WorkZone Content Server database
- Alter table T modify(C varchar2(10 CHAR))
- Import the rest including all data

Oracles globalization support guide

The converting between non UTF8 to UTF8 can be done in other ways, but it depends on the nature of the characters in the database. It is advisable to examine Oracles Globalization Support Guide before making a database for use with more than one language.

Using Oracle proxy users

You can install and upgrade your database through an Oracle proxy user, which enables you to log install and upgrade actions on the database for each proxy user.

WorkZone Content Server does not contain an Oracle proxy user by default and you must create the Oracle proxy user and then assign the proxy user connect rights through the **sjsysadm** schema. The proxy user is then seamlessly handled by WorkZone Content Server installation and upgrade scripts.

For more regarding Oracle proxy users, see Oracle user guides, available online.

Create the WorkZone Content Server database

You can either create the Oracle database using scripts or using the Oracle GUI tool.

> **Prerequisite:** The Oracle database must be created with the necessary table spaces available.

Create the WorkZone Content Server database

This procedure describes how to create a WorkZone Content Server database. You must create the database on the Oracle server.

1. Open the folder, located in:

   ```
   Program Files\KMD\WorkZone\Program\DBSetup\OracleTemplates\<oracle version no.>
   ```

2. Copy the `SJ4.X_Oracle11.2.dbt` (Oracle 11) file.
3. Place the copy of the file in the folder `[ORACLE_HOME]\assistants\dbca\templates`.
4. Start the Oracle Database Configuration Assistant.
5. Follow the guidelines from Oracle describing how to create a new database. Select **SJ4.X Oracle11.2** when you create the database. This ensures correct definition of, for example, the Oracle components, which must be installed.
6. Check and, if necessary, correct the values that are filled in advance. Change the sizes of tablespaces, if necessary.

See also:

Prerequisites for WorkZone Content Server database

Install the WorkZone Content Server database

Install the WorkZone Content Server database

Create, optimize, and synchronize text indexes

Drop and recreate the intermedia text index

Tuning the database

Using Oracle proxy users

Installation errors

Install the WorkZone Content Server database

This procedure describes how to install a new WorkZone Content Server database.

> **Note:** WorkZone databases require a sjsysadm user. If you are installing a new WorkZone database, the sjsysadm user will therefore not be present. In this situation, you must log on to the database as the Sys user and create the sysysadm user and password. The creation process will automatically assign the necessary privileges to the sjsysadm user. See step 2 below.

1. Start the `wzsql.exe` program on the server where WorkZone Content Server is installed. **WZsql** form is displayed with the **Odbc connect** form on top.
2. In the **Odbc connect** form:
    1. **Data Source name** field: Select the relevant database in the **Data Source Name** (DSN) column.
    2. **User name** field: The name of a database system administrator with sufficient rights to install the database
    3. **Password** field: The password of the system administrator defined in the **User name** field above.
       You must use the user name **sys** and the password **<password for**

sys> as **sysdba**, when you are installing a new database from scratch.

3. Click **OK** to log on access and display the **WZsql** form. The title of the **WZsql** form now displays your user name and database name.
4. In the **WZsql** form, click **Sjbase** > **Install/Upgrade db** to open the **Create a privilege to Sjsysadm** form.
5. In the **Create a privilege to Sjsysadm** form:
    1. Click **Select version.txt** to navigate to and select the **version.txt** field for the database to be installed.
    2. In both **Password sjsysadm** fields, enter the sjsysadm password.
6. Click **Save** to save the defined credentials and close the **Create a privilege to Sjsysadm** form.
7. In the **WZsql** form, click **Sjbase** > **Install/Upgrade db** to open the **dbinstall** form.
8. In the **dbinstall** form:
    1. Click **Select version.txt** to navigate to and select the **version.txt** file for the database to be installed.
    2. Select the **Corporate Access Code** check box to install database elements that support the Corporate Access Code security settings in WorkZone. If you are using Standard WorkZone security, clear this check box.
    3. Select all relevant cultures and language packs you want to activate and select one of the selected languages to be the default language of WorkZone.
    4. Click the **Tablespaces** button to map all logical tablespaces to physical table spaces.
    5. Click the **Install/Upgrade** button to start the database installation.
9. When the installation is completed, the overall installation status is displayed in a pop-up window. An overview of any Installation errors can be found in a folder with the database name, located in C:\ProgramData\Scanjour\wzsql on the local machine.

10. Restart Internet Information Services (IIS), see below

Restart Internet Information Services (IIS)

Restart the IIS when the WorkZone Content Server database has been installed. Run IIS reset without any parameters.

See also

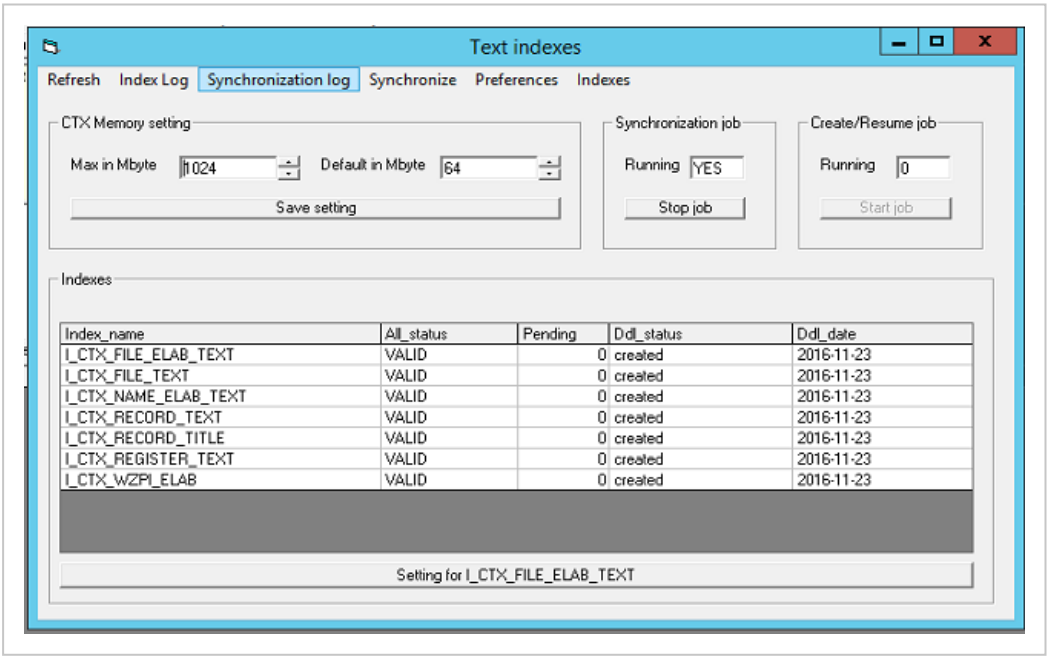
Using Oracle proxy users

Create, optimize, and synchronize text indexes

When the WorkZone Content Server database is installed, you must ensure that the Oracle Text indexes are created and optimized and that the database synchronizes the Oracle Text index with the WorkZone Content Server free text index.

Create, optimize, and synchronize text indexes

1. Select **Sjbase** >**Text indexes**. The **Text indexes** window appears.

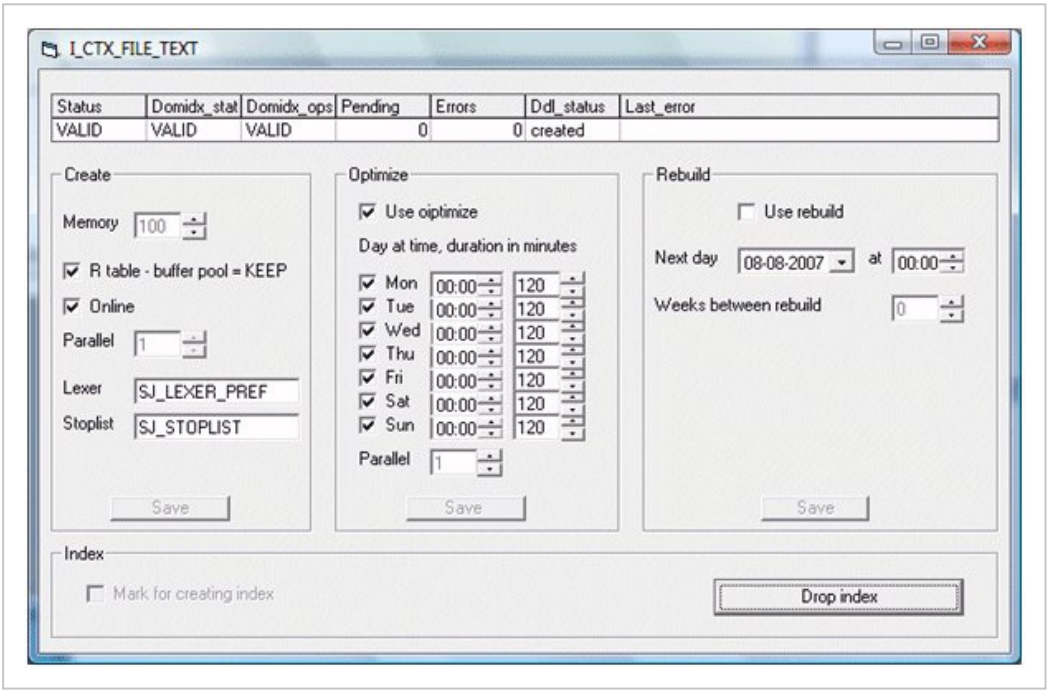


2. In the **Max in Mbyte** and **Default in Mbyte** fields, select the CTX memory size to be used by Oracle when it creates/synchronizes the text index, and click **Save**

setting. The selected memory sizes are saved.

The **Max in Mbyte** field specifies the maximum memory size to be used when creating a text index, and the **Default in Mbyte** field specifies how much memory will be used, if the memory size is not specified.

3. In the **Index_name** column, select the index, which you want to (re)create, and click **Setting for <index name>**.
   The **<index name>** window appears. At the top of the window, status information for the selected index is shown. The lower part of the window contains a number of configuration options.



Tip: You can also create or recreate all indexes at the same time. In the **Text indexes** window, click **Indexes** and then **Create missing indexes**, **Recreate indexes**, or **Set all to optimize** depending on what you want to do.

4. In the lower part of the **<index name>** window, specify configuration options.

Specify options under **Create**

1. In the **Memory** field, specify the memory size to be used for creating the index. If you do not specify a number of Mbytes in the field, the default value is used.
2. Select the **R table – buffer pool = KEEP** check box if you want to place the **R-table** (Oracle's Rowid conversion table) in permanent cache next time the index is created.

   - The check box is selected by default.
   - f you do not want to place the R-table in permanent cache, you must deselect the check box. This means that the R-table is removed from permanent cache next time the index is created. If the R-table must be removed at once, you must perform the procedure described in Tuning. Select the Online check box if you want to be able to use the underlying table at the same time as the index is created.
   - This option is only available if you are using the Oracle Enterprise Edition.

3. Use the buttons in the **Parallel** field to specify the number of parallel processes to be used when creating the index.

   The amount of memory used for creating the index equals the value of the Memory field multiplied by the value of the Parallel field.

4. Click **Save**. The configuration made in **Create** box is saved.

Specify options under **Optimize**

1. Select the **Use optimize** check box to switch on optimization.

   You can clear the check box to switch off optimization for a period without changing the configuration of the other options in the **Optimize** area.

2. Select relevant check boxes to specify the days of the week on which the optimization must take place.

3. For each selected day of the week, specify the time of day on which the optimization must take place.
4. For each selected day of the week, specify the duration in minutes of the optimization process.
5. In the **Parallel** field, specify the number of parallel processes to be used when optimizing the index.
6. Click **Save**. The configuration made in the **Optimize** area is saved.

Specify options under **Rebuild**

1. Select the **Use rebuild** check box to switch on rebuild.

   You can clear this check box to switch off rebuild for a period without changing the configuration of the other options in the **Rebuild** area.
2. In the **Next day** filed, select the date for the next rebuild and in the **at** field, to select the time for the next rebuild.
3. In the **Weeks between rebuild** field, select the number of weeks between the rebuilds.
4. Click **Save**. The configuration made in the **Rebuild** area is saved.

Specify options under **Index**

- Select the **Mark for creating index** check box, if you want the index to be generated.

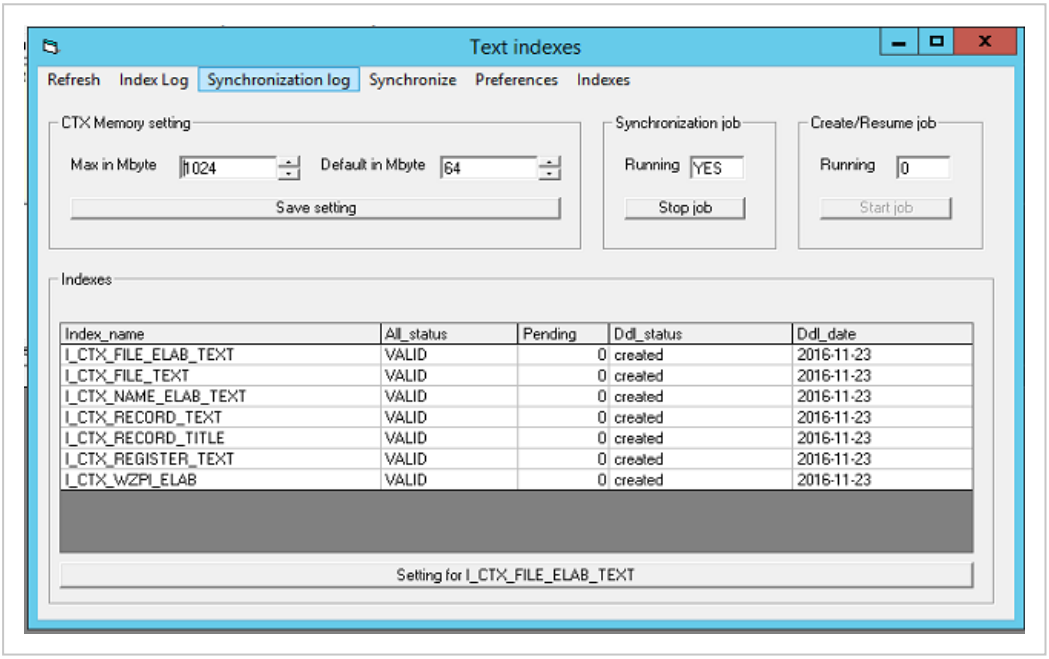
5. Close the **<index name>** window.
6. Repeat the steps 3-5 for each index that you want to (re)create in the table at the bottom of the **Text indexes** window.
7. In the **Text indexes** window, in the **Create/Resume job** area, click **Start job**. The indexes, which have the **Mark for creating index** check box selected, are created sequentially.
8. In the **Text indexes** window, in the **Synchronization job** area, click **Start job**. The job starts synchronizing the indexes, and at the selected day(s) and time(s) for each of the indexes optimizing and/or rebuilding.

You can always change the days and times for executing the job, even though the job is already running.

9. Close the **Text indexes** window.

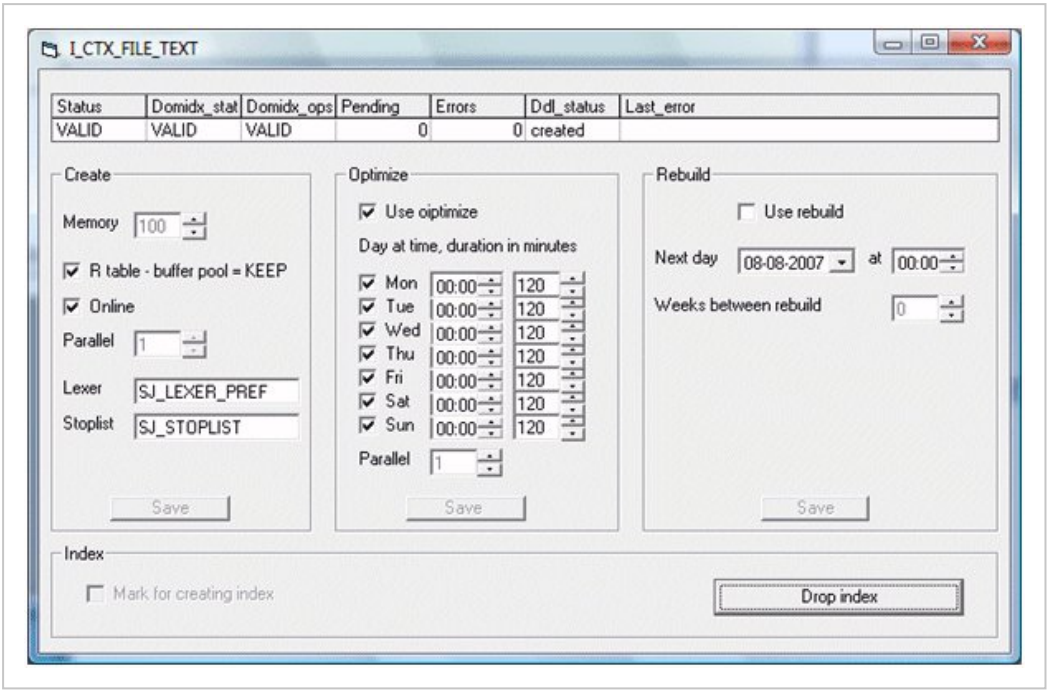
Drop and recreate the intermedia text index

1. Select **Sjbase** > **Text indexes**. The **Text indexes** window appears.



2. In the **Index_name** column, select the index which you want to drop or recreate, and then click **Setting for <index name>**. The **<index name>** window appears. At the top of the window, status information for the selected index is shown. In the

lower part of the window contains a number of catalog sections options.



3. In the **Index** area, click **Drop index** if you want to drop (remove) the index. The **Drop index** button becomes inactive, and the **Mark for creating index** check box becomes active. In the **Text indexes** window, the value **DO NOT EXIST** is shown in the **All_status** column for the selected index, when the index has been dropped.

   It can take a short while, before the index is dropped.

4. In the **Index group** box, select the **Mark for creating index** check box, if you want to recreate the index. The **Mark for creating index** check box becomes inactive.

   If the index is in error, the check box is called **Mark for resuming index**.

5. Close the **<index name>** window.
6. In the **Create/Resume job** area in the **Text indexes**window, click **Start job**. It takes a long time before the index is created. When the index has been created, the value **VALID** is shown in the **All_status** column for the selected index.

   The **Running** field shows the number of jobs currently running.

7. Close the window.

Tuning the database

You can tune the WorkZone Content Server database in order to optimize performance.

1. Select **Sjbase** >**Tuning**.
2. Click **View parameters**.
   At the bottom of the **ScanJour SQL** window a list of parameters is shown. The list can be used for optimizing the WorkZone Content Server database. In the list the actual values and the recommended values of the parameters are shown.

   Since it is only recommendation, there can be other values which are better than the values listed. If the value of a parameter is not OK, it is shown by the text N in the **Value_ok** column, and the row in question is red. When a row is green, this indicates that the value of the parameter is OK.
3. Change the relevant parameters by executing SQL statements in the **ScanJour SQL** window or by changing the init.ora parameters.
4. Click **View candidates**. At the bottom of the **ScanJour SQL** window a list of tables and indexes in permanent cache is shown.
   The text **buffer_pool = KEEP** indicates that a table or index is placed in permanent cache. The text **object_keep = Y** shows which tables and indexes will be moved to permanent cache, and the text **object_keep = N** shows which table and indexes will be removed from permanent cache, if you click **Apply** changes.
5. Click **Apply changes** if you want to move all tables and indexes marked with the text **object_keep = Y** to the permanent cache, and at the same time remove all tables and indexes marked with the text **object_keep = N** from the permanent cache. You must manually change the cache of the table SJ_bpk_objects. This table holds the information about what you want in the keep cache.
6. Close the **Tuning** window.

Installation errors

If the installation of the database is not successful, you will get a message. The message tells you in which log file the error is contained, and thus where to read more information.

You must try to correct the error using the information from the log file, and then you must run the installation again. See Install the WorkZone Content Server database.

The log catalogue for installation of the database is called:

```
C:\Program Files (x86)\KMD\WorkZone\Program\DBSetup\log\<TNS_NAME>
```

where `<TNS_NAME>` is the Oracle TNS name used for the database.

Convert the database from version 12 to 13

Version 12 (and earlier versions) of the database uses Danish names for registers, tables and so on. From version 13 onwards, all names are translated into English.

Therefore, if you want to upgrade a database from version 12 to version 13, you must convert the database from Danish to English, before you can do the upgrade.

- If the database is version 12.0.959.0 or later you can convert the database directly.
- If the database is a version 12 earlier than 12.0.959.0 you must update the database to version 12.0.959.9.

Use the `catalog basen.12.0.959.0` for this purpose.

This means that you must run the upgrade process by selecting **Sjbase** > **Installation/ Upgrading** and then make the conversion afterwards. Upgrading is done using the scripts in the folder `…/Program Files/KMD/WorkZone/Program/DBSetup/basen.12`.

Convert the database

> **Prerequisite:** You must log on as sjsysadm, if you want to upgrade an existing database.

1. Start **scansql.exe**.
   If you use the program for the first time, the **ScanJour SQL** window appears with the **Select Data Source** window on top. In this case, proceed to step 3. Otherwise the **ScanJour SQL** window appears with the **Connections** window on top of it. In this case, proceed to step 2.

2. Select the relevant combination of DSN and UID, and then proceed to step 4.
3. Select the **Machine Data Source** tab and select the relevant database (DSN) in the **Data Source Name** column.
4. Click **OK**. The **Oracle ODBC Driver Connect** window appears. The selected DSN is shown in the **Service Name** field.
5. Enter the user name and password in the **User Name** and **Password** fields.
6. Click **OK**.
   The **Oracle ODBC Driver Connect** window closes, and you can use the **ScanJour SQL** window. In the title bar of the **ScanJour SQL** window, information on the database name, user name, and so on is now shown.
7. Select **Danish to English** > **Converting**.

   If the user sjsysadm has running jobs, you must remove these jobs before continuing.

   The **Danish to English database translation** window appears. The window shows the path to the script that handles the conversion from Danish to English. If you have moved the script to another location, you must find, and select it using the **Browse** button.
8. Click **Execute**.

   A command window appears and starts executing the program cmd.exe. After a moment the **WorkZone Content Server database** window appears with a message showing the version number of your current database, and you are asked if you want to convert from Danish to English.

   During the conversion the database will be upgraded to version 13.
9. Click **Yes**. The conversion starts. It takes a while. When the conversion is completed, you receive a message telling that the database has been upgraded. The message also contains a path to a file, in which you can see the details of the upgrade.

> Important: Upgrade the database after conversion. See Upgrade a WorkZone database.

The database upgrading form

The **Database Upgrading** form is used to define the parameters for upgrading your database.

The following options are available in the **Database Upgrading** form.

Option	Description
Database version	Displays the current database version: • **DBNEW** - This value is displayed when installing a new database. • **<version no.>** - The version of the current database. The version number is displayed upgrading an existing database to a new version.
Upgrade to version	Shows the version number of the database to which you are upgrading. • <> - This value is empty when installing a new database. • <version no.> - The version number of the database you are upgrading to.
Standard	Install a standard WorkZone database.
Government	Install a standard WorkZone database including the extra objects/data required for the government edition solution of WorkZone.
Standard db	Install a standard WorkZone Content Server database. This check box is always selected and cannot be cleared.
Archive	Create an archive database. This check box is always selected and cannot be cleared.
Archive in separate database	Select this check box to archive in another database than the one you are currently installing. If you select this check box, you must specify the name of the ODBC entry of the database where you want to create an archive. See the **DSN** field below.

Option	Description
DSN	Specify the name of the ODBC entry of the database where you want to create an archive. You only have to fill in this field, if you have selected the **Archives in a separate database** check box (see “Archives in a separate database” above).
Auto load fesd data, only when it is a new database	Select this check box to insert the metadata used by FESD in the database. You only need to select this check box when installing a new database. The check box is selected by default, but only when loading data into a new database.
Organization access code	Create the objects/data required for organization access codes.
CVR integration	Create objects/data required for integrating to CVR. **Note:** Further configuration is required for making the integration work, see the WorkZone Content Server, CVR Integration, Configuration Guide.
CPR integration	Create the objects/data required for integrating to CPR are created. **Note:** Further configuration is required for making the integration work, see the document WorkZone Content Server CPR Integration, Configuration Guide.

Troubleshooting

Slow AgentFix caused by an update queue on the $R table

This issue occurs in Oracle version 11.2.0.4 but can also be experienced on Oracle version 12c.

Frequent concurrent updates by multiple users resulted in severe row lock contentions, even when updating completely different rows.

Background

Updates of Text indexes are treated as delete commands followed by insert commands.

While the inserts will be performed during the index sync and batched for all users, the deletes are immediate and happen at commit time.

Text indexes are implemented as LOBs (Large Objects) and therefore during commit time a LOB piecewise update of the $R table will be performed,

setting the rowid of the deleted rows to null. Moreover, a small number of LOBs are used to map all the rows stored.

This is causes the row lock contention experienced in this case.

Fixing the issue

You can create the LOB text indexes without creating the row lock contentions by using this undocumented option (from Oracle support)

alter session set events '30579 trace name context forever, level 268435456';

exec ctx_ddl.create_preference('mypref', 'BASIC_STORAGE');

exec ctx_ddl.set_attribute('mypref', 'small_r_row', 'T');

> **Note:** Depending on the Oracle release version, you might need to install a patch. Navigate to Metalink and search for the "small_r_row" patch for your Orcacle release version.

Install WorkZone 365

> **Prerequisite:** WorkZone 365 Outlook - Mail module is only supported with Microsoft Exchange Server Online. It is not supported with Exchange Server 2019.

The installation process consists of two steps:

1. Installing the WorkZone 365 server.
2. Installing WorkZone 365 client by uploading manifests.

Install WorkZone 365 server

1. Double-click the `KMD WorkZone Office Setup.msi` file.
2. Click **Run**, and then click **Next**.
3. Read the terms and conditions and select the **I accept the terms in the License Agreement** check box. Click **Next**.
4. Click **Install**, and then click **Finish**.

Download manifests

Before installing you must download the manifests from the WorkZone server. Use this link with the proper host name:

`https://[hostname]/app/office/webaddins/office/OfficeManifest.xml`

`https://[host-name]/app/office/webaddins/outlook/meeting/MeetingManifest.xml`

`https://[host-name]/app/office/webaddins/outlook/mail/MailManifest.xml`

Adjust the MeetingManifest.xml

> **Tip:** Save a copy of each manifest locally to easily access GUIDs. It will help you monitor all your instances and versions of WorkZone 365 for Outlook.

If you use:

- Multiple instances of WorkZone 365 for Outlook on the same Exchange server, or
- Different versions of WorkZone 365 for Outlook on the same Exchange server,

you must change WorkZone 365 GUID in the MeetingManifest.xml.

1. Generate a new GUID by using any online GUID generation tool, for example, GUID Generator.
2. When GUID is updated, upload manifest to the Exchange Admin Center.

Install WorkZone 365 for Microsoft Office 365

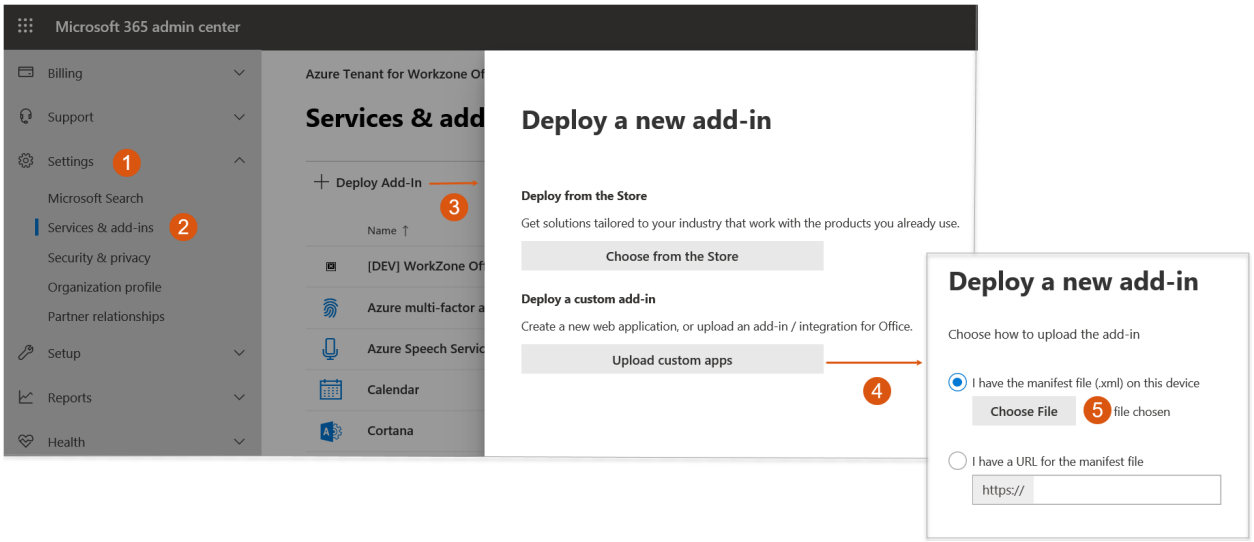
You can install WorkZone 365 for Microsoft Office 365 that includes Word, Excel, PowerPoint, and Outlook by using:

- Microsoft 365 admin center (web interface), or
- Microsoft PowerShell (command line).

Use web interface

If you have access to the Microsoft admin center, use the standard Microsoft guidance to deploy WorkZone 365 for Office 365. See Deploy an Office add-in using the admin center.

> **Tip:** In step 3, click **Upload custom apps** and select the manifest from your computer.



Use command line

You can use Microsoft PowerShell to deploy WorkZone 365 for Office 365. To do this, follow the standard Microsoft guidance. See Use the Centralized Deployment PowerShell cmdlets to manage add-ins.

> **Tip:** See also Deploy and publish your Office Add-in.

> **Note:** By default, WorkZone 365 is disabled after the installation. You can enable it in WorkZone Configurator. To do this, go to **Global > Feature settings > WorkZone 365** , select the needed products, and click **Save**.

Install WorkZone 365 to use meetings in Microsoft Outlook 2016 and 2019

> **Important:** WorkZone 365 is fully supported in Microsoft Office 365, but you can install it for Microsoft Outlook 2016 and 2019 to use WorkZone Meeting functionality.

> **Prerequisite:** Download `MeetingManifest.xml` manifest and add it to a shared folder. To share a folder, right-click it, select **Properties > Sharing > Share**. Add yourself and users and/or groups with whom you want to share WorkZone Meetings. Click **Share**.

There are three installation options:

- via Microsoft Outlook web interface
- via Exchange Admin Center (EAC, web interface)
- via Microsoft PowerShell (command line). See Install add-ins for Outlook for your organization in Exchange 2013 (these article guidelines apply also to the Exchange 2016 and Exchange 2019 versions).

Use Outlook web interface

1. Start Outlook.
2. Click **File**.
3. Click on the link under **Account settings** to start OWA.
4. Login into OWA with your Outlook credentials.
5. Click on the gear icon on the right side.
6. Click **Manage add-ins** > **Add from a file**.
7. Click **Browse** and provide location for the shared folder with the `MeetingManifest.xml` manifest file.
8. Select the `MeetingManifest.xml` file, and click **Open**.
9. Click **Next** > **Install** > **OK**.
10. Go back to Outlook > **Calendar**, and create a new meeting. The **WorkZone 365 Meeting** button will be visible in the navigation ribbon.

Install WorkZone Teams

Prerequisite:

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

The installation process consists of two parts:

1. Installing WorkZone Teams on the server.
2. Installing WorkZone Teams on the client.

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.

Install and configure WorkZone for Office

Install WorkZone for Office server

Install manually

To install WorkZone for Office server, perform these steps:

1. Double-click the `KMD WorkZone Office Server.msi` file. The **Open file - Security Warning** dialog box is displayed.
2. Click **Run**. The **KMD WorkZone Office Server Setup** wizard is displayed.
3. Click **Next**. The **End-User License Agreement** page is displayed. Read the terms and conditions and select the **I accept the terms in the License Agreement** check box.

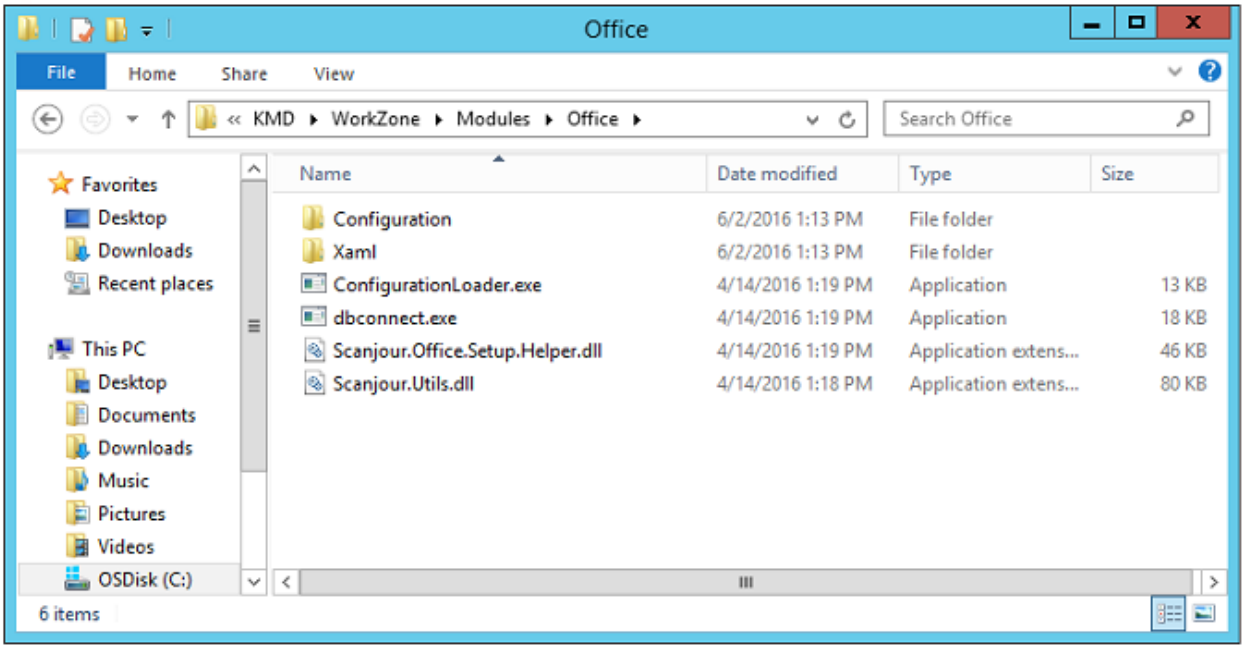
4. Click **Next**. The **Choose Setup Type** page is displayed.

5. Click **Typical**. The **Ready to install KMD WorkZone Office Server** page is displayed.
6. Click **Install**. After installation, the **Completed Setup Wizard** page is displayed.
7. Click **Finish**.

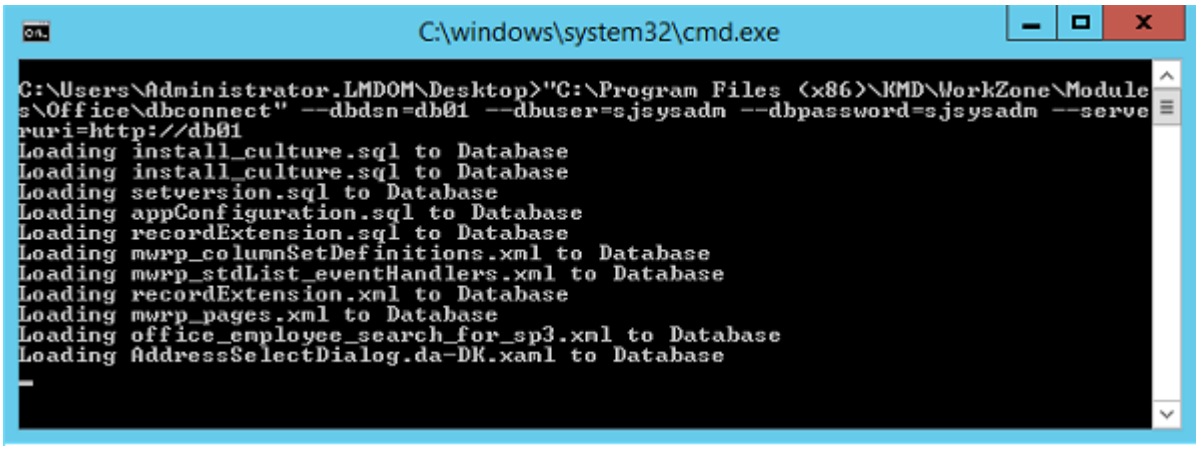
> Important: After you install WorkZone for Office server, you must update the database manually via `dbconnect.exe`.

Update the database

The Office Server installer installs all configuration files and tools into the file system under `C:\Program Files (x86)\KMD\WorkZone\Modules\Office`.



When you have completed the installation, you can load the configuration into the database via the `dbconnect.exe` command line tool. It is located in the Office folder.



`dbconnect.exe` is a command line tool which enables you to load and unload database configuration files, SQL scripts, and XAMLs (dialog boxes).

This tool has the following options:

- `/dbdsn=<dsn>` - The name of the database to be updated (required).
- `/dbuser=<user>` - The name of the database user (required).
- `/dbpassword=<password>` - The password of the database user.
- `/serveruri=<protocol>://<hostname>` - Protocol and hostname for the oData service.

- `/u` - Unloads installed data from the database (optional).
- `/log=<path>` - Writes log to the file at the specified address (optional).

Example:

```
c:\Program Files (x86)\KMD\WorkZone\Mod-
ules\Office\dbconnect.exe /dbdsn=demo /dbuser=sjsysadm /db-
password=xyzz /serveruri=https://demo.captialive.com /u
```

Note: `dbconnect.exe` updates only one database at a time. If you want to update multiple databases, run it several times with a different `/dbdsn` option.

Important: Restart IIS (Internet Information Services) for the configuration changes to take effect on the server.

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 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 `CcRe-`

Element	Default value	Description
		cipient 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 CcRe-cipient roles are values from the domain on the party:-custom_label field in the record register (custom_label with domain parameter 'AP').
PartyRoleKeys - CcRe-cipient	Kopimodt	Defines the values used for the sender, recipient, and Cc recipient roles on archived emails. Valid values of the Sender, Recipient, and CcRe-cipientroles 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 CcRe-

Element	Default value	Description
		cipientroles 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 Replyis 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.
AutoCreateMissingContact	True	Defines whether the system should create contacts from the email sender, recipient, and Copy fields if the contacts do not exist.
SuggestAnyContactWhenSav-ingEmail	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

Element	Default value	Description
		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_drafts`	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 navigation pane, including two subfolders: • **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

Element	Default value	Description
		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.
`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

Element	Default value	Description
		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 Multiple 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

Element	Default value	Description
		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.
`SuggestAnyContactWhenCrea-tingCase`	`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;`
	`my_organized_meet-ings;`
	`my_temporary_cases;`
	`my_recent_cases;`
	`my_changed_cases`
		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 case and meeting. Find the full list of search filters in the Available case and meeting lists table.

`SearchFilters - Register`	`my_reading_list_`	Simplifies the search process.

Element	Default value	Description

`Name="Record"`
`BlackList`
	`records;`
	`my_changed_records;`
	`my_recent_records;`
	`thrashed_records`
		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 preselected 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 the path: • Absolute path • Relative path • UNC format If the path is not defined, the Office **Template selection** dia-

Element	Default value	Description
		log box opens.
<AccessCodesAf-fectRequiredFields>	<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_
drafts</PredefinedFilters>
                <Register-
SelfWhenSaveEmail>False</RegisterSelfWhenSaveEmail>
                <Check-
AllUnresolvedContacts>False</CheckAllUnresolvedContacts>
                <UseCur-
rentUserAsCaseHandler>False</UseCurrentUserAsCaseHandler>
                <MassRegistration>
                    <EnableEditCom-
monMetadata>false</EnableEditCommonMetadata>
                </MassRegistration>
                <Dis-
playDateFormat>SystemDefault</DisplayDateFormat>
                <SearchFilters>
```

```
                <Register Name="Case" BlackList="my_reading_list_
cases;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>
                <Column Name="closed" Value-
e="&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\Mod-
   ules\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 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 Content Server. 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 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

User interface name	Name in code	Description
		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 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.

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

Install WorkZone for Office client

The WorkZone for Office installation wizard contains the following modules:

- WorkZone for Excel
- WorkZone for Outlook
- WorkZone for PowerPoint
- WorkZone for Word

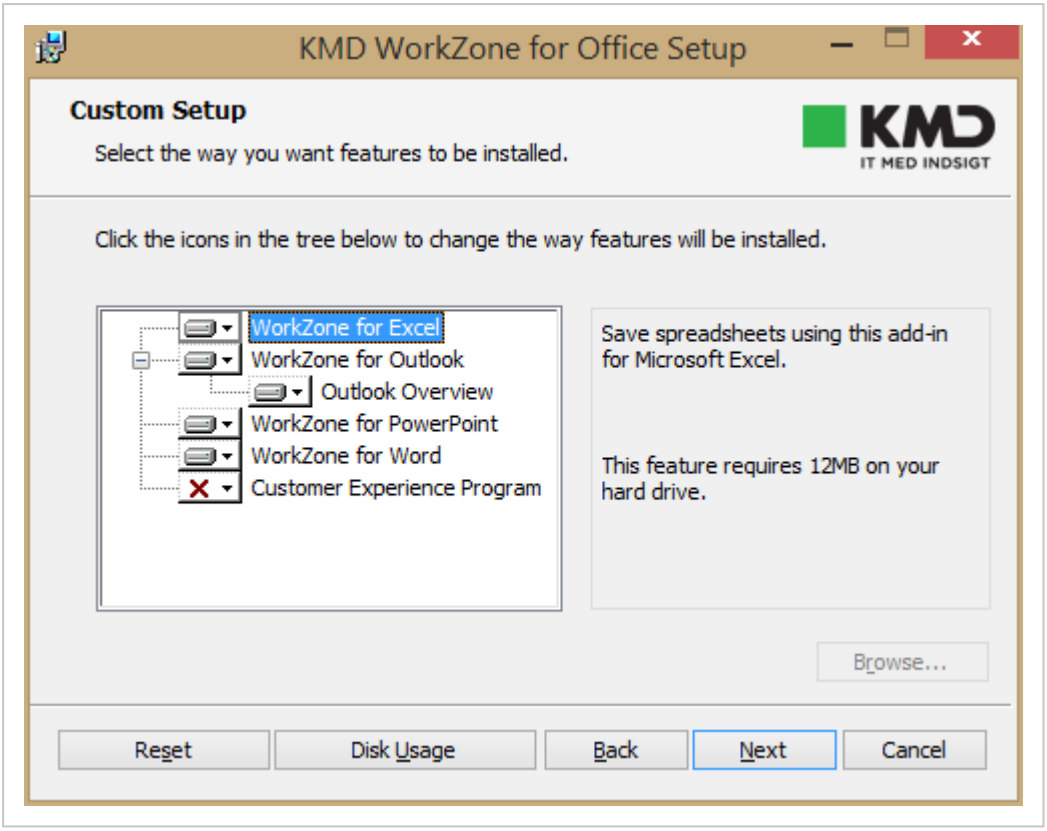
Install manually

To install WorkZone for Office, you must perform the following steps:

1. Double-click the `KMD WorkZone for Office.msi` file. If you are installing on a x64 bit version of Microsoft Office, then choose the `KMD WorkZone for Office x64.msi` file.
   KMDWorkZone for Office x64 is only supported by Microsoft Office 2016.
2. The **KMD WorkZone for Office Setup** wizard is displayed. Click **Next**.
3. The **End-User License Agreement** page is displayed. Read the terms and conditions, and select the **I accept the terms in the License Agreement** check box. Click **Next**.
4. On the **Service Address** page, enter the Web Services host. Optionally, select the **Use Net.TCP protocol** check box to use Net.TCP instead of https for data transfer. Click **Next**.

   - If your users upload documents with a size of around 50 MB and more, it makes sense to use Net.TCP.
   - By using Net.TCP, the size of documents can be increased up to 100 MB. Possibility to use documents of a bigger size depends on different parameters such as server settings, limitations at user PCs, etc. and must be tested individually.
5. The **Custom Setup** page is displayed. By default, all Office modules are selected.

   If you do not want to install all modules, you can deselect one or more of the modules (for example, WorkZone for Excel) by clicking the icon next to their names. Then they will not be installed. Click **Next**.



6. The **Ready to install** page is displayed. Click **Install**.
7. After installation, the **Completed Setup Wizard** window is displayed. Click **Finish**.

> **Tip:** By default, all settings are written to the HKEY_LOCAL_MACHINE registry during the installation. To enable user custom settings for a user who works on the same PC/Terminal Server together with other users, enter all data into HKEY_CURRENT_USER.

Install silently

You can perform automated deployment of WorkZone for Office in a scripted approach using `msiexec` where arguments are passed in via command line parameters, or in any other way suitable to you.

Use command line parameters

If you use the `msiexec` utility, set the below parameters to execute the installer.

64-bit Office

If you are installing on a x64 bit version of Office, then choose the `KMD WorkZone for Office x64.msi` file

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=<protocol>://<hostname> CMD_UI_SERVERURL-
L=<protocol>://<hostname> ADDLOCAL=ALL CMD_UI_NETTCP=#<use_
nettcp> /qn /lv*x c:\log\log.txt
```

Where:

- `<protocol>` is https. WorkZone Content Server must be configured to run on https. See Configuring https.
- `<hostname>` is the name of the WorkZone Content Server server.
- `<log_file>` is a file which contains the installation log. If the installation fails, you can find a related error message in this file.
- `<use_nettcp>` is a flag of the Net.TCP protocol usage. 0 - the Net.TCP protocol is disabled, and 1 - the protocol is enabled.

Code example:

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=https://demo.captialive.com CMD_UI_SERVERURL-
L=https://demo.captialive.com ADDLOCAL=ALL CMD_UI_NETTCP=#0 /qn
/lv*x c:\log\log.txt
```

Selectable installation using command line

You can select which modules of WorkZone for Office to install by specifying them in the `ADDLOCAL` parameter (for more information, see Microsoft library). Multiple values must be separated by commas.

Value	Module
`Scanjour.Office.ExcelAddIn`	WorkZone for Excel
`Scanjour.Office.OutlookAddIns`	Parent feature to select both WorkZone for Outlook and WorkZone Process for Outlook mod-

Value	Module
	ules
`Scanjour.Office.OutlookAddIn`	WorkZone for Outlook
`Scanjour.Office.Overview`	WorkZone Outlook Overview
`Scanjour.Office.PowerPointAddIn`	WorkZone for PowerPoint
`Scanjour.Office.WordAddIn`	WorkZone for Word

Install WorkZone for Office client

The WorkZone for Office installation wizard contains the following modules:

- WorkZone for Excel
- WorkZone for Outlook
- WorkZone for PowerPoint
- WorkZone for Word

Install manually

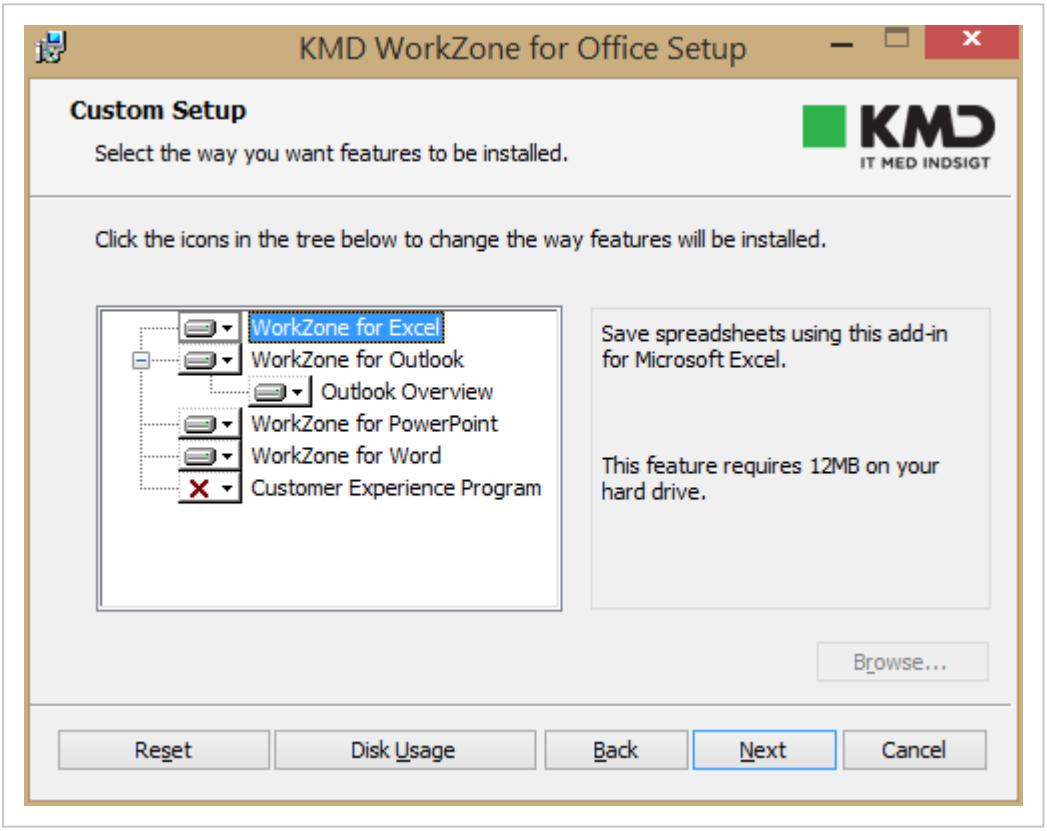
To install WorkZone for Office, you must perform the following steps:

1. Double-click the `KMD WorkZone for Office.msi` file. If you are installing on a x64 bit version of Microsoft Office, then choose the `KMD WorkZone for Office x64.msi` file.
   KMDWorkZone for Office x64 is only supported by Microsoft Office 2016.
2. The **KMD WorkZone for Office Setup** wizard is displayed. Click **Next**.
3. The **End-User License Agreement** page is displayed. Read the terms and conditions, and select the **I accept the terms in the License Agreement** check box. Click **Next**.
4. On the **Service Address** page, enter the Web Services host. Optionally, select the **Use Net.TCP protocol** check box to use Net.TCP instead of https for data transfer. Click **Next**.

- If your users upload documents with a size of around 50 MB and more, it makes sense to use Net.TCP.
- By using Net.TCP, the size of documents can be increased up to 100 MB. Possibility to use documents of a bigger size depends on different parameters such as server settings, limitations at user PCs, etc. and must be tested individually.

5. The **Custom Setup** page is displayed. By default, all Office modules are selected.

   If you do not want to install all modules, you can deselect one or more of the modules (for example, WorkZone for Excel) by clicking the icon next to their names. Then they will not be installed. Click **Next**.



6. The **Ready to install** page is displayed. Click **Install**.
7. After installation, the **Completed Setup Wizard** window is displayed. Click **Finish**.

> **Tip:** By default, all settings are written to the HKEY_LOCAL_MACHINE registry during the installation. To enable user custom settings for a user who works on the same PC/Terminal Server together with other users, enter all data into HKEY_CURRENT_USER.

Install silently

You can perform automated deployment of WorkZone for Office in a scripted approach using `msiexec` where arguments are passed in via command line parameters, or in any other way suitable to you.

Use command line parameters

If you use the `msiexec` utility, set the below parameters to execute the installer.

64-bit Office

If you are installing on a x64 bit version of Office, then choose the `KMD WorkZone for Office x64.msi` file

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=<protocol>://<hostname> CMD_UI_SERVERURL-
L=<protocol>://<hostname> ADDLOCAL=ALL CMD_UI_NETTCP=#<use_
nettcp> /qn /lv*x c:\log\log.txt
```

Where:

- `<protocol>` is https. WorkZone Content Server must be configured to run on https. See Configuring https.
- `<hostname>` is the name of the WorkZone Content Server server.
- `<log_file>` is a file which contains the installation log. If the installation fails, you can find a related error message in this file.
- `<use_nettcp>` is a flag of the Net.TCP protocol usage. 0 – the Net.TCP protocol is disabled, and 1 – the protocol is enabled.

Code example:

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=https://demo.captialive.com CMD_UI_SERVERURL-
L=https://demo.captialive.com ADDLOCAL=ALL CMD_UI_NETTCP=#0 /qn
/lv*x c:\log\log.txt
```

Selectable installation using command line

You can select which modules of WorkZone for Office to install by specifying them in the `ADDLOCAL` parameter (for more information, see Microsoft library). Multiple values must be separated by commas.

Value	Module
`Scanjour.Office.ExcelAddIn`	WorkZone for Excel
`Scanjour.Office.OutlookAddIns`	Parent feature to select both WorkZone for Outlook and WorkZone Process for Outlook modules
`Scanjour.Office.OutlookAddIn`	WorkZone for Outlook
`Scanjour.Office.Overview`	WorkZone Outlook Overview
`Scanjour.Office.PowerPointAddIn`	WorkZone for PowerPoint
`Scanjour.Office.WordAddIn`	WorkZone for Word

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\Mi-
crosoft\Office\Outlook\Addins\Scanjour.Office.OutlookAddIn]
```

```
"LoadBehavior"=dword:00000003
```

```
[HKEY_CURRENT_USER\Soft-
ware\Mi-
crosoft\Of-
fice\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\Power-
Point\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\Of-
fice\16.0\Outlook\Resiliency\CrashingAddinList]
```

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

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

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

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

Automated deployment

You can perform automated deployment of WorkZone for Office:

- in a scripted approach using `msiexec` where arguments are passed in via command line parameters, or
- using Group Policy Object (GPO), or
- in any other way suitable to your company.

Use command line parameters

If you use the `msiexec` utility, set the parameters listed below to run the installer.

64-bit Office

If you are installing on a x64 bit version of Office, then choose the `KMD WorkZone for Office x64.msi` file

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=<protocol>://<hostname> CMD_UI_SERVERURL-
L=<protocol>://<hostname> ADDLOCAL=ALL CMD_UI_NETTCP=#<use_
nettcp> /qn /lv*x c:\log\log.txt
```

Where:

- `<protocol>` is https.

  > **Note:** Before you deploy WorkZone for Office to run on https, ensure that WorkZone Content Server is configured accordingly. See Configuring https.

- `<hostname>` is the name of the WorkZone Content Server server.
- `<log_file>` is a file which contains the installation log. If the installation fails, you can find a related error message in this file.
- `<use_nettcp>` is a flag of the Net.TCP protocol usage. 0 - the Net.TCP protocol is disabled, and 1 - the protocol is enabled.

Code example:

```
Msiexec /i "KMD WorkZone for Office.msi" CMD_UI_SERVERWS-
S=https://demo.captialive.com CMD_UI_SERVERURL-
L=https://demo.captialive.com ADDLOCAL=ALL CMD_UI_NETTCP=#0 /qn
/lv*x c:\log\log.txt
```

Selectable installation using command line

You can select which modules of WorkZone for Office to install by specifying them in the `ADDLOCAL` parameter (for more information, see Microsoft library). Multiple values must be separated by commas.

Value	Module
`Scanjour.Office.ExcelAddIn`	WorkZone for Excel
`Scanjour.Office.OutlookAddIns`	Parent feature to select both WorkZone for Outlook and WorkZone Process for Outlook modules
`Scanjour.Office.OutlookAddIn`	WorkZone for Outlook
`Scanjour.Office.Overview`	WorkZone Outlook Overview
`Scanjour.Office.PowerPointAddIn`	WorkZone for PowerPoint
`Scanjour.Office.WordAddIn`	WorkZone for Word

Use group policy objects

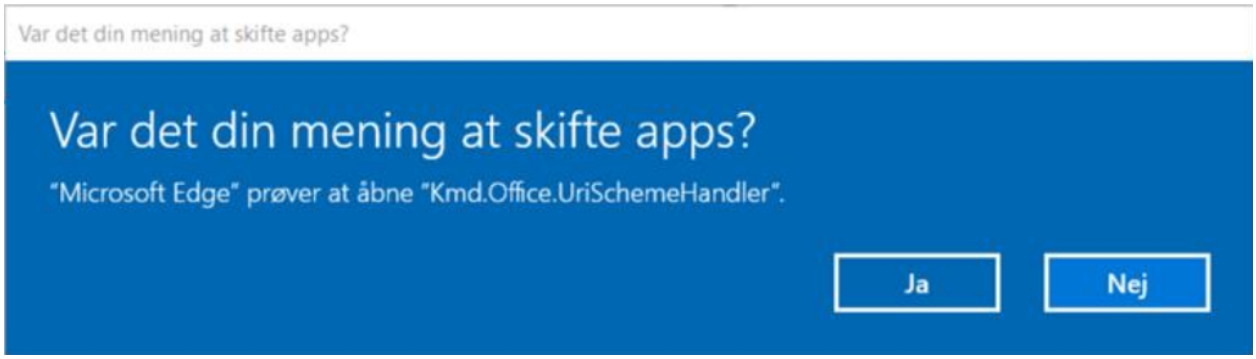
To deploy using GPO, the MSI package must be customized with the values that you would otherwise provide through the installation UI.

- Base address and protocol of the web services (`CMD_UI_SERVERWS`)
- Address of the WorkZone Content Server website (`CMD_UI_SERVERURL`)

Installation fails if any of the command line parameters, mentioned above, is not specified.

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]
```

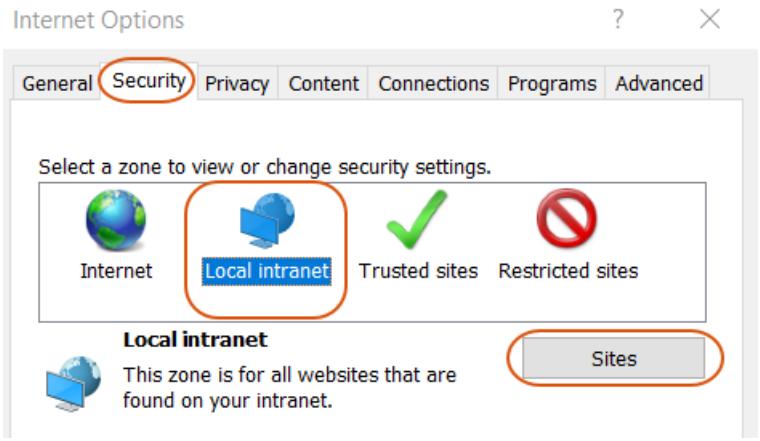
```
"WarnOnOpen"=dword:00000000
```

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://help.workzone.kmd.dk` 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**.

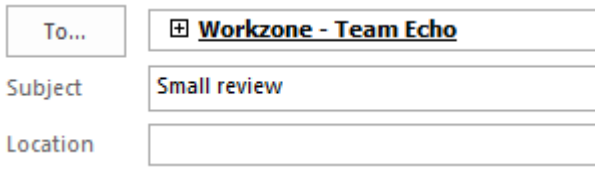


3. Click **Advanced**.
4. Type in `https://help.workzone.kmd.dk`, and click **Add**.

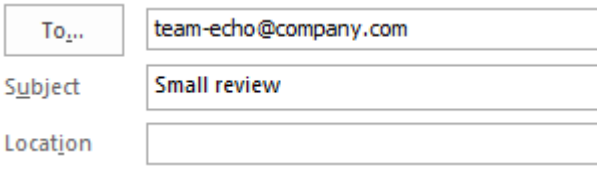
A meeting was sent to a group, but its contacts are not saved as parties on case.

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\Soft-
ware\Microsoft\Office\16.0\Outlook\Security] "EnableRoam-
ingFolderHomepages"=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.

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 Content Server installation. Note that it is not required to install a client, such as WorkZone Client.

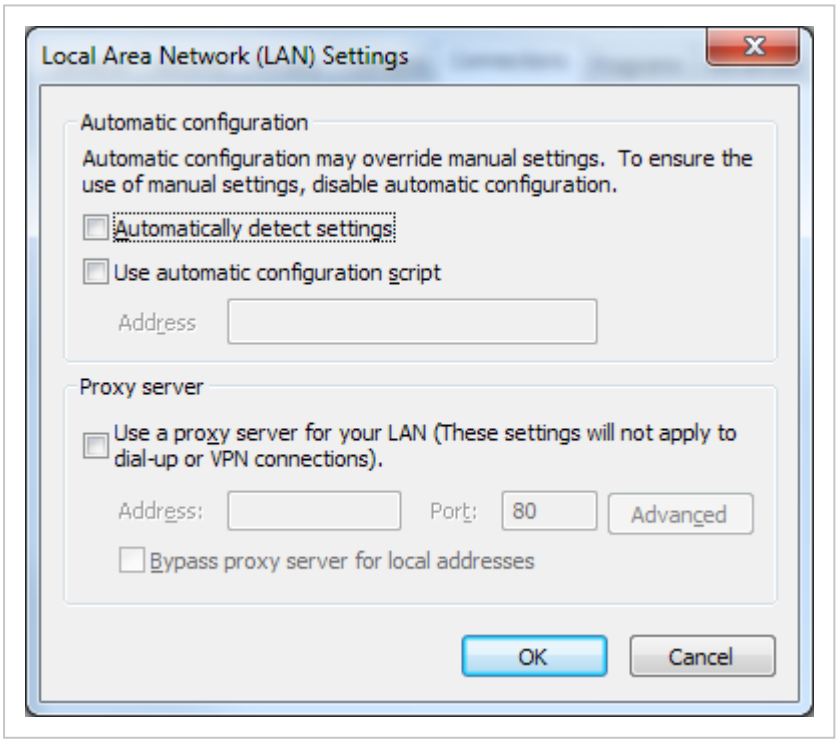
Optimizing performance and user experience

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

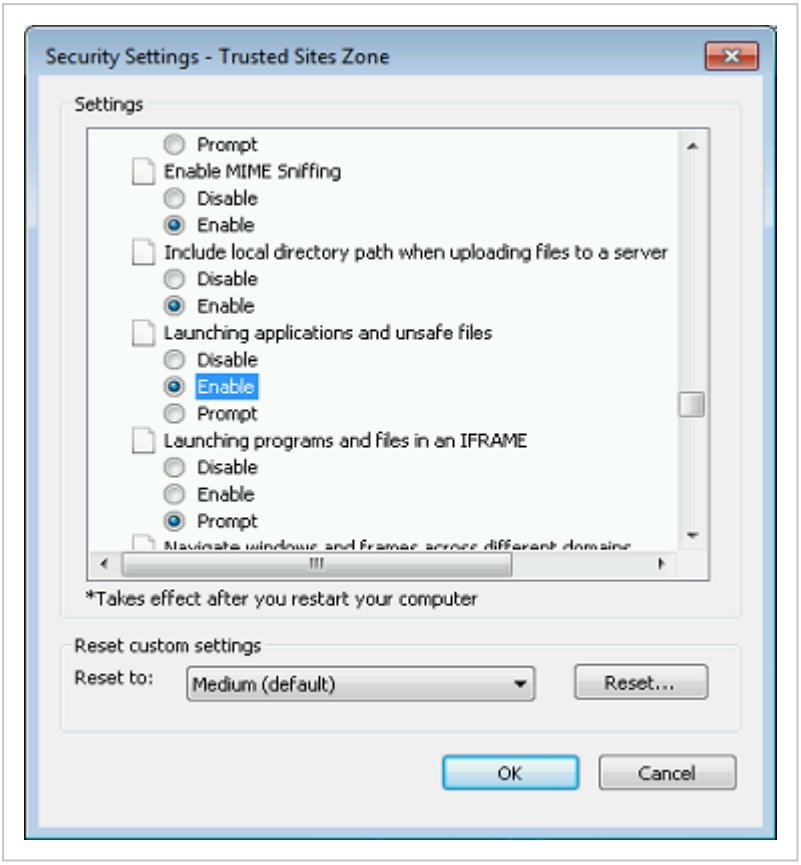
The WebDAV protocol is based on http, can run over https, and Internet Security zones therefore apply to WorkZone Explorer. To ensure the best user experience and optimal performance, the WorkZone Explorer host name must be configured correctly in the Internet Security Zones.

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.



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]).[Exten-
sion]
```

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://d-b01.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 943280. Follow the instructions listed under **Registry information** in the **Resolution** section.

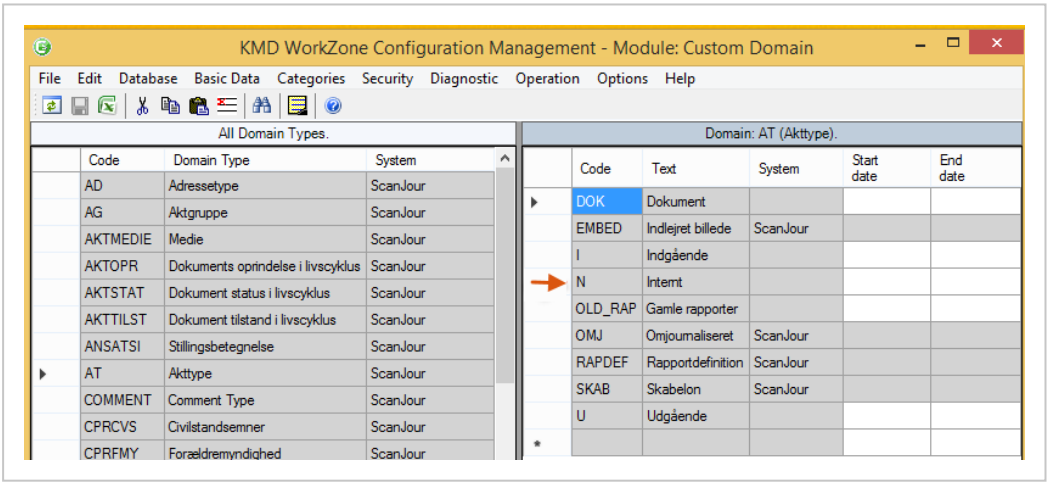
Note:

- 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 as a custom domain and that the `DefaultRecordType` parameter is set to **N** in the web.config file. Please check if this document type has been created in WorkZone Configuration Management and in the WorkZone web.config file.

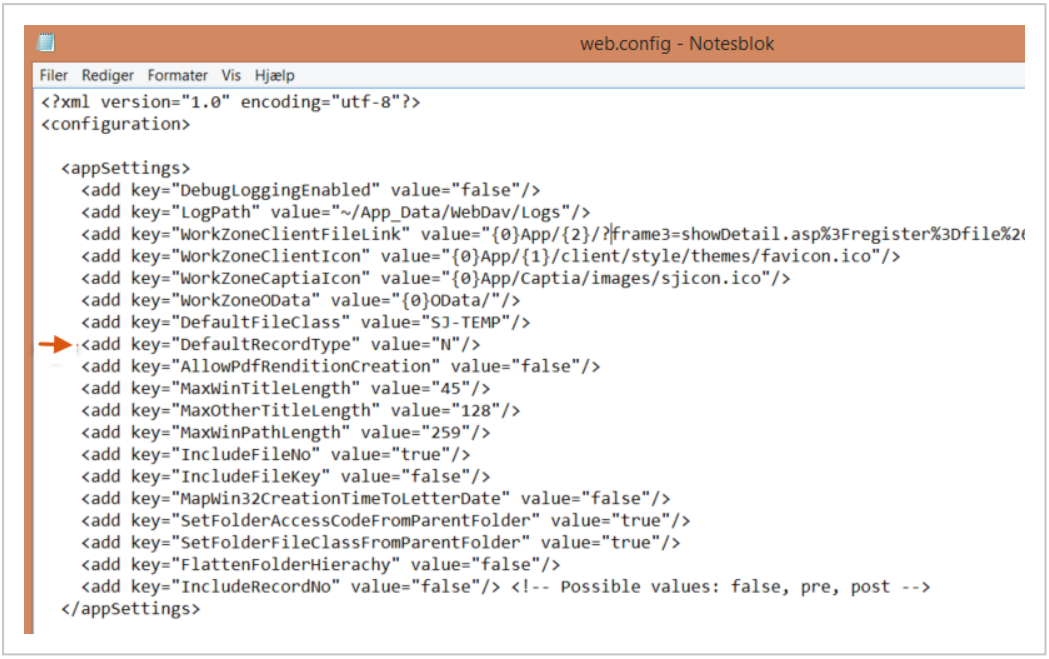
1. Check if the document type is created in WorkZone Configuration Management. Click **Basic data** > **Custom Domain**.



   If the document type **N** does not exist as a custom domain, you must create it. For more information about creating custom domains, see the Configuration Management Online Help.

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**, you need to

specify 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.

Install WorkZone Client

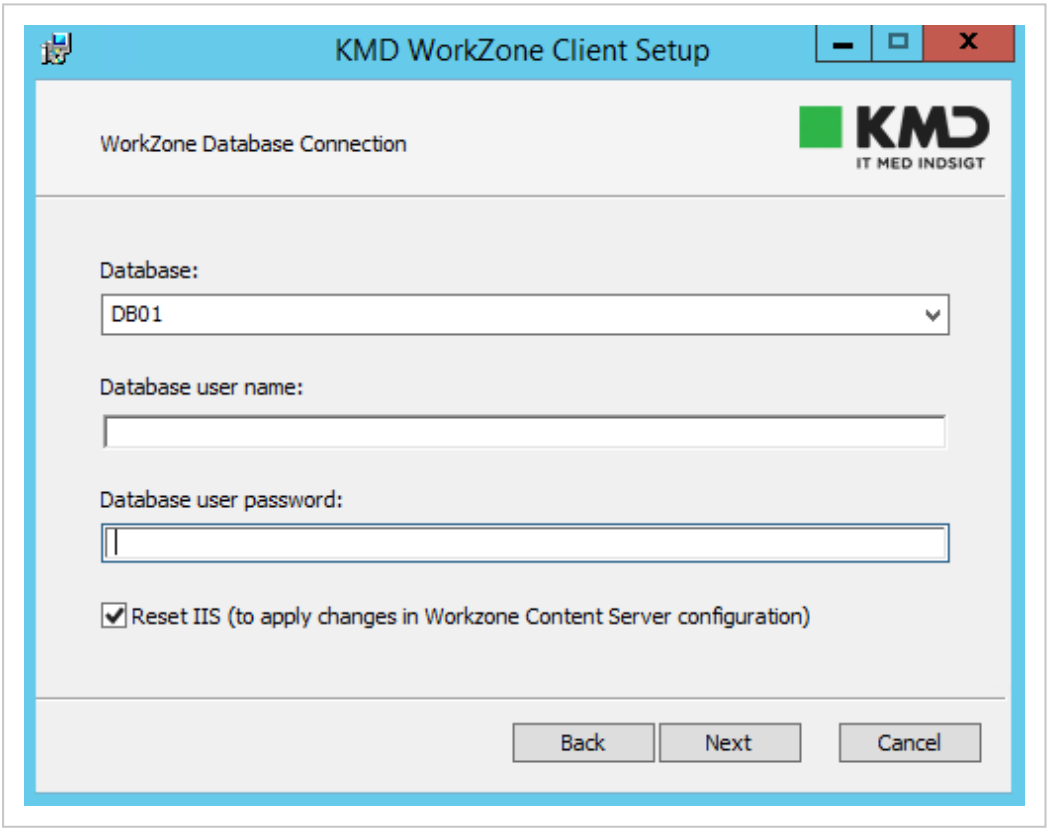
Install WorkZone Client on a single database

> **Prerequisite:** To install WorkZone Client, you must have administrative rights on the local machine.

Manual installation

1. Double-click the `KMD WorkZone Client.msi` file. The **KMD WorkZone Client Setup Wizard - Welcome** page is displayed.
2. Click **Next**. The **End-User License Agreement** page is displayed.
3. Read the license agreement, select the **I accept the terms in the License Agreement** check box and then click **Next**. The **Custom Setup** page is displayed.
4. On the **WorkZone Database Connection** page, you can view a list of Oracle database names on which WorkZone Content Server has been installed. Select the needed Oracle database from this list and then enter your credentials for database access. By default, the IIS (Internet Information Services) will be restarted. If you need to skip the IIS restart, clear the **Reset IIS** check box.

   Click **Next**.



5. On the **Ready to Install KMD WorkZone Client** page, click **Install**.
6. After installation, the **KMD WorkZone Client Setup Wizard Completed** page is displayed. Click **Finish**.

Silent installation

In the command line, execute the following command:

```
msiexec /i "KMD WorkZone Client.msi" DB_NAME=<db_name> USER_NAME-
E=<user> PASSWORD=<password> /qb
```

Where:

- `<DB_NAME>` is the name of the Oracle database.
- `<USER_NAME>` and `<password>` are the credentials to the database.

Example:

```
msiexec /i "KMD WorkZone Client.msi" DB_NAME=db01 USER_NAME-
E=user1 PASSWORD=12345 /qb
```

Install WorkZone Client on several databases

You can install WorkZone Client on several databases and support the user access to these databases through the same client. For each database you need to perform a new instance of WorkZone Client installation, that is, to run the `KMD WorkZone Client.msi` file.

On the server, you can install up to 50 instances of WorkZone Client on different databases.

Every installed instance of WorkZone Client will be listed in **Programs and Features** with a database name in the title. For example, `KMD WorkZone Client - db01`, `KMD WorkZone Client - db02`, and so on.

Manual installation

1. Run a new instance of the WorkZone Client installation (that is, run the `KMD WorkZone Client.msi` file).
2. Follow steps 2-6 of the manual installation on a single database. Note that at step 4 you need to provide a different database name each time when you install WorkZone Client on a different database.

Silent installation

To install WorkZone Client on several databases from a command line, execute the following command for each database:

```
msiexec /i "KMD WorkZone Client.msi" DB_NAME=<db_name> USER_NAME-
E=<user> PASSWORD=<password> MSINEWINSTANCE=1 TRANSFORMS-
S=:Instance<instance_number> /q
```

Where:

- <DB_NAME> is the name of the Oracle database.
- <USER_NAME> and <PASSWORD> are the credentials to the databases.
- <instance_number>, from 0 to 49, is the number of the WorkZone Client installation instance.

Code example:

In this example, two databases (db01 and db02) are installed on a web server. To enable users to access data from these databases, an administrator installs two WorkZone Client instances. To do this, the following commands are executed:

```
msiexec /i "KMD WorkZone Client.msi" DSN_NAME=Client DB_NAME-
E=db01 USER_NAME=user1 PASSWORD=12345 MSINEWINSTANCE=1
TRANSFORMS=:Instance0 /qb
```

```
msiexec /i "KMD WorkZone Client.msi" DSN_NAME=Client DB_NAME-
E=db02 USER_NAME=user2 PASSWORD=67890 MSINEWINSTANCE=1
TRANSFORMS=:Instance1 /qb
```

Now users can access data from both databases.

Install WorkZone Configurator

Install WorkZone Configurator

Manual installation

1. Double-click the `KMD WorkZone Configurator Setup.msi` file. The **Welcome to the KMD WorkZone Configurator Setup Wizard** page is displayed.
2. Click **Next**. The **KMD – End User License Agreement** page is displayed.
3. Read the license agreement, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
4. On the **Ready to Install KMD WorkZone Configurator** page, click **Install**.
5. After installation, the **Completed the KMD WorkZone Configurator Setup Wizard** page is displayed. Click **Finish**.

Silent installation

In the command line, execute the following command:

```
msiexec /i "KMD WorkZone Configurator Setup.msi" /qb
```

WorkZone Configurator on multiple databases

Once you install WorkZone Configurator on the web server, it will work on all databases installed on this web server and will support the user access to these databases through the same client.

Repair the installation

You can repair a damaged installation at any given time in one of the following ways:

- Right-click the.msi file, and then select **Repair**.

  -or-

- Run the.msi file, and then select **Repair**.

  -or-

- Go to **Programs and Features**, select **KMD WorkZone Configurator**, and then select **Repair**.

Install WorkZone Configuration Management

When a new version of WorkZone Configuration Management has been installed on the server, and you try to open it locally, access is denied and you must install the new version on your PC.

The WorkZone Configuration Management program file is called `Scanjour.Sysadm.exe`.

Install WorkZone Configuration Management

1. Start Microsoft Internet Explorer.
2. In the address field, enter the address:
   `https://<database name>/ConfigurationManager/Client/`

   for example:
   `https://db01/ConfigurationManager/Client/`

   Press **Enter**.

   The **InstallShield One-Click Install – KMD WorkZone Configuration Management Setup** page displays.
3. Click **Install**.
   The **Installshield Wizard** page displays, and WorkZone Configuration Management is installed.
4. After successful installation, close Internet Explorer.

Note: If you run Internet Explorer 11, make sure to switch on compatibility view before you start the installation of WorkZone Configuration Management. Click **Tools** > **Compatibility View settings** and add `https://<database name>` to Compatibility View.

Open WorkZone Configuration Management

1. Click **Start** > **All programs** > **KMD** >**Configuration Management**.

   WorkZone Configuration Management opens with the **Logon** dialog box on top. The location of the latest database you logged on to is displayed in the **Database location** field.

2. Enter a different database location, or click **OK**.

Log on from another domain

You can configure WorkZone Configuration Management so that it is possible to log on from a client that is not part of the same domain as the server where WorkZone Configuration Management is installed. This is done by making a change in the `Scanjour.Sysadm.exe.config` file, which adds fields for entering credentials in the **Logon** dialog box.

1. From `C:\Program Files\KMD\WorkZone\ConfigManager`, open the `Scanjour.Sysadm.exe.config` file in Notepad and search for the tag `<applicationSettings>`.
2. Set the value to **True**:

   ```
   <setting name="LogonWithPassword" serializeAs="String">
   <value> True </value> </setting>
   ```

3. Save the file.
4. Start WorkZone Configuration Management and enter your logon credentials (User name, password and Domain) in the **Logon** form.

Verify the publisher

The installation might be interrupted by a security warning saying that “Windows has blocked this software because it can’t verify the publisher”.

To solve this, add the publisher to the trusted sites list.

Log file

When WorkZone Configuration Management is installed, the log file `%temp%\WZCM.log` is created. If errors occur during the installation, you can look in this log file.

Install and configure WorkZone Process

You must complete the following processes to install and configure WorkZone Process on the server.

See also Troubleshooting.

Install and configure WorkZone Process

To run WorkZone Process you need to complete the following procedures.

Install WorkZone Process

Important:

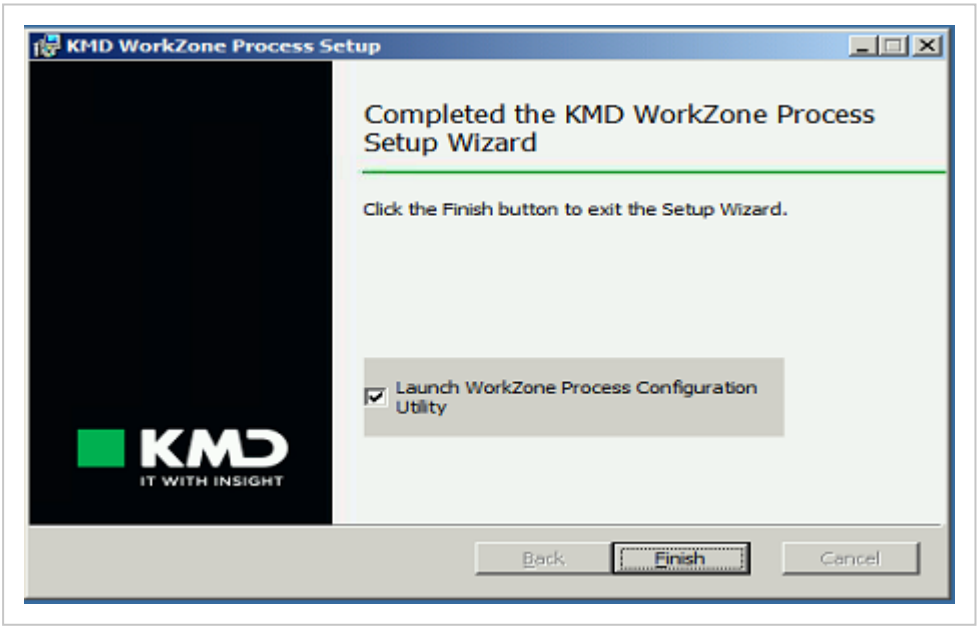
- Run the WorkZone Process installer on both the agent server and on all web servers.

- Always run the WorkZone Process configurator after installation because the WorkZone Process installer only copies files to the server. It does not do any setup of services, IIS, and so on.

Install WorkZone Process

1. Double-click the `KMD Process Setup.msi` as administrator to start the **KMD WorkZone Process Setup** wizard, and click **Next**.
2. On the **End User License Agreement** page, read the license agreement, and select the **I accept the terms in the license agreement** check box. Click **Next**.
3. On the **Ready to install KMD WorkZone Process** page, click **Install**.
4. The **Completed the ScanJour WorkZone Setup Wizard** page opens. All files that are required to configure and run WorkZone Process are copied to the server.

   The next step is to Configure WorkZone Process. Click **Finish** and the **KMD WorkZone Process Configuration Wizard** will start immediately.



If you want to proceed with the configuration later, clear the **Launch WorkZone Process Configuration Utility** check box, and then click **Finish**.

Command line installation

To install, type the following command:

```
msiexec.exe /i KMD Process Setup.msi /qn /l*v install.log
```

Configure WorkZone Process

You use the **WorkZone Process Configuration Wizard** to configure process packages and service workflows.

> **Important:** The wizard removes any previous configurations when you run it.

1. Start the **KMD WorkZone Process Configuration Wizard** in one of the following ways:

    - In the **KMD WorkZone Process Setup Wizard**, select the **Launch WorkZone Process Configuration Utility** check box. See Install WorkZone Process.

        -or-

    - From C:\Program Files (x86)\KMD\WorkZone\Process\Bin or C:\Program Files\KMD\WorkZone\Process\Bin, double-click `Scan-jour.Process.Configurator.exe`.

    The **KMD WorkZone Process Configuration Wizard** opens.

2. On the **Welcome** page, select a role, **Web**, **Agent**, or **DBOnly**, depending on what you want to configure, and then click **Next**.

    - Select **Web**, if you want to install and configure process packages and process service workflows on a web server.

        - **Process services in IIS** - Installs the process site and service workflows in IIS.
        - **Process Packages** - Installs the packages that you select later in this wizard.

- **Asset Update Service** - If there are database changes, this service ensures that the changes will be downloaded to the web server.
- **Process module in WorkZone Configurator** - Makes process settings available from the **Process** menu in WorkZone Configurator.

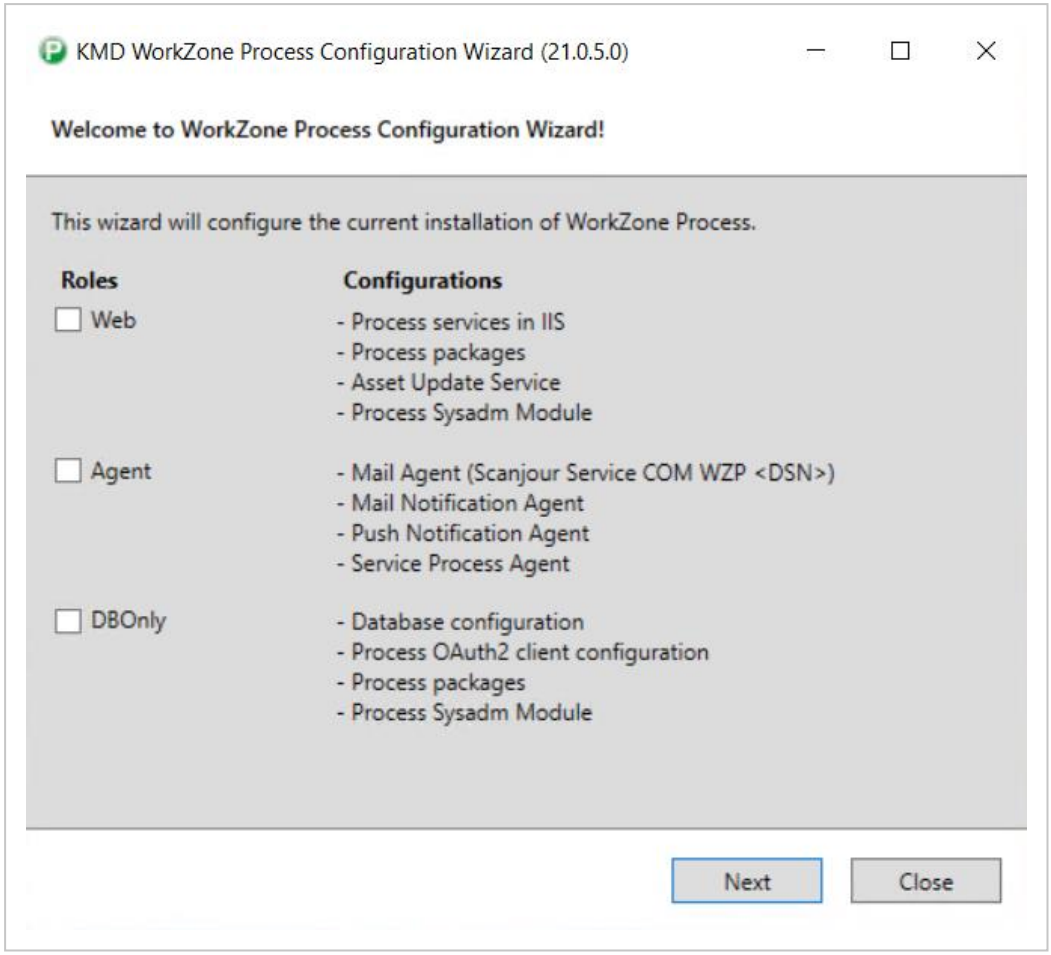
- Select **Agent**, if you want to install service workflows and configure agents on an agent server.

  - **Mail Agent (Scanjour Service COM WZP <DNS>)** - Handles sending of smartmails.
  - **Mail Notification Agent** - Handles sending of notifications by email.
  - **Push Notification Agent** - Handles sending of push notifications to mobile devices.
  - **Service Process Agent** - Enables service workflows, such as Mailbox Monitor, F2 Requisition Handler, and e-Boks Message Handler.

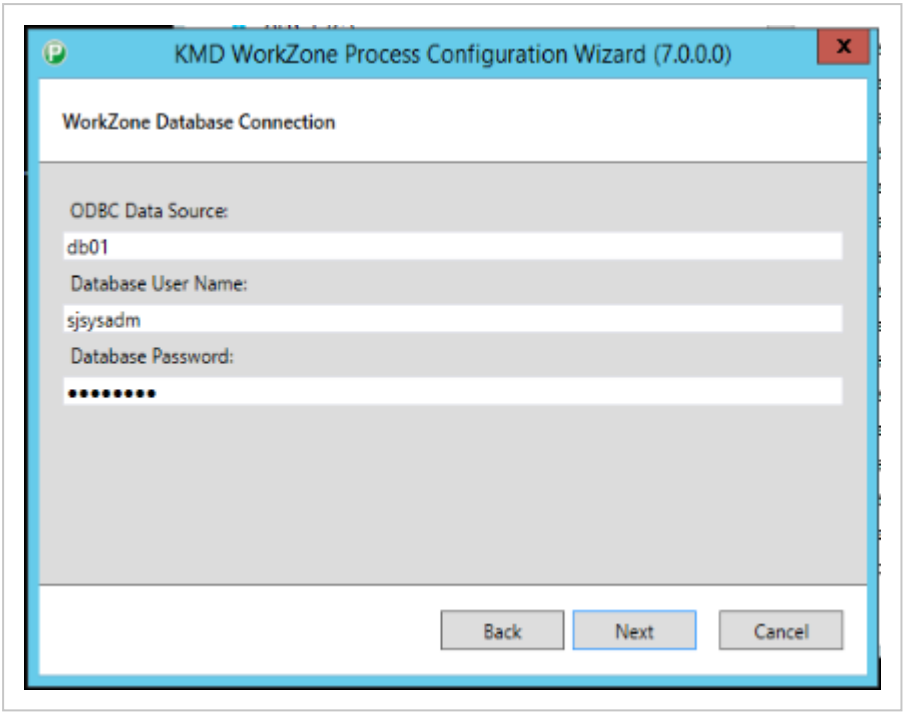
    All services are installed. You can stop a service in Windows Services, if you do not need it.

- Select **DBOnly** as the only role, if you just want to configure the database for WorkZone Process. You cannot select this role in combination with the web and agent roles.

  - **Database configuration** - Executes configuration sql scripts.
  - **Process OAuth2 client configuration** - Configures an OAuth2 client for WorkZone Process.
  - **Process packages** - Loads process packages into the database.
  - **Process SysAdm Module** - Loads dependencies for managing process settings into the database.



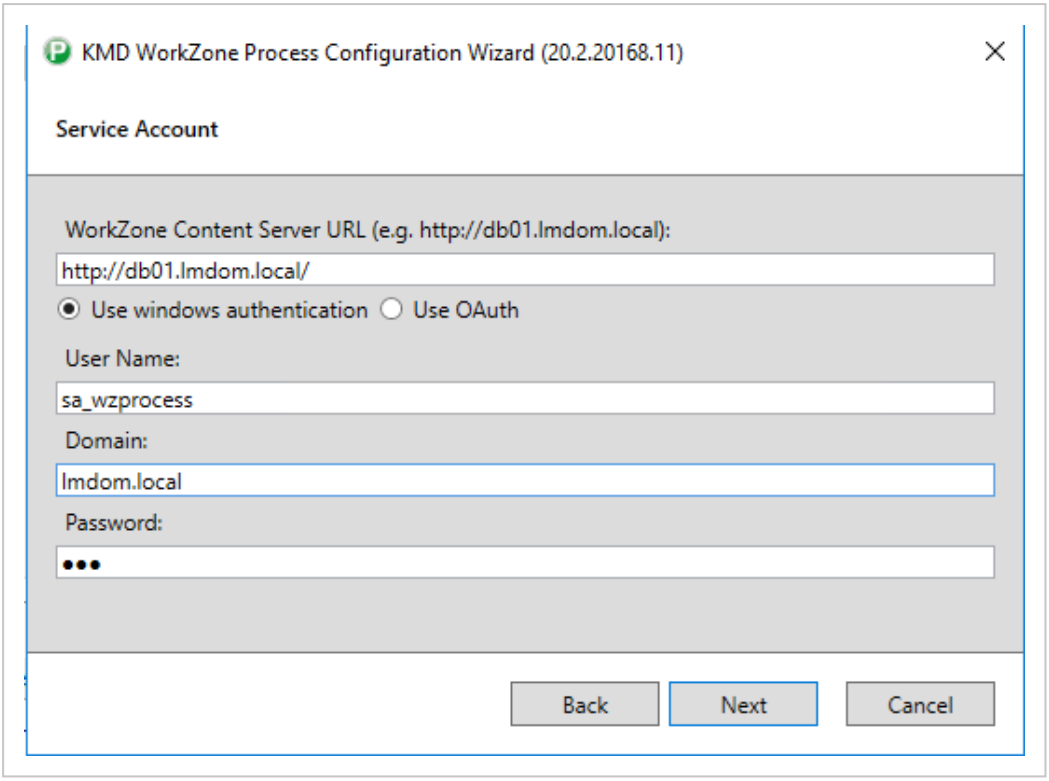
3. On the WorkZone **Database Connection** page, enter the name of the database and the credentials, and then click **Next**.



4. On the **Service Account** page, enter the WorkZone Content Server URL.
5. Select the **Use Windows authentication** check box or the **Use OAuth** check box depending on the authentication method you want to use. See the examples below.

Use Windows authentication

- **WorkZone Content Server URL**: https://db01.lmdom.local
- **User Name**: sa_wzprocess
- **Domain**: lmdom.local
- **Password**: Password of the service user.

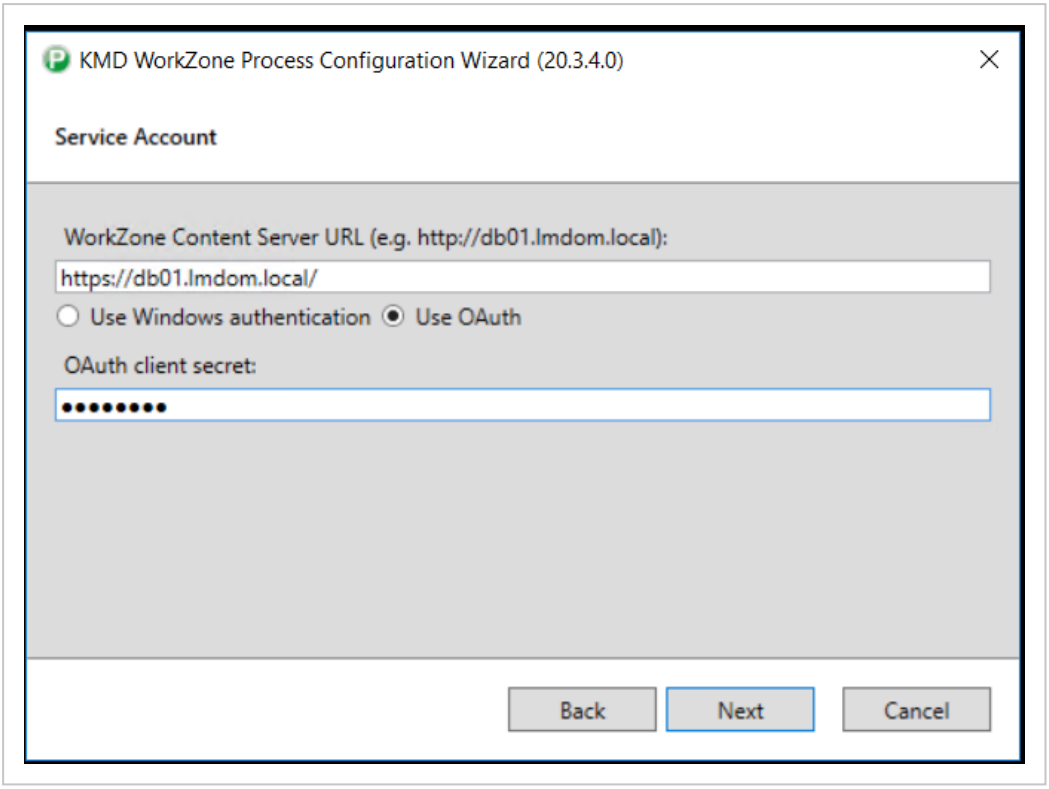


The host should be a Domain Name System (DNS) that can be accessed from all clients.

Use OAauth authentication

WorkZone Content Server must be configured to run with OAuth authentication. See The OAuth2 framework and Install WorkZone Content Server.

- **WorkZone Content Server URL**: https://db01.lmdom.local
- **OAuth client secret**: <A password>



You can see the WorkZone Process OAuth client configuration in WorkZone Configurator. See OAuth2 settings in the WorkZone Configurator Administrator Guide.

If the WorkZone Process OAuth client is already configured, and you don't know the existing client secret, you have two options:

- Delete the existing WorkZone Process OAuth client from WorkZone Configurator and re-configure WorkZone Process with a new client secret on all servers.
- Overwrite the existing WorkZone Process OAuth client with a new client secret in WorkZone Configurator and reconfigure WorkZone Process on all servers with the new secret.

> Important: After completion of the WorkZone Process Configuration Wizard, verify that **Anonymous Authentication** is enabled for the **Process** site in the IIS Manager if you use OAuth authentication.

6. On the **Smartmail** page, fill in the fields depending on how you want WorkZone Process to handle sending of smartmails and email notifications via Exchange On-Premises or Exchange Online.

   If you select the **Use autodiscover of Web Services URL** check box, and autodiscover for Exchange is set, and your service account user is mapped to an Exchange user, you can click **Next** without making any changes on this page. See Exchange prerequisites and Service accounts.

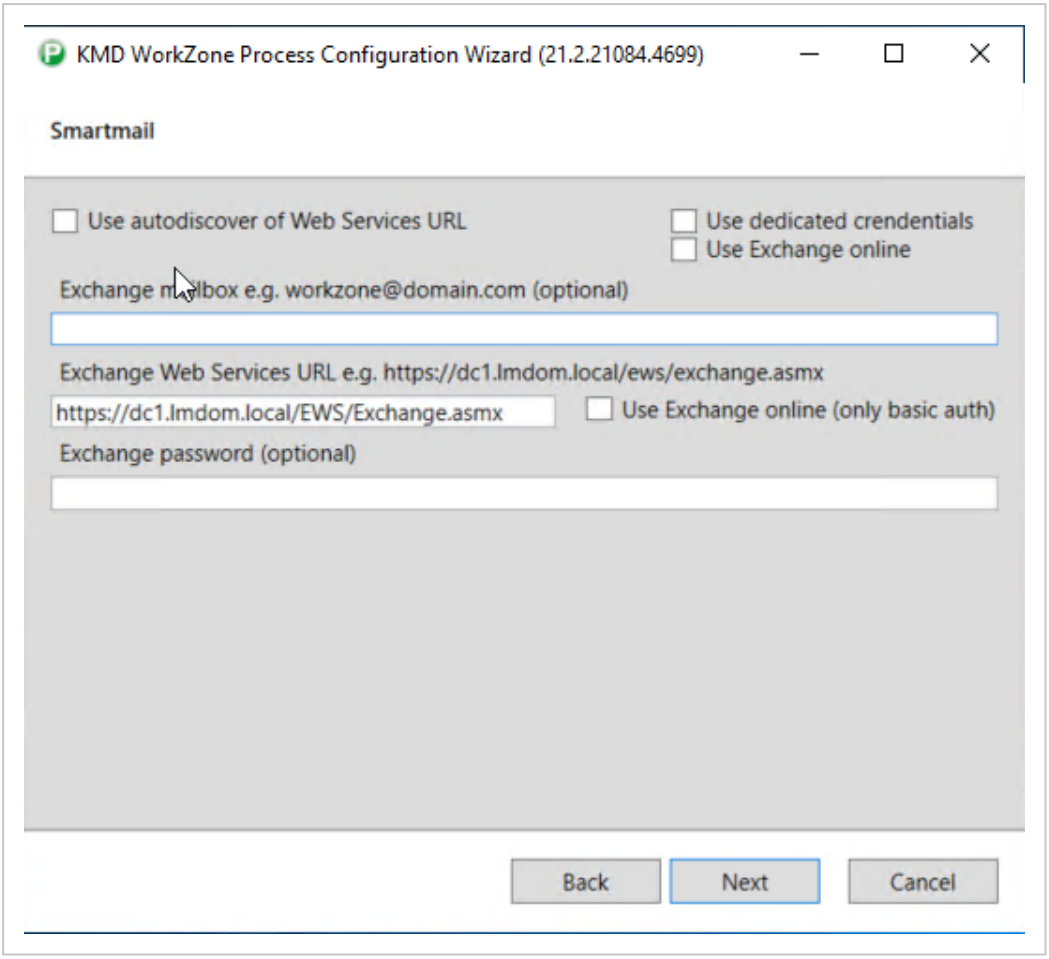
   > **Note:** You cannot use the autodiscover option, if you have configured WorkZone Process to use OAuth authentication. You must enter dedicated credentials for the user name, password, domain, and URI. See Dedicated credentials.

   You can configure Exchange in different modes.

   Service account user

   In this mode, Exchange will be configured to use the credentials of the service account user. The mail agents will use this account to connect and send emails.

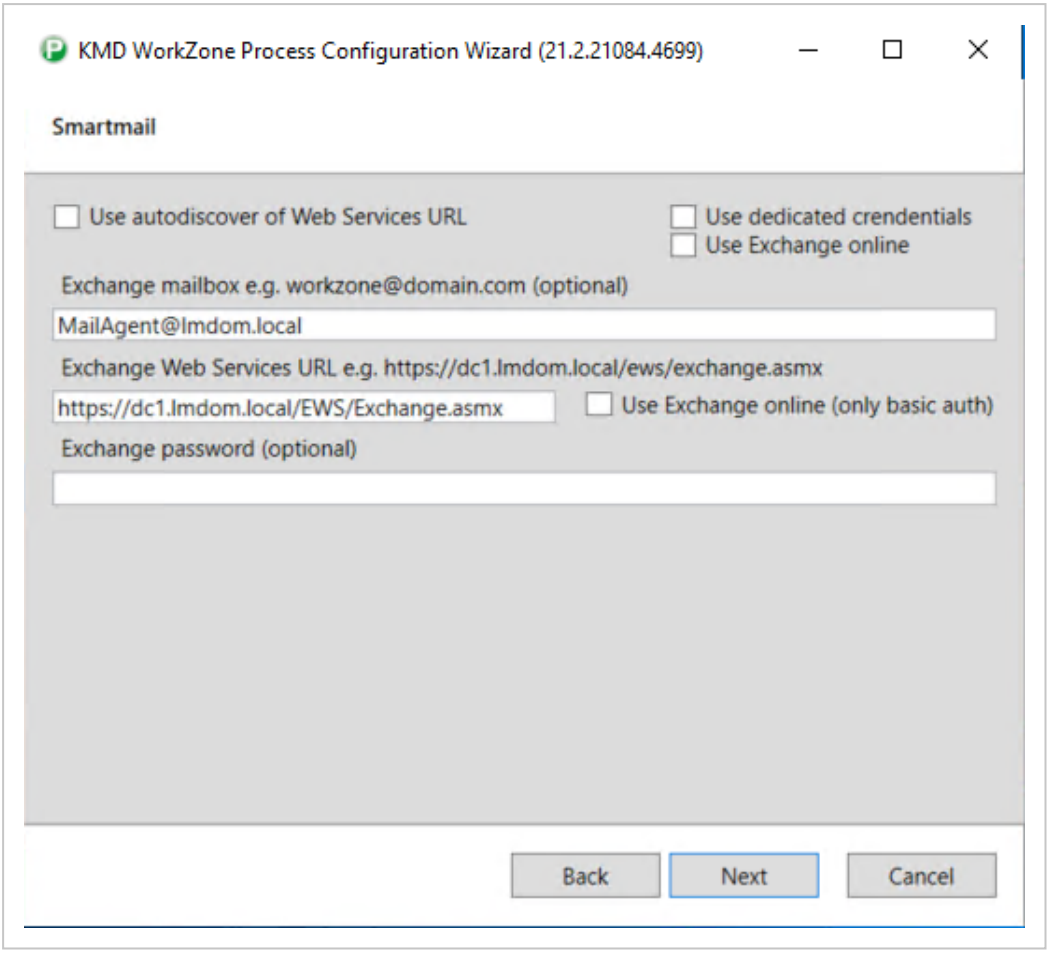
   To activate this mode, fill in the **Exchange Web Services URL** field.



Service user account on behalf

This mode is the same as the Service account user mode except that when the mail agent sends emails, the emails will be sent on behalf of the email account specified in the **ExchangeMailbox** field.

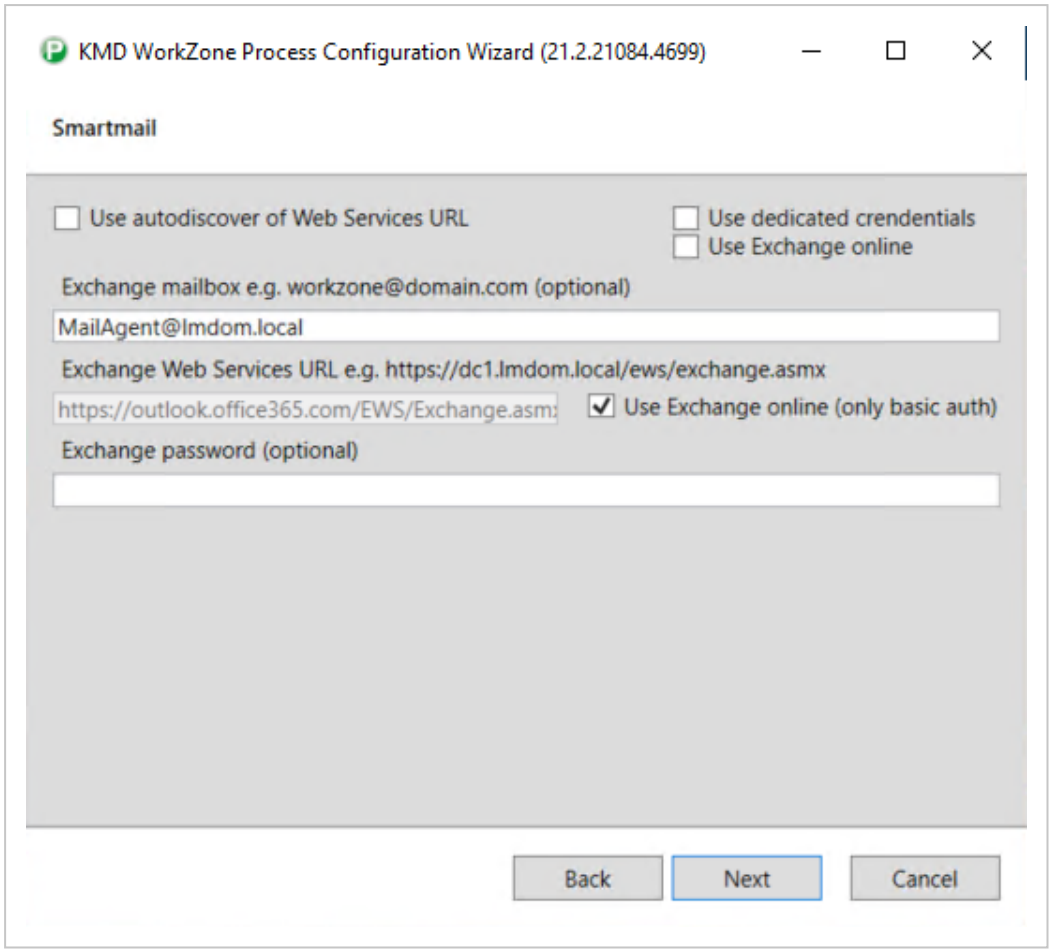
To activate this mode fill in the **Exchange mailbox** and the **Exchange Web Services URL** fields.



Mailbox credentials

In this mode, the account specified in the **Exchange mailbox** field together with the **Exchange password** field is used as credentials for accessing the Exchange server when the mail agents send emails. This mode is typically used for accessing Exchange Online but it can also be used for a different On-Premises account.

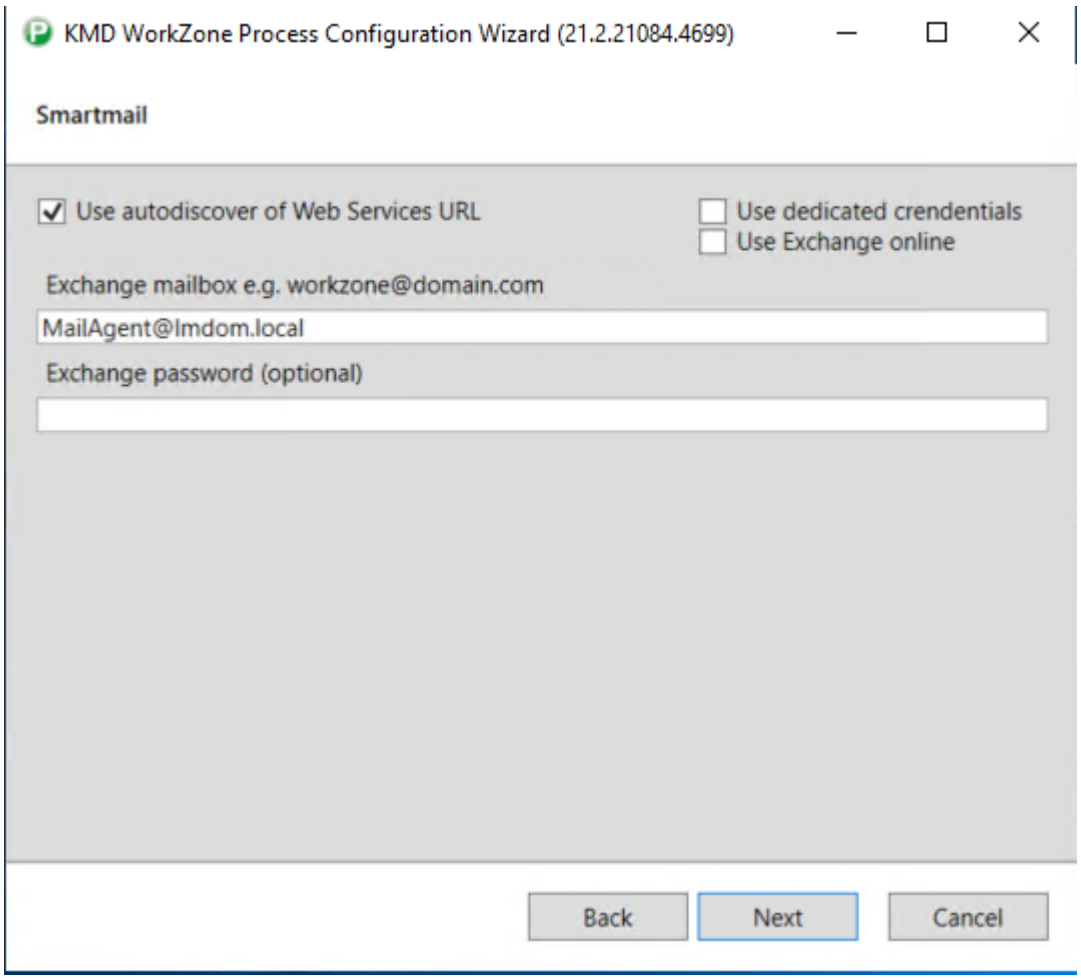
To activate this mode, fill in the **Exchange mailbox**, the **Exchange Web Services URL**, and the **Exchange password** fields.



Use autodiscover of Web Services URL

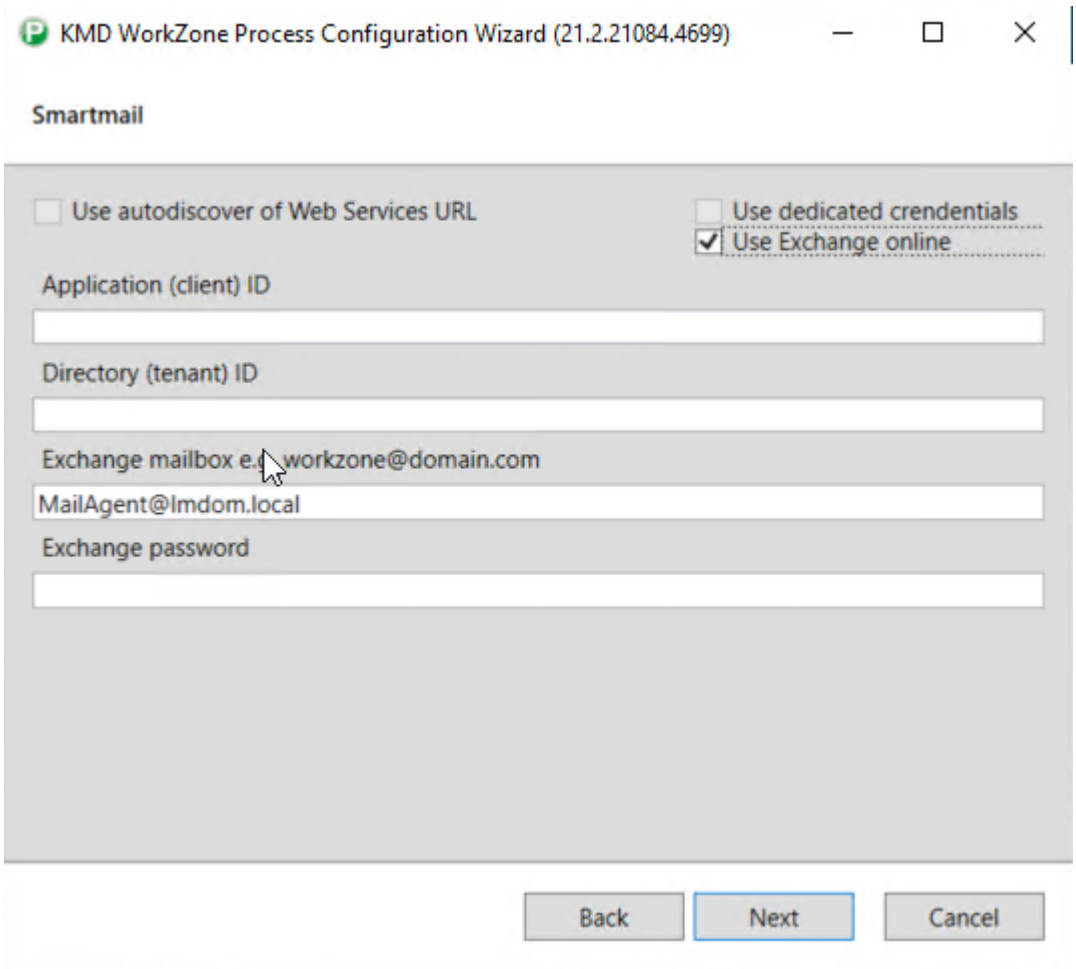
If you select the **Use autodiscover of Web Services URL** check box, you do not need to fill in the **Exchange Web Services URL**. This field will be filled in automatically using the Exchange autodiscover service, if it is available.

The mail agents will use the autodiscover service to find the Exchange endpoints every time the services are started.



Use Exchange Online

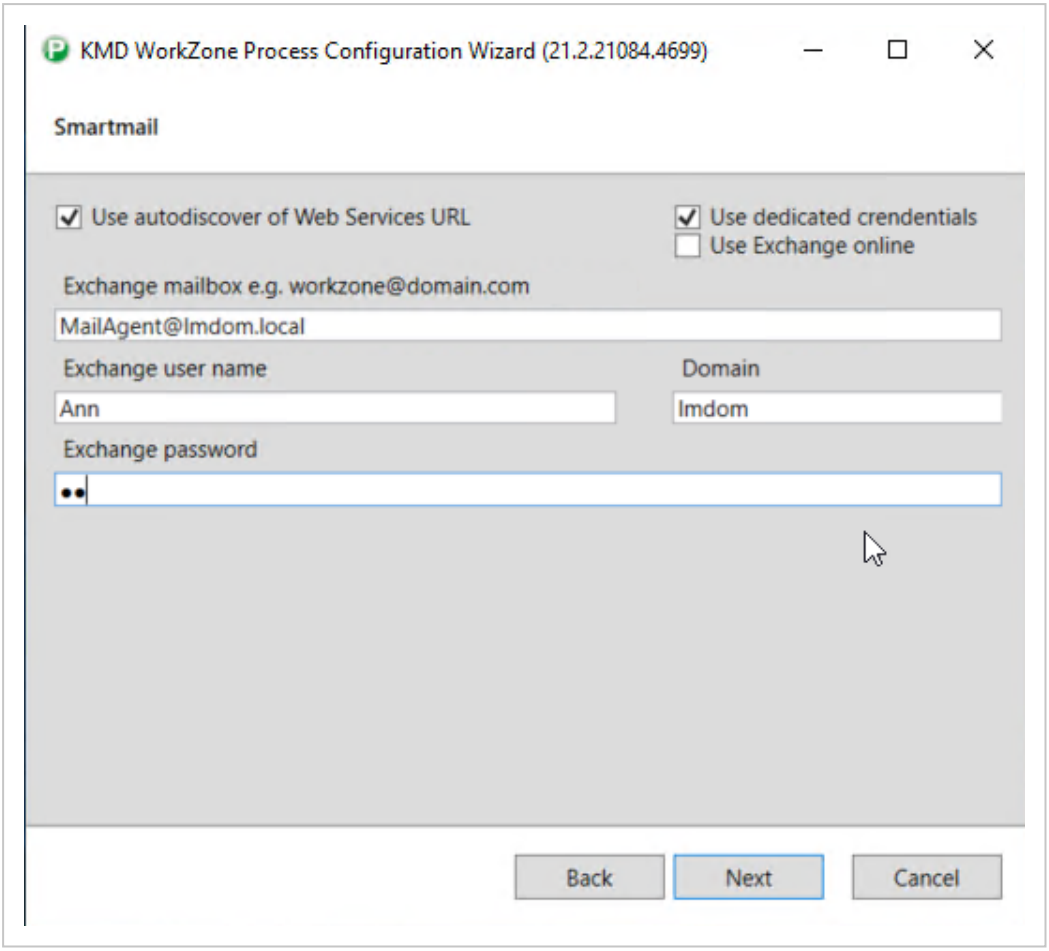
If you select the **Use Exchange Online** check box, the **Use autodiscover of Web Services URL** and the **Use dedicated credentials** check boxes will be disabled, and you must fill in the GUIDs in the **Application (client) ID** and **Directory (tenant) ID** fields and email address and password in the **Exchange mailbox** and **Exchange password** fields.



Dedicated credentials

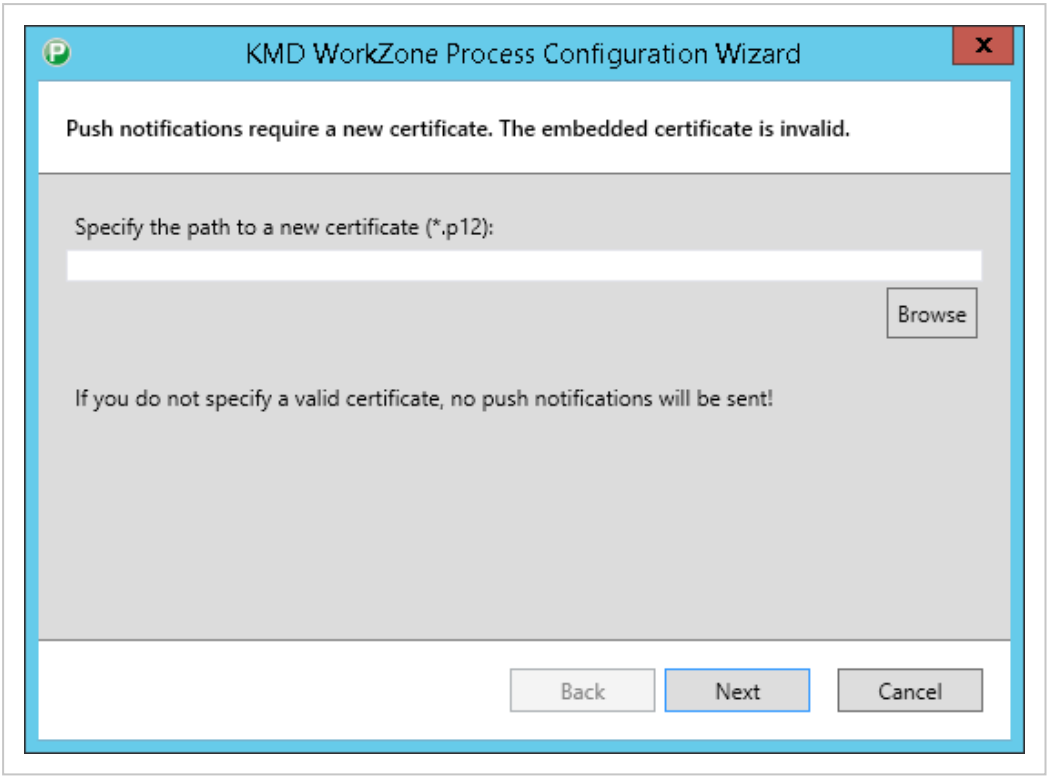
You can use dedicated credentials if you want to use a different specific user account. If you select the **Dedicated credentials** check box, you must fill in the **Exchange user name**, the **Domain** and **Exchange password** fields.

In the example, a local user account is used as the exchange account for the mail services.



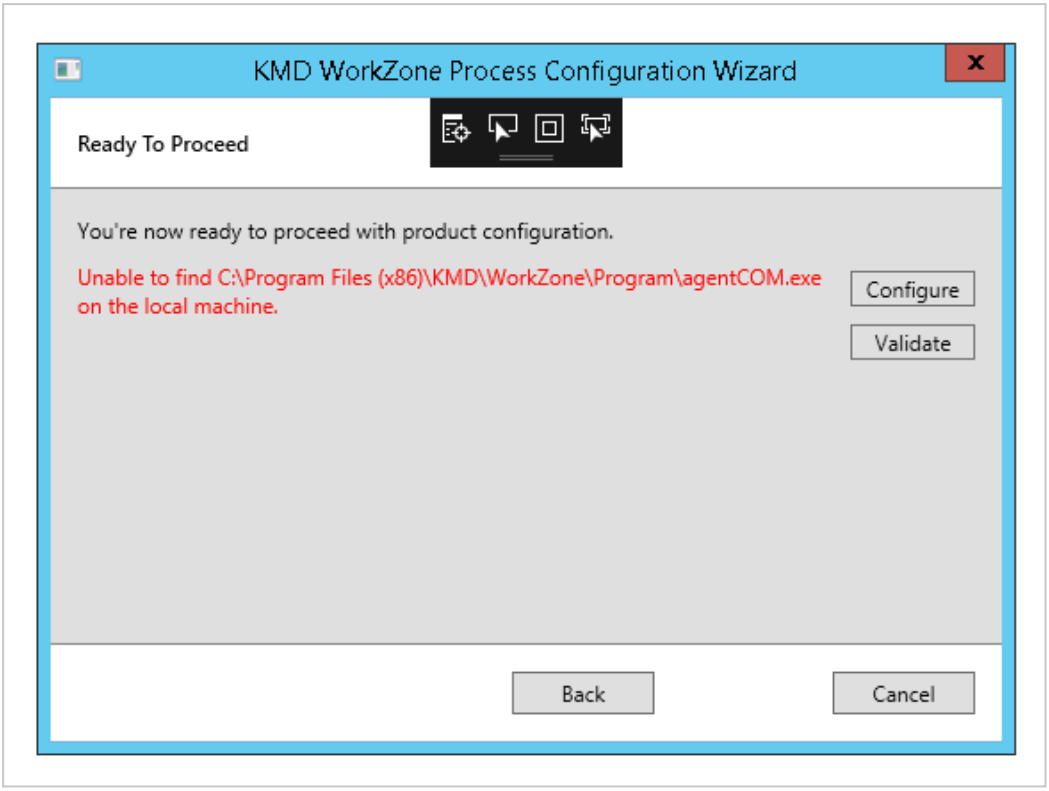
7. On the **Push notifications require a new certificate** page, click **Browse** to select a valid certificate and then click **Next**. If the certificate expires, push notifications will no longer be sent.

   This page only appears if the current mobile certificate is no longer valid.

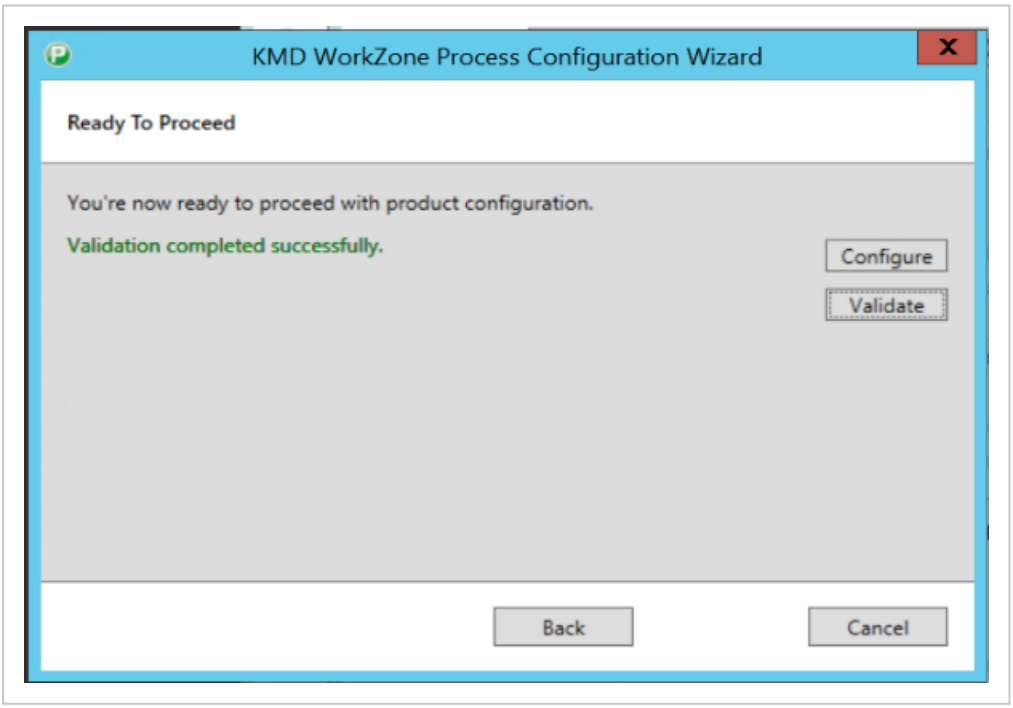


8. On the **Ready To Proceed** page, you can choose to validate prerequisites or start the configuration right away:

   - Click **Configure** to start the configuration. The WorkZone **Configuration Wizard** removes any previous configurations before applying your configurations.
   - Click **Validate**, if you want to validate that prerequisites and features connected with the specific role are in place before you start the configuration. If some pre-requisites or features are missing, error messages will be listed.



If all prerequisites are in place, you will see the message *Validation completed successfully*, and you can then click **Configure** to start the configuration.



What is validated?

Prerequisites (always validated)

- WorkZone Content Server is installed.
- Correct version of WorkZone Content Server is installed.
- SQL*Plus is installed (sqlplus.exe exists).
- CaptiaLoadDataDict is installed (loaddatadict.exe exists).
- At least one role is selected.
- Database connection.
- WorkZone Configurator version is not older than the installed version of WorkZone.
- The specified service account user name (usually sjserviceagentuser4) exists in the specified domain (for example, `lmdom`) on the Service Account page.
- The service user (usually sjserviceagentuser4) has been granted the 'Log OnAsService' privilege
- The connection to WorkZone Content Server.
- The executing user exists in the database/the user is a WorkZone user. Validates if the user exists in the **Users** table.

Agent role validation

- The connection to the Exchange server.
- AgentCOM is installed (agentCOM.exe exists).
- Valid certificate for the Push Notification Agent.
- Access to Apple Push Notification Service.
- Notification Agent Host is installed (Scanjour.Process.Notification.AgentHost.exe exists).

Web Role validation

- Correct version of IIS is installed.
- The WorkZone site and OData services exist in IIS.

Command line configuration

You can configure process packages using command line parameters. The parameters that are used in the command line depend on the selected role.

Cross Origin Resource Sharing (CORS)

If WorkZone Process services are to be requested from web clients executed by a web browser and loaded from other domains (for example WorkZone Client and WorkZone Configurator applications hosted on a different host than Process service), you must configure the Cross-Origin Resource Sharing parameters (**AllowedCORSOrigins** and **AllowedCorsHeaders**).

See the list below for an overview of parameters and roles.

General configurations

Parameter	Role	Description	Required/Optional
-quiet	All	Runs the Configurator without displaying the user interface.	Optional
-verbose	All	Displays progress information during configuration. The verbose mode is only relevant to use together with the quiet mode.	Optional
-remove	All	Removes the configuration.	Optional
-val	All	Validates specific roles and their associated features. No configuration will be done.	Optional
-log:C:\1.log	All	Name and destination of log file. Logs output from the Configurator to the log file.	Optional

Parameter	Role	Description	Required/Optional
Roles	All	Specifies which role to configure. Roles are: `All`, `Web`, `Agent`, `Web;Agent`, and `DBOnly`. The `All` and `Web;Agent` values are the same. `Web;Agent` is the default value. In the WorkZone Process Configuration Wizard, only the `Web`, `Agent`, and `DBOnly` options are available. For example, if you do not provide the **Roles** parameter using command line configuration, and you execute the configurator in user interface mode, the wizard will open the start page with the **Web** and **Agent** options selected corresponding to the default value `Web;Agent`. ### DBRole Select the `DBOnly` role, if you only want to configure the database. `Roles="DBOnly"` **Note:** You cannot select the `DBOnly` role in com-	Optional

Parameter	Role	Description	Required/Optional
		bination with other roles. If you select a wrong set of values and launch the WorkZone Process Configuration wizard in quiet mode, it will return an error message. The correct values for the **Roles** parameter are: `ALL`, `Web`, `Agent`, `Web;Agent`, and `DBOnly`. **Example**: `Roles="DBOnly"`—to configure the database. `Roles="Web;Agent" SetupDatabase=false`—to configure everything else except the database.	
IgnoreCertificateErrors	All	Configures all process workflows and ignores certificate errors.	Optional
DataSourceName=<ODBC datasource name>	All	The name of the database.	Required
DatabaseUserName=<name>	All	The user name of the WorkZone database admin-	Required

Parameter	Role	Description	Required/Optional
		istrator. For example, sjsysadm.	
DatabasePassword=<password>	All	The password for the WorkZone database.	Required
ContentServerUri=<url>	All	Link to the WorkZone site. For example, https://d-b01.lmdom.local	Required
Packages=<Extended.wzp>	Web	File name(s) of packages in the Packages folder. The Basis package is always installed. You do not need to specify it.	Optional
SetupDatabase	Database	Configures the database. By default, this parameter is set to `True`. If you set the **SetupDatabase** parameter to `False`, WorkZone Process Configurator will not make any connections to the database. This is relevant, if you do not yet have a database available. Be aware that until a database is available and configured, WorkZone Process will not work.	Optional
ForcePackageLoad	Web	Forces reload of process packages. By default, process packages are only loaded once into the database but in	Optional

Parameter	Role	Description	Required/Optional
		some situations you may want to reload the packages, for example when you install a hotfix.	
PackageLoadTimeout	Web	Controls the timeout for loading a process package. You can specify a time using the time format hh:mm:ss. For example: • 00:05:00 (5 minutes) • 00:00:30 (30 seconds) • 01:00:00 (One hour) If you do not specify this parameter, the default timeout is 5 minutes.	Optional
OAuthClientSecret	All	Secret for the WorkZone Process OAuth client. The client is added automatically by WorkZone Process Configurator. The secret can be any string, but it must be exactly the same for all servers configured with WorkZone Process Configurator. You can see the WorkZone Process OAuth client configuration in WorkZone Configurator. See OAuth2 settings in the WorkZone Con-	Optional

Parameter	Role	Description	Required/Optional
		figurator Administrator Guide. If the WorkZone Process OAuth client is already configured, and you don't know the existing client secret, you have two options: • Delete the existing WorkZone Process OAuth client from WorkZone Configurator and re-configure WorkZone Process with a new client secret on all servers. • Overwrite the existing WorkZone Process OAuth client with a new client secret in WorkZone Configurator and reconfigure WorkZone Process on all servers with the new secret. **Note:** This parameter is required if you use the OAuth authentication method.	

Parameter	Role	Description	Required/Optional
AllowedCorsOrigins	Web	Define which web client applications executed in a browser hosted on other domains will be able to perform CORS requests from the server. An origin for the **AllowedCorsOrigins** parameter[1] must be defined as: <scheme>://[<hostname>.]<host>[:<port>], for example Https://WZClient if the WorkZone Client is hosted on Https://WZClient and the rest of WorkZone services are hosted on another domain, such as Https://WZServices. Origins are separated with semi-colons ";". When using Cross-Origin Resource Sharing (CORS) with WorkZone , this parameter should be set to the specific origins as most browsers will prevent passing credentials or tokens to the service when the wild card (*) is used as the origin. Using the wild card (*) origin means the WorkZone Process service is open for every	

Parameter	Role	Description	Required/Optional
		origin. It is used when the wild card origin (*) is the only origin that is set in the configuration file or in the corresponding system environment variable, or the origin of the request is not found and the **AllowedCorsOrigins** parameter contains the wild card origin (*). **Example**: The following parameter in the Web Config file: <add key="allowCorsOrigin" value="*" /> will fail unless the wild card origin "*" is replaced with the specific origins of the web client to be accessed. The default value if no origins are specified is wild card (*).	
AllowedCorsHeaders	Web	Used in a response to OPTIONS preflight request. Indicates which headers can be used during the actual HTTP CORS request. The **AllowedCorsHeaders** parameter corresponds to	

Parameter	Role	Description	Required/Optional
		Access-Control-Allow-Header response header (ACAH) and acts as an answer to request's Access-Control-Request-Headers request header. The **AllowedCorsHeaders** parameter[1] can be configured with: - "*" The Access-Control-Allow-Header will contain headers requested by the request as well as specific PDF headers. - specified headers (ACAH header will contain these headers as well as specific PDF headers). - both * and specified headers (ACAH will contain headers from the configuration and headers requested by the request as well as specific PDF headers). The default value if no origins are specified is wild card (*).	

[1] These parameters are also mapped to the following system environment variables on the server:

- WORKZONE_PROCESS_CORS_ALLOWEDORIGINS
- WORKZONE_PROCESS_CORS_ALLOWEDHEADERS

System environment variables take precedence over the parameters defined in the web.config files.

Exchange configurations using EWS (Exchange Web Services)

The Exchange configurations depend on whether your organization uses Exchange On-Premises or Exchange Online. The difference between the Exchange Online and On-Premises configurations is the credentials that are used when communicating with the Exchange server. On-Premises communication uses the credentials of the process service account user and the Online communication uses the credentials of the email account.

Parameter	Role	Description	Environment variables	Required /Optional
ExchangeWebServicesUri=<Exchange EWS url>	Agent	The endpoint for the Exchange service, for example: https://dc1.lmdom.ocal/EWS/Exchange.asmx **Note:** This parameter is not required if the UseAutodiscover parameter is set to TRUE.	WORKZONE_PROCESS_EXCHANGE_SERVER_URI	Required
ExchangeMailbox=<mail address>	Agent	The email address of the Exchange user who sends smartmails. If the parameter is not defined, the email address defined in the ServiceUserName parameter is used. For example, mailagent@lmdom.local. **Note:** This parameter is required if the UseAutodiscover parameter is set to TRUE.	WORKZONE_PROCESS_EXCHANGE_MAILBOX	Optional

Parameter	Role	Description	Environment variables	Required /Optional
UseAutoDiscover	Agent	If set to TRUE, Autodiscover is called every time the service starts to resolve the ExchangeWebServicesUri parameter. Default is FALSE **Note:** This parameter is not applicable if you have configured WorkZone Process to use the OAuth authentication method.		Optional
ExchangeUserName=<name>	Agent	The email address of the Exchange user who sends smartmails. If specified, it is used as part of the credential. Note that if you specify a user name, you must also specify a password in the ExchangeUserPassword parameter. **Note:** This parameter is required if you use the OAuth authentication method.	WORKZONE_PROCESS_EXCHANGE_USER_NAME	Optional
ExchangeUserPassword=<password>	Agent	The email address password of the Exchange user who sends smartmails. If the ExchangeUserName para-	WORKZONE_PROCESS_	Optional

Parameter	Role	Description	Environment variables	Required /Optional
		meter is specified, the password is used as part of the credentials. **Note:** This parameter is required if you use the OAuth authentication method.	EXCHANGE_USER_PASSWORD	
ExchangeUserDomain=<domain>	Agent	The domain where the Exchange user is located. If the ExchangeUserName parameter is specified, the domain is used as part of the credentials. If you have specified the domain as part of the ExchangeUserName parameter, leave this parameter empty. **Note:** This parameter is required if you use the OAuth authentication method.	WORKZONE_PROCESS_EXCHANGE_USER_DOMAIN	Optional
ExchangeServerVersion	Agent	Used to identify which version of Exchange is used server side.	WORKZONE_PROCESS_EXCHANGE_VERSION	Optional

Exchange configurations in cloud using Microsoft Graph

WorkZone Process Configurator supports both the public client and client credential authentication flows for Exchange Online with OAuth.

Public client flow

The public client flow corresponds to the configuration that you can set up using the **WorkZone Process Configuration Wizard** where you specify email address and password. See Use Exchange Online.

Azure Active Directory prerequisites

The PublicClient flow requires that an application registration is added in AAD (Azure Active Directory) for the specific tenant and that the **Allow public client flows** option is set for this application on the **Authentication** page on the control panel for the added application. It is also required to add the following delegated permissions for Microsoft Graph:

- Mail.ReadWrite
- Mail.ReadWrite.Shared
- Mail.Send
- Mail.Send.Shared
- User.Read
- User.ReadBasic.All

Parameter	Role	Description	Environment variable	Required /Optional
ExchangeOAuthClientId	Agent	The GUID of the client ID.	WORKZONE_ PROCESS_ EXCHANGE_ CLIENTID	Required
ExchangeOAuthTenantId	Agent	The GUID of the tenant ID.	WORKZONE_ PROCESS_ EXCHANGE_ TENANTID	Required
ExchangeMailbox	Agent	The email address of	WORKZONE_	Required

Parameter	Role	Description	Environment variable	Required /Optional
		the Exchange user who sends smart-mails.	PROCESS_ EXCHANGE_ MAILBOX	
ExchangeUserPassword	Agent	The password of the service user mailbox.	WORKZONE_ PROCESS_ EXCHANGE_USER_ PASSWORD	Required

The client credential flow

This flow is only supported using command line configuration. You cannot use the **WorkZone Process Configuration Wizard**. It is more complex to configure this flow properly to keep the desired security level, and setting the permissions requires setting a higher access level from the AAD administrators. Therefore this is not the recommended flow.

Azure Active Directory prerequisites

The ClientCredentials flow requires that an application registration is added in AAD (Azure Active Directory) for the specific tenant and that the following application permissions are added for Microsoft Graph:

- Mail.ReadWrite
- Mail.Send
- User.Read.All

Furthermore, permissions must be scoped to the desired mailbox accounts to ensure proper security. See: Scoping application permissions to specific Exchange Online mailboxes in the Microsoft documentation.

Parameter	Role	Description	Environment variable	Required /Optional
ExchangeOAuthClientId	Agent	The GUID of the client ID.	WORKZONE_ PROCESS_ EXCHANGE_ CLIENTID	Required

Parameter	Role	Description	Environment variable	Required /Optional
ExchangeOAuthTenantId	Agent	The GUID of the tenant ID.	WORKZONE_PROCESS_EXCHANGE_TENANTID	Required
ExchangeMailbox	Agent	The email address of the Exchange user who sends smartmails.	WORKZONE_PROCESS_EXCHANGE_MAILBOX	Required
ExchangeOAuthClientSecret	Agent	The secret used to access the application in Azure Active Directory.	WORKZONE_PROCESS_EXCHANGE_CLIENTSECRET	Required

Service account configuration parameters (also used by the mail agents)

Parameter	Role	Description	Agent and Web
ServiceUserName=<service user>	Agent and Web	The user name of a WorkZone service account user who can access WorkZone. The credentials of the service account user is used when communicating with the Exchange server if the ExchangeUserName parameter is empty. For example: mailagent@lmdom.local.	Required
ServicePassword=<password>	Agent and Web	The password for the WorkZone service account user. The credentials of the service account user is used when communicating with the Exchange server if the ExchangeUserName parameter is	Required

Parameter	Role	Description	Agent and Web
		empty.	
ServiceDomain=<domain>	Agent and Web	The domain where the WorkZone service account user is located. Anders: The credentials of the service user account is used when communicating with the Exchange server if ExchangeUserName is empty.	Required

Command line configuration examples

When you have installed all options, you can configure the servers. Copy the code examples below to use the code strings as a starting point for the server configurations.

Configure command line - install both roles

The following example can be modified to configure the web.and agent roles.

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName-
e=DB01 DatabaseUserName=sjsysadm DatabasePassword=<password> Con-
tentServerUri=https://db01.lmdom.local ServiceUserName=<service
user> ServiceDomain=<domain> ServicePassword=<password>
ExchangeServerUri=https://DC1.lmdom.local/EWS/Exchange.asmx
ExchangeMailbox=mailagent@lmdom.local Pack-
ages=<Package1.wzp,Package2.wzp> -log:C:\1.log
```

Configure command line - Install agent role only

The following example can be modified to configure the agent role.

```
Scanjour.Process.Configurator.exe -quiet -verbose Roles="Agent"
DataSourceName=DB01 DatabaseUserName=sjsysadm Data-
basePassword=<password> ContentServerUri=https://db01.lmdom.local
ServiceUserName=<service user> ServiceDomain=<domain> Ser-
vicePassword=<password> ExchangeServer-
```

```
Uri=https://DC1.lmdom.local/EWS/Exchange.asmx ExchangeMail-
box=mailagent@lmdom.local -log:C:\1.log
```

Configure command line - Install web role only

The following example can be modified to configure the web role.

```
Scanjour.Process.Configurator.exe -quiet -verbose Roles="Web"
DataSourceName=DB01 DatabaseUserName=sjsysadm Data-
basePassword=<password> ContentServerUri=https://db01.lmdom.local
ServiceUserName=<service user> ServiceDomain=<domain> Ser-
vicePassword=<password> Packages=<Package1.wzp,Package2.wzp> -
log:C:\1.log
```

Use a different user or Exchange server in a foreign domain

To be able to send e-mails from an Exchange server in a foreign domain, add the following parameters `ExchangeUserName:<name>`, `ExchangeUserPassword:<password>`, `ExchangeUserDomain:<domain>`.

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName-
e=DB01 DatabaseUserName=sjsysadm Data-
basePassword=<password>ContentServerUri=https://db01.lmdom.local
ServiceUserName=<service user> ServiceDomain=lmdom Ser-
vicePassword=<password> ExchangeServer-
Uri=https://DC1.lmdom.local/EWS/Exchange.asmx
ExchangeUserDomain=lmdom.local ExchangeUserName=<name>
ExchangeUserPassword=<password> -log:C:\1.log
```

Exchange Online configuration

To be able to send smartmails from an Online Exchange account, add the following parameters UseLocalExchangeServer=false ExchangeUserName=<name> ExchangeUserPassword=<password>.

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName-
e=DB01 DatabaseUserName=sjsysadm DatabasePassword=<password>
```

```
ContentServerUri=https://db01.lmdom.local Ser-
viceUserName=<service user> ServiceDomain=<domain> Ser-
vicePassword=<password> UseAutodiscover=True
ExchangeUserName=<name> ExchangeUserPassword=<password> Pack-
ages=<Package1.wzp,Package2.wzp> -log:C:\1.log
```

Remove/cleanup quietly without removing version from database

```
Scanjour.Process.Configurator.exe -remove -quiet -verbose
```

OAuth authentication method

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName-
e=DB01 DatabaseUserName=sjsysadm DatabasePassword=<password>
OAuthClientSecret=<secret> Con-
tentServerUri=https://db01.lmdom.local ExchangeServer-
Uri=https://DC1.lmdom.local/EWS/Exchange.asmx
DedicatedExchangeCredentials=true ExchangeUserName=sa_wzprocess
ExchangeUserDomain=lmdom ExchangeUserPassword=<password> -
log:C:\1.log
```

Ensure that access codes and start and end dates are not overwritten

Using the `Packages`parameter, you can modify access codes and the start and end date for a process. If the package does not contain values for the entries that you modify, your values will be preserved if the package is loaded again.

Package names should not contain special characters, including [.] and [,]. The reason behind this recommendation is that the -packages argument is interpreted as a comma separated list and compares the specified names with the name of the package in the package folder.

Install the notification agent on a separate server

If you install the Notification agent role on a server that is different from the web server running WorkZone Process, the WorkZone Process service must be configured to point to the agent server.

Configure the WorkZone Process service to point to the agent server

1. Navigate to the process installation folder on the web server or web servers that host the process service, and edit the Web.config file. The file is usually located under C:\Program Files (x86)\KMD\WorkZone\Process\Web\Services.
2. Locate the `<client>` object under `<system.serviceModel>`.
3. In all the child objects of the type `<endpoint>`, replace '`localhost`' in the address attribute with the host name or the IP address of the server running agents.
4. Recycle the **WzpSvc** application pool.

Ports

When running separate web and agent servers, the web server must be able to send messages to the agent server that runs the notification agents. For this to be possible, traffic must be allowed on ports 1801, 2103, and 2105 from the web server to the agent server.

Furthermore, traffic must also be allowed on the ports used for the push and mail notification agents. The defaults are ports 8080 and 8081.

Configuration for multiple databases

If you operate in an environment with multiple organizations where data is stored on multiple databases, you can install WorkZone Process on more than one database. To run WorkZone Process on more than one database, you need to complete the configuration and install the required packages for each of the databases.

With a multiple-database configuration, valid databases run consistently and databases where WorkZone Process is not installed are ignored. Also, the situation where a valid database is temporarily unavailable can be handled in WorkZone Process.

For information about how to install and configure WorkZone, see Install WorkZone Process and Configure WorkZone Process.

> **Example**: Command line code as applied for each database in a multiple-database setup

When you install a series of databases, each database must have a unique reference. View the following example to identify how to reference databases in a multiple-database installation.

Database one

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName=DB01 DatabaseUserName=sjsysadm DatabasePassword=<password> ContentServerUri=https://db01.lmdom.local ServiceUserName=<service user> ServiceDomain=<domain> ServicePassword=<password> ExchangeServerUri=https://DC1.lmdom.local/EWS/Exchange.asmx ExchangeMailbox=mailagent@lmdom.local SetupDatabase=true Packages=<Package1.wzp,Package2.wzp> -log:C:\1.log
```

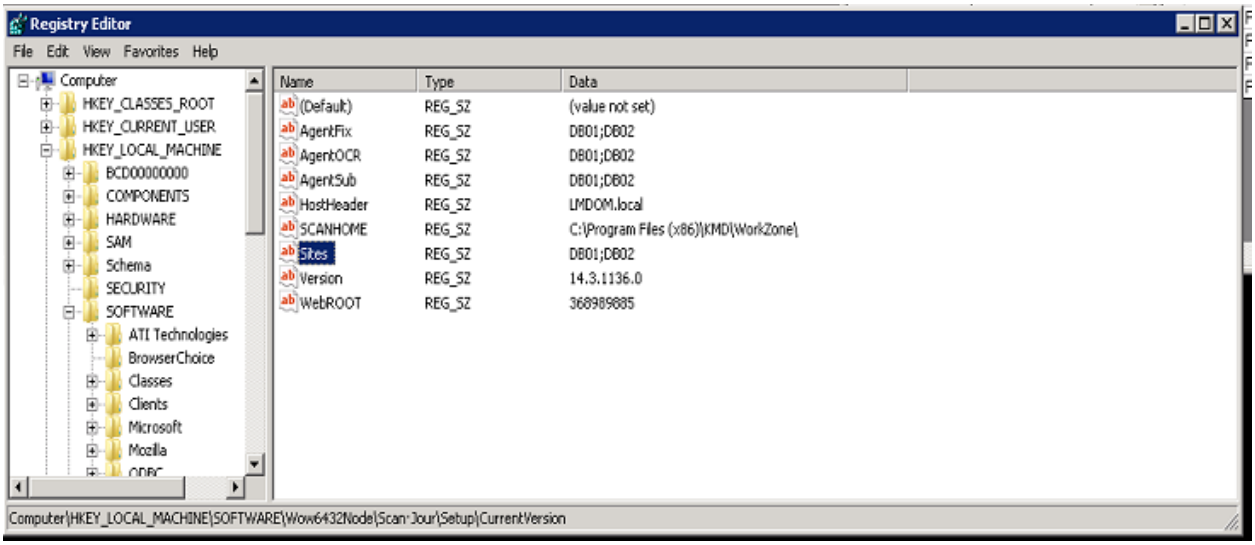
Database two

```
Scanjour.Process.Configurator.exe -quiet -verbose DataSourceName=DB02 DatabaseUserName=sjsysadm DatabasePassword=<password> ContentServerUri=https://db02.lmdom.local ServiceUserName=<service user> ServiceDomain=<domain> ServicePassword=<password> ExchangeServerUri=https://DC1.lmdom.local/EWS/Exchange.asmx ExchangeMailbox=mailagent@lmdom.local SetupDatabase=true Packages=<Package1.wzp,Package2.wzp> -log:C:\1.log
```

Database overview

In an environment where WorkZone Process supports multiple databases, you can open the Windows Registry to identify the databases where WorkZone Process is installed.

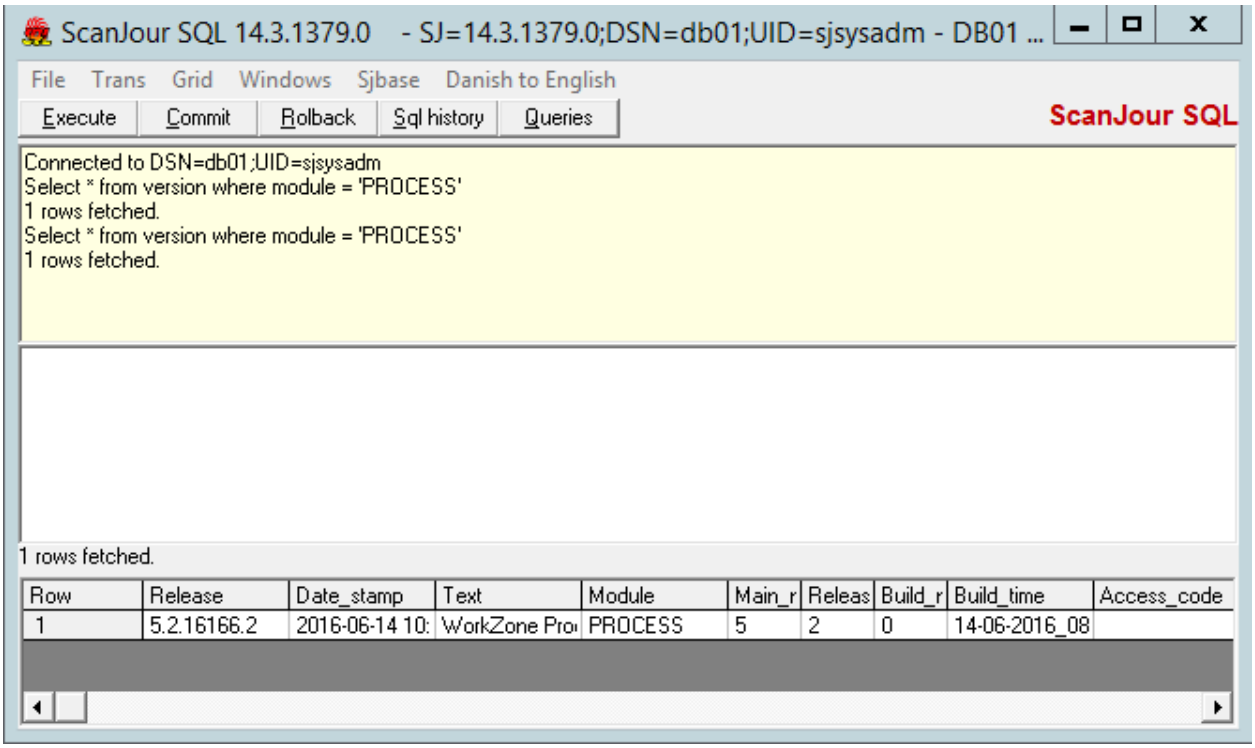
- In Registry Editor, go to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Scan·Jour\Setup\CurrentVersion\Sites



Support of WorkZone Process on individual databases

From ScanJour SQL, you can verify if WorkZone is supported on a specific database.

- In ScanJour SQL, enter the following SQL statement: `Select * from version where module = 'PROCESS'`



Configure Exchange Server and Web Services

Configure the Exchange server

Recommendations

According to recommendations by Microsoft - see Set Message Size Limits for Exchange Web Services - a message size limit can be calculated by the following formula:

```
Message Size Limit = Original Message Size * 4/3
```

where `4/3` represents a message that is approximately `33` percent larger than the original. However, message size increase may be much larger, depending on the type of attachment that is sent, the attachment size, whether the attachment is already compressed, and the messaging client from which the message is sent. In some cases, you may experience message size increases of 100 percent after encoding (that is, messages that are twice the size of the original messages).

> **Note:** The unit of measure is kilobytes (KB.)

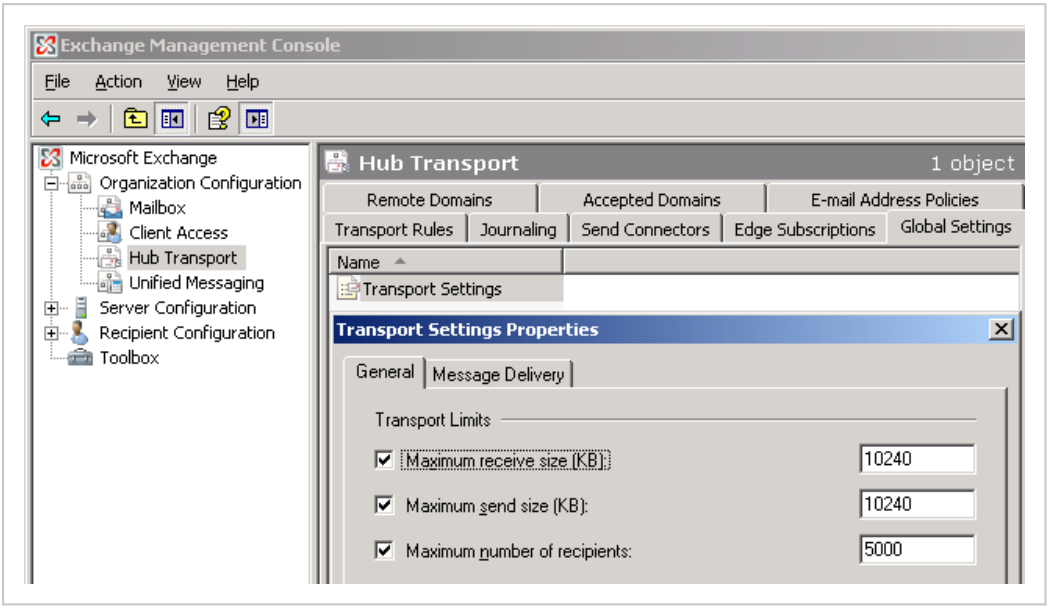
Exchange Shell

Run `'Set-TransportConfig -MaxReceiveSize X -MaxSendSize Y' cmdlet`, where `X` represents the size of received messages, and `Y` the size of sent messages.

> **Note:**
>
> - To calculate the limits, see the recommendations above.
> - The steps in this procedure are applicable to Exchange Server 2010.

Exchange Management Console

1. Open **Exchange Management Console**.



2. In the **Hub Transport** settings, click the **Global Settings** tab.
3. Under **Transport Settings**, enter values in the **Maximum receive size (KB)** and **Maximum send size (KB)** fields.
4. Save the changes.

Modify the EWS throttling policy to handle concurrent connections

If you use the Mailbox Monitor and F2 integration service workflows, you can set up the Exchange server to handle concurrent Exchange connections on the same user. The EWS throttling policy determines the number of concurrent connections that the Exchange server can handle using the **EWSMaxConcurrency** parameter.

By setting the **EWSMaxConcurrency** parameter, you define the number of concurrent open connections that a specific user can have against an Exchange server.

The default and recommended values for the parameter depend on Exchange Server version:

Exchange Server version	Default value
2010	10

See the Microsoft article EWS throttling in Exchange for more information.

You modify the default throttling policy on an Exchange server using cmdlets:

cmdlets	Exchange Server version	Microsoft articles
Set-Throttling-Policy	Exchange Server 2010 SP2 Exchange Server 2010 SP3 Exchange Server 2016 on-premises	Set-ThrottlingPolicy
Set-Throt-tlingPolicyAssociation	Exchange Server 2010 SP2 Exchange Server 2010 SP3 Exchange Server 2016 on-premises	Set-Throt-tlingPolicyAssociation

Configure the Exchange Web Services

WorkZone Process distributes smartmails using Exchange. This sections describes how to set up Exchange Web Service (EWS) and how to adjust Exchange for larger mail sizes which could be required, depending on the volume of documents distributed using smartmails.

Recommendations

For information about calculating limit sizes for sent or received messages, see Exchange Server Configuration.

> **Note:** If you use Exchange Server 2010, it is not necessary to adjust the limit sizes, but you should verify it.

Exchange Server 2010

1. Open the `web.config` file for editing. The file is located here:

   ```
   '%ProgramFiles%\Microsoft\Exchange Server-
   \ExchangeVersion\ClientAccess\exchweb\ews\
   ```

2. Change the value of `maxRequestLength`.
3. Change the `maxReceivedMessageSize` value of `EWSAnonym-ousHttpBinding`.

   -Or-

If you use SSL (https), change the `maxReceivedMessageSize` value of `EWSAnonymousHttpsBinding`.

Install process packages

About process packages

As part of the WorkZone Process installation all standard process packages are installed but only the Basis process package is enabled by default. You can enable other packages using WorkZone Configurator. See Activate process packages.

To install and activate customer specific packages, use the WorkZone Process Package Loader. See Install and activate customized process packages.

The table below gives you an overview of which processes and service workflows are included in the different process packages.

Package name	Processes/Service workflows in packages
Basis	Hearing (Basis) Submission (Basis) Mailbox monitoring Mailbox handler Create report Process monitoring Case monitoring
Extended	Distribution (Extended) Submission (Extended) Submission (Advanced)
Agency	Ministerial
ExternalCommunication	SmartPost e-Boks message handler

Package name	Processes/Service workflows in packages
F2	F2 requisition handler F2 delivery F2 information F2 update
CaseActivity (Demo)	Public access
InteractConnector	Interact connector

Activate process packages

As part of the WorkZone Process installation all standard process packages are installed but only the Basis process package is activated by default. You can activate other packages using WorkZone Configurator.

1. Open WorkZone Configurator.
2. Go to **Global** > **Feature settings** > **WorkZone Process**.
3. Select the check box next to the process package you want to activate.

See also Feature settings in the WorkZone Configurator Administrator Guide.

Install and activate customized process packages

All standard process packages are installed as part of the WorkZone Process installation. You activate and deactivate standard packages using WorkZone Configurator. To install and activate additional customized process packages, you must run the program `Scanjour.Process.PackageLoader.exe`. This program is part of the WorkZone Process installation.

After installation, the Package Loader program is located here: `..\KMD\WorkZone\Process\Bin`.

The minimal syntax of the command line is:
`Scanjour.Process.PackageLoader.exe /uri:<uri> /package:<package>`

The specified package will be loaded into the database that is identified by the `/uri` parameter.

Required parameters

Depending on the authentication method used, you need to specify either Windows or OAuth specific parameters.

Parameters	Description
Windows authentication	
`/uri:<uri>`	The WorkZone Content Server URI where WorkZone Process is installed.
`/package:<package>`	The name of the package to be loaded.
OAuth authentication	
`/uri:<uri>`	The WorkZone Content Server URI where WorkZone Process is installed.
`/package:<package>`	The name of the package to be loaded.
`/oauth_server_uri`	The OAuth server URI.
`/oauth_client_id`	The WorkZone Process client Id (WZP).
/oauth_client_secret	The WorkZone Process client secret.

Optional parameters

Optional parameters apply to both Windows and OAuth authentication.

Parameters	Description
`</credentials=<credentials>`	Windows credentials of the WorkZone user by which the package will be loaded.
`<login>`	The name of the Windows account to be used for accessing WorkZone Content Server.
`<domain>`	The name of the realm (domain or computer) that the account belongs to.
`<password>`	The password required for the account authentication.

Parameters	Description
`<odatapath>`	The relative path to the OData endpoint that will be used for loading the package data.
`<defaultdisabled>`	If the package is related to a feature in the **Version** table, this argument can disable this feature by default.
`<defaultenabled>`	If the package is related to a feature in the **Version** table, this argument can enable this feature by default.
`/help`	Shows help information and exit.

Example: Windows authentication

```
Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:MinisterialServices.wzp

Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:Package.wzp /credentials:admin@domain/password

Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:Package.wzp /odatapath:/odata/v3

Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:Package.wzp /defaultdisabled

Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:Package.wzp /defaultenabled
```

Example: OAuth authentication

```
Scanjour.Process.PackageLoader.exe /uri:https://db01 /package:Basis.wzp /oauth_server_uri:https://db01/oauth2 /ouath_client_id:WZP /oauth_client_secret:secret
```

> **Important:** After deploying a new package, you must either restart IIS or recycle the WzpSvc application pool on all relevant web servers.

Display customized process packages in WorkZone Configurator

You can display customized process packages on the **Feature settings** page in WorkZone Configurator, so that an administrator can activate or deactivate packages in the same way as standard packages.

To display packages, you need to specify the following elements in the `<PackageDefinition>` section of the package.xml file:

- `<FeatureName>` – The name of the process package.
- <ParentFeatureName> – Adds the process package under this node on the **Feature settings** page. For example, `<ParentFeatureName>PROCESS</ParentFeatureName>` adds the package below the WorkZone Process node.
- `<FeatureSelectable>` – J or N specifies if the package can be activated.
- `<PackageDefaultEnabled>` – J eller N specifies if the package will be installed by default on a new installation.

See Activate process packages and Feature settings in the WorkZone Configurator Administrator's Guide.

Install and configure WorkZone e-Boks Push Service

WorkZone e-Boks Push Service is a web service that makes it possible for WorkZone to receive e-Boks messages using Digital Post 2 and Next generation Digital Post (NgDP).

You can install the push service behind or in front of the firewall or in a DMZ at a separate location, for example in Azure. By default, the push service is installed behind the firewall. You need a hole in the firewall to allow access to the push service as illustrated in the diagram below. This means that you must open port 443 on the server that you have installed the push service on.

You can only install one instance of the push service for each retrieval system. The push service is self-contained with a data store. By default, the data store is placed in the same location as the push service. If you want the data store in a different location, for example where you

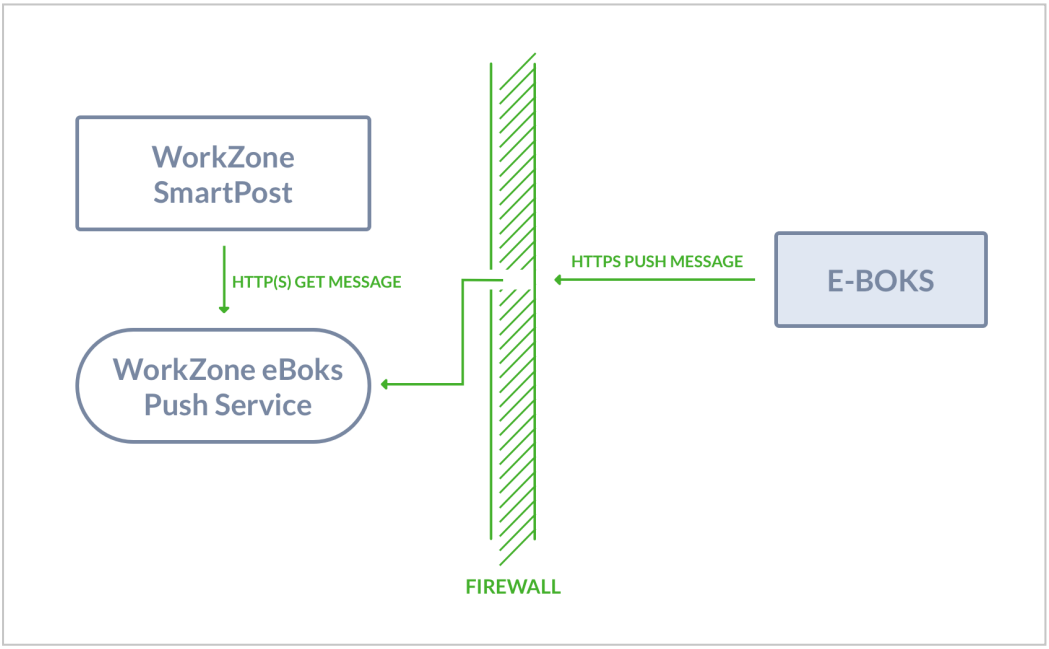
have your backup, or where you have more space, you can change the location. You change the location of the data store as well as other settings in the app config file named **Appsettings.json**, which is placed in the same location as the push service. To change the location of the data store, change the configuration of the **ConnectionStrings** parameter.

Regardless of whether your setup is with only one server that acts as both web server and agent server or the push service is installed on a separate server, the database must be populated. See Replicate the configuration from the WorkZone database to the push service (NgDP).

Digital Post 2

As of the WorkZone 2020.1 release, SmartPost supports Digital Post 2. The most significant difference between Digital Post 1 and Digital Post 2 is that the polling for new messages is replaced by a push. For information about Digital Post, see Vejledninger Digital Post and Kom godt igang - for virksomheder, Digital Post 2.

To use SmartPost with e-Boks using Digital Post 2, you need to install WorkZone e-Boks Push Service. e-Boks requires an end point that can receive messages. The WorkZone e-Boks push service exposes the required interface to e-Boks.



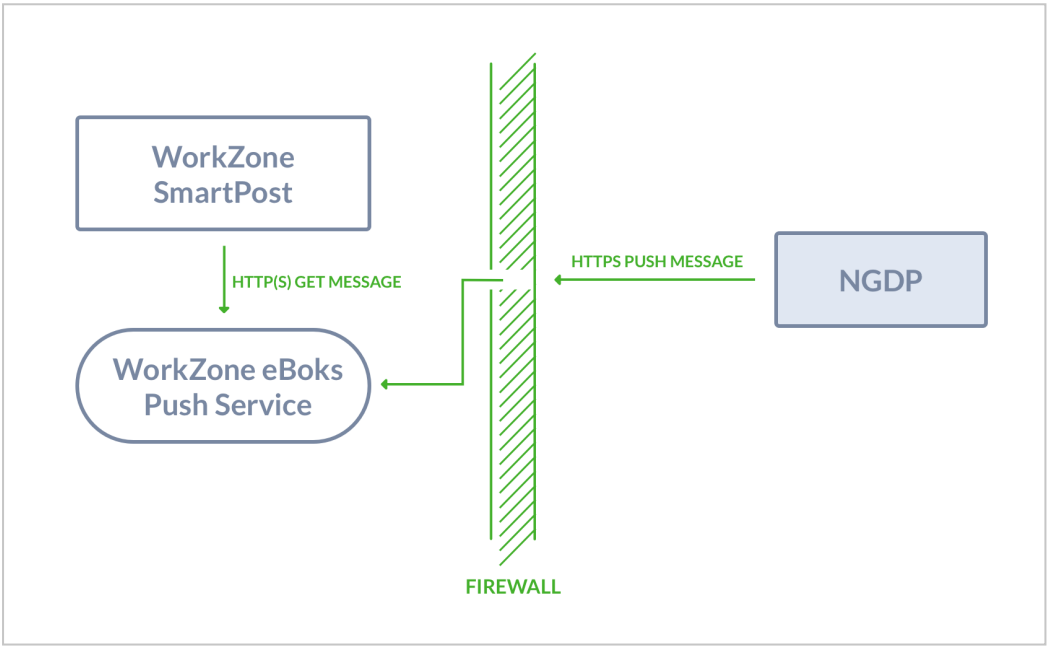
NgDP

As of the WorkZone 2022.0 release, SmartPost supports NgDP in production. For more information, see Configure SmartPost to use next generation Digital Post (NgDP).

WorkZonee-Boks Push Service receives messages and receipts on incoming calls from a Next generation Digital Post (NgDP) system and transforms messages between the MeMo format and Digital Post 1 or 2.

For more information about MeMO, please refer to Det nye meddelelsesformat on the Agency for Digitisation's website (Digitaliseringsstyrelsen).

The push service must be accessible from NgDP and from the local web servers. Because of the incoming NgDP calls, it is required to configure firewalls and routers to allow these requests and ensure that a legal HTTPS server certificate is installed.



The IIS server should be configured to only allow requests with NgDP client certificates, and the certificate that your organization uses.

Install WorkZone e-Boks Push Service

To install and configure the push service, you need to complete the following steps:

1. Run the installer that sets the site for the push service on all web and agent servers. This step also involves configuring the service for the retrieval and dispatch systems in use.
2. Configure the e-Boks dispatcher to use the push service.
3. Set up the e-Boks Administrationsportal to send messages to the push service.

Prerequisite:

- WorkZone Process including SmartPost must be release 2018.0 or later.
- The WorkZone site must be configured to run in https mode.
- .NET Core Windows Hosting Bundle (dotnet-hosting-5.0.7-win.exe) must be installed.
  See Install .NET Core Windows Hosting Bundle.
- Microsoft Visual C++ 2015 Redistributable (vc_redist.x64.exe) must be installed.

Install .NET Core Windows Hosting Bundle

You can run the **Microsoft .Net 5.07 Windows Server Hosting** installer (dotnet-hosting-5.0.7-win.exe) which is delivered with WorkZone Process to install .NET Core Windows Hosting Bundle, or you can install it with a PowerShell script.

Install with a PowerShell script

1. Run Windows PowerShell as administrator.
2. Run the script:

```
powershell -NoProfile -ExecutionPolicy unrestricted -Command "
[Net.ServicePointManager]::SecurityProtocol = [Net.Se-
curityProtocolType]::Tls12; &([scriptblock]::Create((Invoke-
WebRequest -UseBasicParsing 'https://dot.net/v1/dotnet-
install.ps1'))) -channel 5.0 -Runtime aspnetcore"
```

Install WorkZone e-Boks Push Service with the WorkZone e-Boks Push Service Setup wizard

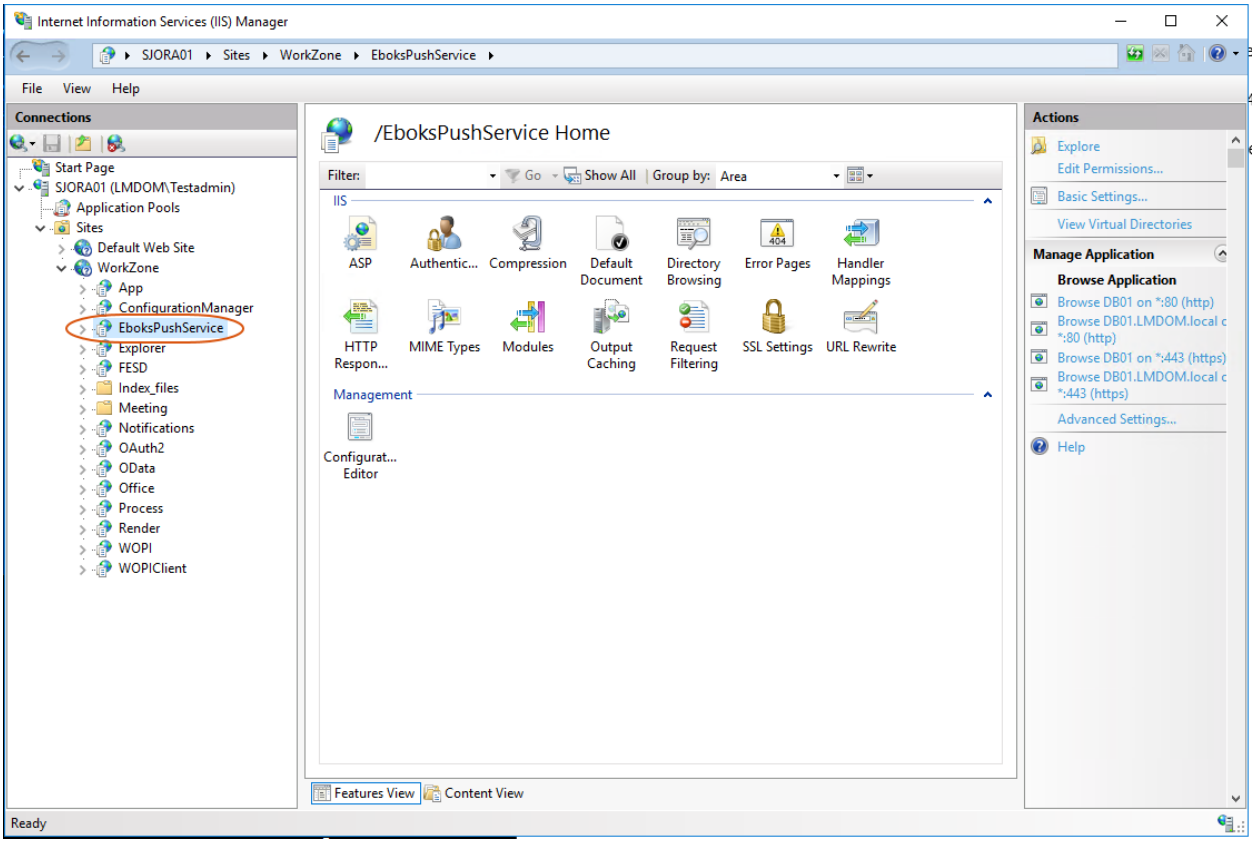
You must run the installer with elevated privileges on both web and agent servers where the WorkZone Process web profile is already installed.

1. Run the WorkZone e-Boks Push Service Setup wizard, WorkZone.Dispatcher.Eboks.PushService.Setup.msi.
2. Click **Next** through the wizard until you get to the **Complete the WorkZone e-Boks Push Service Setup** page. If you see this page, the service has been installed

successfully.

3. Click **Finish** to close the wizard.

After the installation, the **EboksPushService** web application is created under the WorkZone site as shown in IIS Manager.



Install with Olympus

If you have a test setup with only one server that acts as both web server and agent server, you can use the Olympus installation to automatically deploy the push service by setting the **InstallEboksPushService** parameter to **True** in the `<WZP>` configuration element.

```
    <WZP Install="True" Version="Latest" Url="http://{0}/" Roles="Web;Agent" ServiceUserName="sa_wzprocess" ServiceDomain="LMDOM" ServicePassword="WZP"
ExchangeServerUri="http://dc1/EWS/Exchange.asmx" ExchangeMailbox="MailAgent@lmdom.local"
InstallPackages="Basis.wzp,Ministerial.wzp,Extended.wzp,F2.wzp,Agency.wzp,CaseActivity (Demo).wzp,ExternalCommunication.wzp,Interact.wzp"
InstallEBoksPushService="true" />
```

In a more complex setup, you need to deploy the push service manually by using the WorkZonee-Boks Push Service Setup wizard. See Install WorkZone e-Boks Push Service with the WorkZone e-Boks Push Service Setup wizard.

Verify the installation

You can verify that the e-Boks push service responds by invoking the URL:

```
https://<data-
base>/Ebok-
sPushService/api/MeddelelseV2/afhentningssystem/0000/meddelelser
```

It should result in the following XML:

```
<MeddelelseReferenceSamling xmlns="urn:oio:dkal:2.0.0" />
```

You can also use the following URL:

```
https://<data-
base>/Ebok-
sPushService/api/MeddelelseV1/afhentningssystem/0000/meddelelser
```

which results in the following XML:

```
<MeddelelseReferenceSamling xmlns="urn:oio:dkal:1.0.0" />
```

Note: As long as the resulting XML contains a return value of either "urn:oio:dkal:1.0.0" or "urn:oio:dkal:2.0.0", the installation is verified

Install a stand-alone e-Boks Push Service

You can install the e-Boks Push Service on a Windows server that does not have a WorkZone database or WorkZone Process installed.

Prerequisite: The following Windows features must be installed on the server:

- Web-Default-Doc
- Web-Dir-Browsing
- Web-Http-Errors
- Web-Static-
- Web-ASP
- Web-Asp-Net45
- Web-ISAPI-Ext
- Web-ISAPI-Filter
- Web-WebSockets
- Web-Mgmt-Tools
- BitLocker, EnhancedStorage
- RSAT
- RSAT-Feature-Tools
- RSAT-SMTP
- SMTP-Server

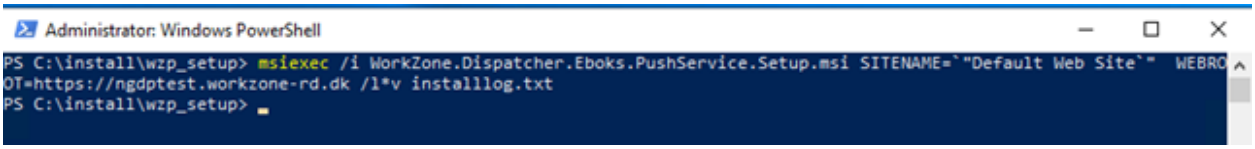
Content
- Web-Health
- Web-Http-Logging
- Web-ODBC-Logging
- Web-Performance
- Web-Stat-Compression
- Web-Dyn-Compression
- Web-Security
- Web-Filtering
- Web-Basic-Auth
- Web-Windows-Auth
- Web-App-Dev
- Web-Net-Ext45
- Web-AppInit
- Web-Mgmt-Console
- Web-Mgmt-Compat
- Web-Metabase
- Web-Lgcy-Mgmt-Console
- NET-Framework-45-Features
- NET-Framework-45-Core
- NET-Framework-45-ASPNET
- NET-WCF-Services45
- NET-WCF-HTTP-Activation45
- NET-WCF-TCP-Activation45
- NET-WCF-TCP-PortSharing45
- System-DataArchiver
- Windows-Defender
- PowerShellRoot, PowerShell
- PowerShell-ISE
- WAS
- WAS-Process-Model
- WAS-Config-APIs
- WoW64-Support
- XPS-Viewer

For the NgDP PUSH dispatcher to work, you need to install the hosting bundle supplied with the WorkZone Process (dotnet-hosting-X.X.X-win.exe).

When installing the push service, you must run the MSI installer manually from an elevated PowerShell session.

```
msiexec /i WorkZone.Dispatcher.Eboks.PushService.Setup.msi
SITENAME=`"Default Web Site`" WEBROOT=https://<full qualified
servername> /l*v logfile.txt
```

If you invoke the installation through a remote PowerShell session, you can add the `/quite` flag the arguments.



Whitelist IP addresses

Make sure to whiteliste IP addresses from NgDP to WorkZone. Please refer to Technical Integration NgDP v1.30 on the Agency for Digitisation's website (Digitaliseringsstyrelsen). You also need to make sure that the WorkZone web and agent servers are whitelisted.

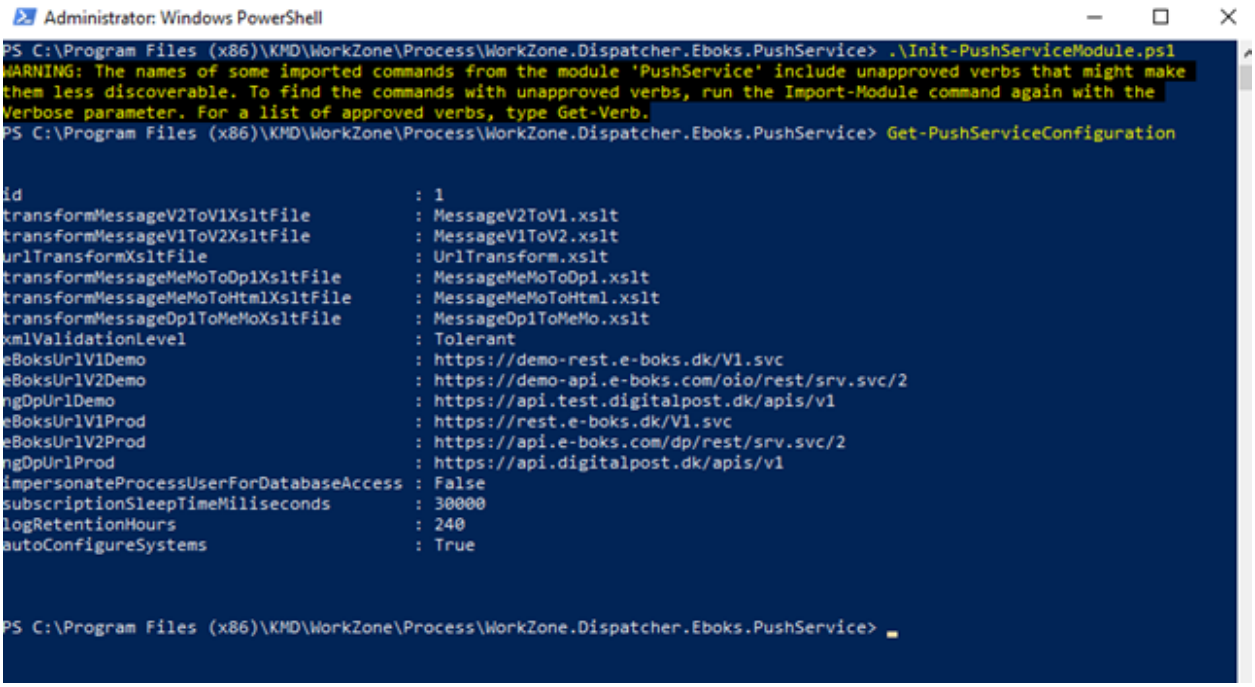
Verify the installation

You can verify that the push service is installed and works by running the administration script `Init-PushServiceModule.ps1` located in

C:\Program Files (x86)\KMD\WorkZone\Process\WorkZone.Dispatcher.Eboks.PushService\

Invoke the cmdlet `Get-PushServiceConfiguration`.

The service is installed correctly if no errors occur.

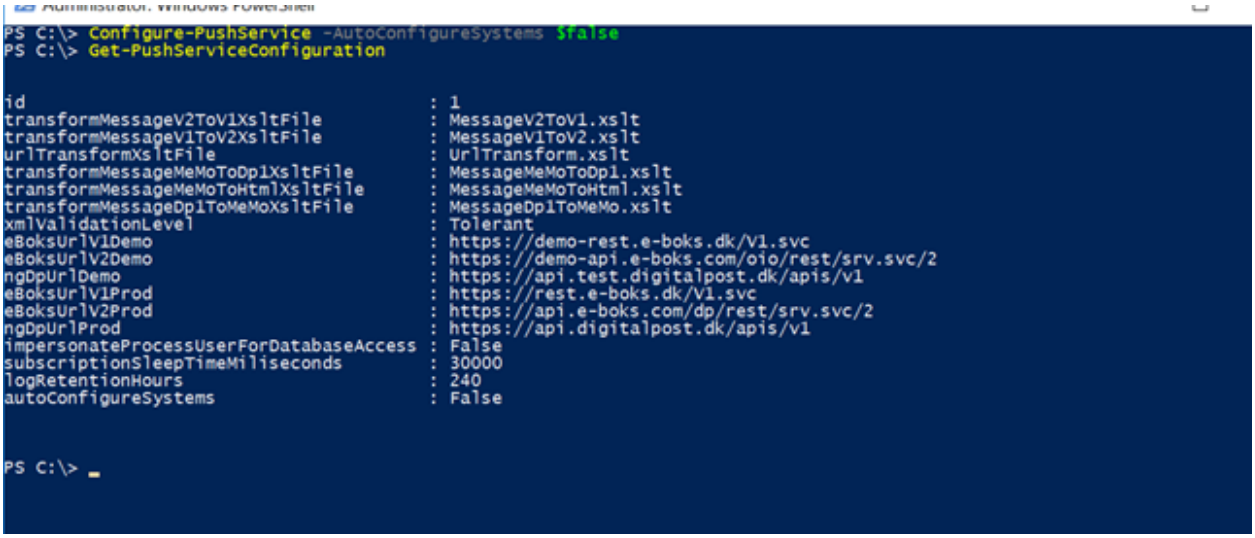


Replicate the configuration from the WorkZone database to the push service (NgDP)

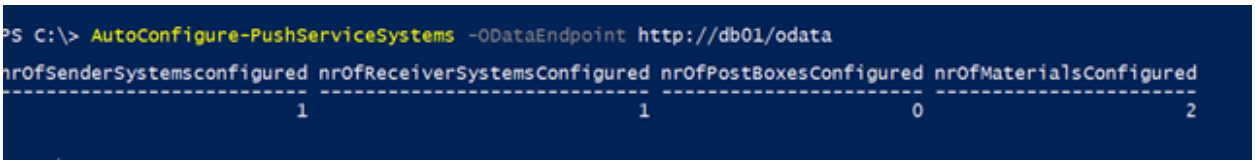
The push service has its own local configuration database that must be populated. In a one-server test installation, the database is populated automatically when the push service application pool is recycled. If the push service is installed manually on another server, the database can be populated using the PowerShell interface for the push service.

If the push service is installed on a separate server, it is recommended to turn of the auto-configure feature by setting the **configure-pushservice -AutoconfigureSystems** to **False**.

```
configure-pushservice -AutoconfigureSystems $false
```



You can do manual configuration from a WorkZone database using the cmdlet **AutoConfigure-PushServiceSystems**. This cmdlet takes the ODataEndpoint of the database as an argument and returns the number of configuration items that are returned from the system.



The credentials of the current user is used to access OData. The current user must have the rights to access OData and read the configuration data.

This cmdlet must be called on a regular basis or manually after a change of the configuration.

Use contact points on outgoing messages (NgDP)

You can test if it is possible to send NgDP messages to a specific contact point. Contact points can be assigned to addresses in the WorkZone database by using custom address info with the label **NgDpCp**.

To test if it is possible to send NgDP messages, it is required to create the metadata for the address property and address type. This can be done with the cmdlet **New-NgDpMetadata**.

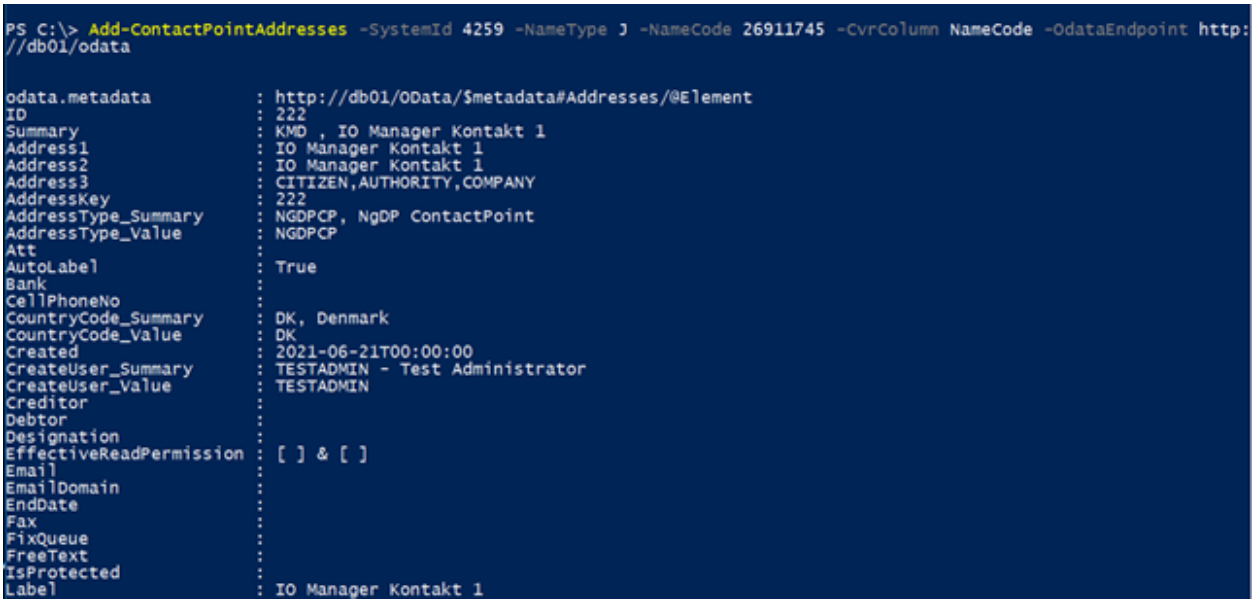
```
PS C:\> New-NgDpMetadata -SystemId 4259


odata.metadata          : http://db01/OData/$metadata#SystemCustomLabels/@Element
ID                      : NgDpCp,D_AI
Summary                 : NgDpCp
CustomLabel             : NgDpCp
CustomLabelLang         : NgDpCp
CustomLabelRev_Summary  :
CustomLabelRev_Value    :
EndDate                 :
LabelSyno               : NotNull
RegExpName_Value        :
Routine                 :
StartDate               :
SyndicationTitle        : (NgDpCp,D_AI)
System                  :
Text                    :
Type                    : D_AI
TypeReference_Value     :
UserKey                 :
Value                   : NgDpCp

Contact point address info created
odata.metadata    : http://db01/OData/$metadata#SystemCustomDomains/@Element
ID                : NGDPCP,AD
UserKey           : AD - NGDPCP
Summary           : NGDPCP, NgDP ContactPoint
Code              : NGDPCP
CtrlTxt           : NgDP ContactPoint
EndDate           :
Rank              :
Selection         :
StartDate         :
SyndicationTitle  : AD - NGDPCP (NGDPCP,AD)
System            :
Text              : NgDP ContactPoint
Type_Summary      : AD, Address type
Type_Value        : AD
Value             : NGDPCP

Address type NgDP Contact type created
```

To create WorkZone addresses for a specific CVR contact that corresponds to the contact point that is defined in the NgDP system for the same CVR number, use the cmdlet **Add-ContactPointAddresses**.



PowerShell cmdlets

The following e-Boks Push Service cmdlets are available:

- Initialize-PushServiceModule
- Get-SubscriptionStatus
- Configure-PushService
- AutoConfigure-PushServiceSystems
- Get-PushServiceConfiguration
- Configure-PushServiceSystem
- Get-PushServiceSystemConfiguration
- Delete-PushServiceSystemConfiguration
- Get-PushServiceLogs
- Delete-PushServiceLogs
- New-Receipt
- Get-Receipt
- Delete-Receipt

- Get-PendingRecipients
- Create-PendingReceipts
- Push-TestMessage
- Ship-TestMessage
- Configure-Material
- Get-Material
- Delete-Material
- Get-ContactPoints
- New-NgDpMetadata
- Add-ContactPointAddresses

Map NgDP error messages to e-Boks error messages

Errors that are returned from the NgDP system are mapped to e-Boks errors using in the appsettings.json file of the service. The default location this file is:

`"C:\Program Files (x86)\KMD\WorkZone\Process\WorkZone.Dispatcher.Eboks.PushService\WebService"`

Below is an example of a mapped error informing that the title column exceeds the maximum length:

```
                "NgDpErrorCodes": {
    "message.create.label.size": {
      "ErrorCode": 4071,
      "ErrorText": "Feltet MeddelelsesTitelTekst indeholder mere end
256 tegn."
    }
  }
```

See also e-Boks errors.

Appsettings.json

The table below provides descriptions of parameters in the Appsettings.json file.

Name	Description
Logging	Configuration log levels for various components. Logging is done in the eventlog.
AllowedHosts	Configuration of hosts that are allowed to call the service. It should only be allowed to call the service from e-Boks and the servers that are running WorkZone Process. `https://docs.microsoft.com/en-us/-dot-net/ap-i/mi-crosoft.aspnet-core.host-fil-ter-ing.host-filteringoptions.allowedhosts?view=aspnetcore-5.0`
ConnectionStrings	Configuration of the location of the temporary store of the messages. The connect string `StoreContext`" references a file that contains the temporary store. To move the file to another location, change the path to `Meddelser.db`. By default it is stored in the same folder as the service binaries. It is recommended that the database file is stored in a location that has backup. The user running the service must have read/write access to the file.
Trans-formMes-sageV2ToV1XsltFile	Reference to an xslt file that can transform e-Boks from V2 to V1.
Trans-formMes-sageV1ToV2XsltFile	Reference to an xslt file that can transform e-Boks from V1 to V2.

Name	Description
UrlTransformXsltFile	Reference to a xslt file that can transform e-Boks entities that contains URL references.
EBoksUrlV1Demo	The e-Boks demo v1 endpoint. By default, the endpoint is `https://demo-rest.e-boks.dk/V1.svc`.
EBoksUrlV2Demo	The e-Boks demo v2 endpoint. By default, the endpoint is `https://demo-api.e-boks.com/oio/rest/srv.svc/2`.
EBoksUrlV1Prod	The e-Boks production v1 endpoint.By default, the endpoint is `https://rest.e-boks.dk/V1.svc`.
EBoksUrlV2Prod	The e-Boks production v2 endpiont.By default, the endpoint is `https://api.e-boks.com/dp/rest/srv.svc/2`.
EBoksUrlV1Custom	Can be used to set up a custom v1 endpoint for the **RelayMessageCallsToCustomEndpoint** setting on e-Boks systems.
EBoksUrlV2Custom	Can be used to set up a custom v2 endpoint for the **RelayMessageCallsToCustomEndpoint** setting on e-Boks systems.
ServiceUserName	The user name of the process user that is used for impersonation. It is filled out automatically during installation.
ServiceUserDomain	The domain of the process user. It is filled out automatically during installation.
ServiceUserPassword	The encrypted password of the process user. It is filled out automatically during installation.
ImpersonatePro-cessUser-ForDatabaseAccess	True or false. If set to True, the process user is impersonated when database calls are made.

Configuration per system in the array “EBoks”:”Systems”[]

Name	Description	Example
SystemId	SystemId of the e-Boks system	4259
EBoksSystemType	"AfsenderSystem" or “AfsenderSystem”. It must match the configuration in the e-Boks Administrationsportal.	AfsenderSystem
EBoksApiVersion	The API version of the configuration at e-Boks must match the API version set in the e-BoksAdministrationsportal. Only ‘1’ and ‘2’ are legal values that correspond to v1 and v2 in the e-Boks Administrationsportal.	1
UseEboksProduction	This can be either True or False. This value is used to resolve the URL for the endpoint of the e-Boksservice using the settings `EBoksUrlVxProd` and `EBoksUrlVxCustom`.	False
ClientCertificateStore	Configuration of where the certificate used for communicating with e-Boks is stored. The legal values are `LocalMachine` and `CurrentUser`.	LocalMachine
ClientCertificateThumbPrint	The thumbprint of the certificate used for communicating with e-Boks.	F63A18100F5AA0454E17D25AD85082362D96AFC2

Name	Description	Example
ClientCertificateFile	File name that contains the client certificate. Storing the certificate in a file is an alternative to storing it in the certificate store. If the setting `ClientCertificateFile` is not empty, the `ClientCertificateThumpPrint` must be empty, and vice versa.	/home/cert.pfx
ClientCertificatePassword	Contains the password that protects the `ClientCertificateFile`.	Secret
RelayMessageCallsToCustomEndpoint	This setting can be used to redirect calls to a remote installation of the **EBoksProxy** service that receives the messages from e-Boks.	False
RelatedSystem	The ID of the 'reverse' system. For SenderSystem it should be the ID of the reciver system, and vice versa.	4259

Troubleshooting

Click an issue below to see the solution or workaround.

In environments with WorkZone Client the WzpSvc application pool and WorkZone Process web service are not removed as expected.

To work around this issue:

Uninstall WorkZone Client before uninstalling WorkZone Process.

Cannot install agent role

If you are unable to connect to WorkZone Content Server on a specified URL using the service account, ensure that the `SJPROCESSUSER` in the `USERS` register has an active directory SID. See also Service accounts.

Upgrading WorkZone Process corrupts the registry

When upgrading WorkZone Process, two registry entries,

`shReg.sjRegSag.1` and `sjReg.sjRegGenerisk.1`, get an additional `InProgServer32` entry under `InProgServer32`. These files are used for the repair option in MSI so a deletion of the files is not the proper way to resolves the corruption.

To resolve this problem, you must complete a repair on WorkZone Content Server:

> Open **Control Panel** and identify the WorkZone Content Serverentry in **Uninstall or change a program** under **Programs** > **Programs and Features**.

Error when entering an Exchange Web Service URL

The error message “Failed to connect to the Exchange Web Service using service account” might be displayed when you configure WorkZone Process and get to the point where you enter the Exchange Web Services URL. At this point you have already completed the verification step "Verify access to Exchange server and oData" as part of the configuration prerequisites. However, the error occurs because the current service account user does not have a valid mailbox.

To resolve the issue, set up a mailbox for the service account user.

Unable to connect to Exchange Web Services

When you run the configurator in quiet mode, it may fail if the configurator has been run at least once before. The configurator log will contain the error message "Unable to connect to Exchange Web Services".

Workaround:

Remove the mail agent configuration file `C:\Program Files (x86)\KMD\WorkZone\Process\Bin\Scanjour.Process.MailAgent.dll.config` and run the configurator again.

The mail agent or the WorkZone PDF fails upon installation on an agent server

If the mail agent is installed together with WorkZone PDF on an agent server one of the products will fail. The mail agent requires access to the web server via the database name while WorkZone Content Server requires local access to PDF via the database name.

To work around this issue, install the **Webserver** role on the agent server. For more information about installing roles, see Install WorkZone Process.

WorkZone Process installation fails with Agent role and Notification Agent Role installed prior to Webserver Role

When installing WorkZone Process on two servers, the sequence in which the roles are installed is essential to make the installation succeed.

You can complete an installation in one of two ways:

On server 1: Start by installing the Webserver role and then, on server 2, install the Agent role and the Notification agent role

-or-

Install all three roles at the same time.

If you start out by installing the Agent role and the Notification agent role before you install the Webserver role, the installation will fail.

To resolve the issue when an installation has failed, just uninstall WorkZone and reinstall with all three roles.

Problem with installation of a package with the same version number

If you install a package with the same version number that is already installed, and workflows are running, you may experience problems downloading the new DLL files in the **Dependencies** folder

To solve the problem, stop the **WzpSvc** app pool, and then delete all files in the **Dependencies** folder, which is located in (C:\Program Files (x86)\KMD\WorkZone\Process\Web\Services\Dependencies). In some cases, you may also have to stop the ScanJour

Process Mail Notification Agent and the ScanJour Process Push Notification Agent in Windows Services.

Users do not receive smartmails

Please see Troubleshooting in the WorkZone Operations Guide.

WorkZone Mass Dispatch

Install WorkZone Mass Dispatch

The manual installation procedure for WorkZone Mass Dispatch depends on whether you install Mass dispatch in a single-server or multi-server environment.

> **Important:**
>
> In a WorkZone environment with multiple servers, you must only install WorkZone Mass Dispatch on one server because mass dispatch processes must be started and completed on the same server.
>
> Install WorkZone Mass Dispatch on one server under the Default Web Site, and make sure that the **MassDispatchServiceUrl** parameter in the wzp_settings table is configured to point to this server. If you want to use HTTPS, you need a certificate on the server that you install WorkZone Mass Dispatch on.

- You must run WorkZone Mass Dispatch under the WorkZone Process service account. See Service accounts.
- By default, WorkZone Mass Dispatch is disabled after the installation. You enable it in WorkZone Configurator. Go to **Global** > **Feature settings**, select **Mass Dispatch**, and click **Save**.

Single-server environment

1. Copy the `KMD.WorkZone.MassDispatch.Setup.msi` file to your computer.
2. Execute the following command as administrator:

   ```
   msiexec /i <Path to the location of the msi file> ServiceDomain="<Domain>" ServiceUserName="sa_wzprocess" ServicePassword="<Password of the service user>"
   ```

   For example:

   ```
   msiexec /i C:\Users\testadmin\Desktop\KMD.WorkZone.MassDispatch.Setup.msi ServiceDomain="LMDOM" ServiceUserName="sa_wzprocess" ServicePassword="WZP"
   ```

Multi-server environment

Prerequisite:

- Ensure that HTTP/HTTPS (port 80/443) traffic is allowed from the web servers to the server where WorkZone Mass Dispatch is installed.
- If you use HTTPS, a server certificate is needed on the server where WorkZone Mass Dispatch is installed.

1. Copy the `KMD.WorkZone.MassDispatch.Setup.msi` file to your computer.
2. Execute the following command as administrator:

   ```
   msiexec /i <Path to the location of the msi file> SiteName="Default Web Site" ServiceDomain="<Domain>" ServiceUserName="sa_wzprocess" ServicePassword="<Password of the service user>"
   ```

   For example:

```
msiexec /i C:\User-
s\testadmin\Desktop\KMD.WorkZone.MassDispatch.Setup.msi
SiteName="Default Web Site" ServiceDomain="LMDOM" Ser-
viceUserName="sa_wzprocess" ServicePassword="WZP"
```

Configure WorkZone Process to use the WorkZone Mass Dispatch service in a multi-server environment

For WorkZone Process to use the WorkZone Mass Dispatch service, you must configure the Process parameter named **MassDispatchServiceUrl** to point to the URL of the service. Currently, you can set the parameter in the wzp_settings table using ScanSql.

Before you set the parameter, make sure it doesn't already exist. You can, for example, delete the parameter before you insert it.

```
DELETE from wzp_settings where module = 'WorkZone' and key =
'MassDispatchServiceUrl';
```

And then insert the parameter:

```
INSERT into wzp_settings(row_id, module, key, value,type) values
(wzp_settings$row_id.nextval, 'WorkZone', 'MassDis-
patchServiceUrl', 'https://<server name>/MassDispatch', 'URL');
```

Where `<server name>` is the fully qualified server name of the server that WorkZone Mass Dispatch is installed on.

Mass Dispatch access codes

You need to apply one or both of the two access codes below to users who will work with mass dispatch.

- Apply the **MASSDISPATCH** access code to users who should be able to start a mass dispatch.
- Apply the **MASSDISPATCHSEND** access code to users should be able to execute the actual mass dispatch.

Install and configure WorkZone PDF

WorkZone PDF is a WorkZone product that is used to convert existing documents to PDF. WorkZone PDF converts documents to either the default PDF format (PDF v1.7) or to the PDF/A format (PDF/A-3b). You can specify which PDF format to convert to during the WorkZone PDF installation. WorkZone PDF can be used as a standalone application or in combination with other WorkZone products.

Installation order

> **Prerequisite:** Create a user with the "Log on as a service" rights prior to installation.

To install and configure WorkZone PDF, follow the following steps:

1. Perform database configuration
2. Deploy reports
3. Install PDF Engine
4. Install PDF Crawler
5. Configure WorkZone PDF

Prior to the installation, please choose an installation scenario that is the most relevant to your organization.

Installation scenarios

The WorkZone product contains two modules:

- **The WorkZone PDF Engine** – It can be installed either as standard installation with pre-defined parameters or as a customized installation, where you can specify custom parameters.
- **The WorkZone PDF Crawler** – It can only be installed as a complete installation.

In Windows **Programs and Features**, all three modules are combined and appear as WorkZone.

In general, the following setup is recommended:

- Install WorkZone PDF Engine on the same server as WorkZone Content Server using the Real-time conversions profile.
- Install WorkZone PDF Crawler on a dedicated server because of the high demand on system resources. On small installations, however, it is possible to install WorkZone PDF Crawler on the same server where you run WorkZone Content Server.

> **Important:**
>
> - If you use multiple databases, you must install at least one instance of WorkZone PDF Crawler for each database.
> - To increase productivity of WorkZone PDF Crawler, you can install up to 99 its instances on a database.

The WorkZone may be installed in different installation scenarios depending on an organization's setup.

Cross Origin Resource Sharing (CORS)

If WorkZone PDF Engine services are to be requested from browsers or web clients from other domains (for example WorkZone Client and WorkZone Configurator applications running on a different host than PDF Engine), you must configure the Cross-Origin Resource Sharing parameters (**AllowedCorsOrigins** and **AllowedCorsHeaders**).

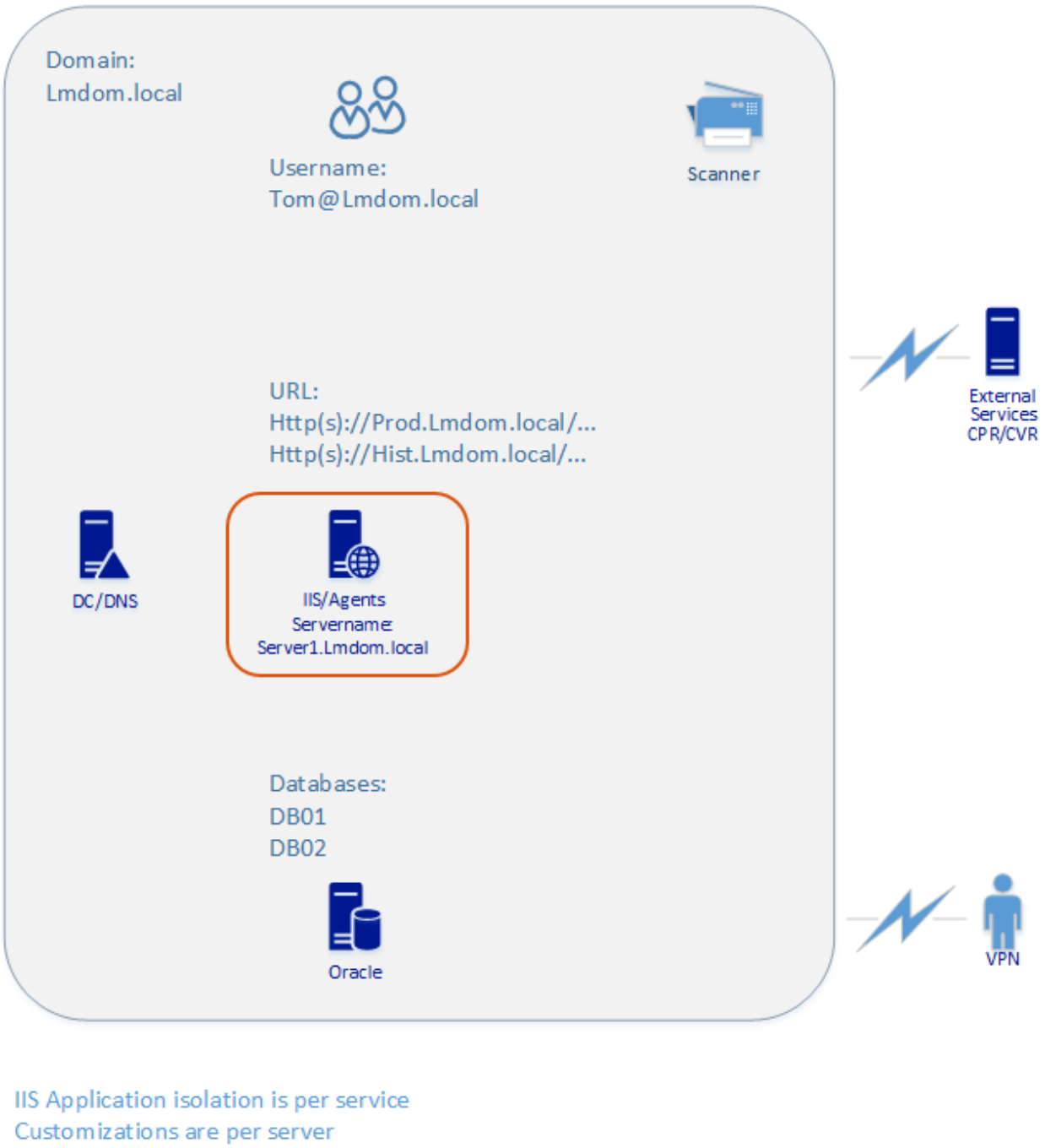
Scenario 1: Install on one server

In this scenario, all required WorkZone products are installed on one single server.

To preview documents in WorkZone Client, you need to install:

- WorkZone Content Server (IIS)
- OData
- WorkZone Client
- WorkZone PDF Engine

For users to be able to create PDF documents, you must install the WorkZone PDF Crawler



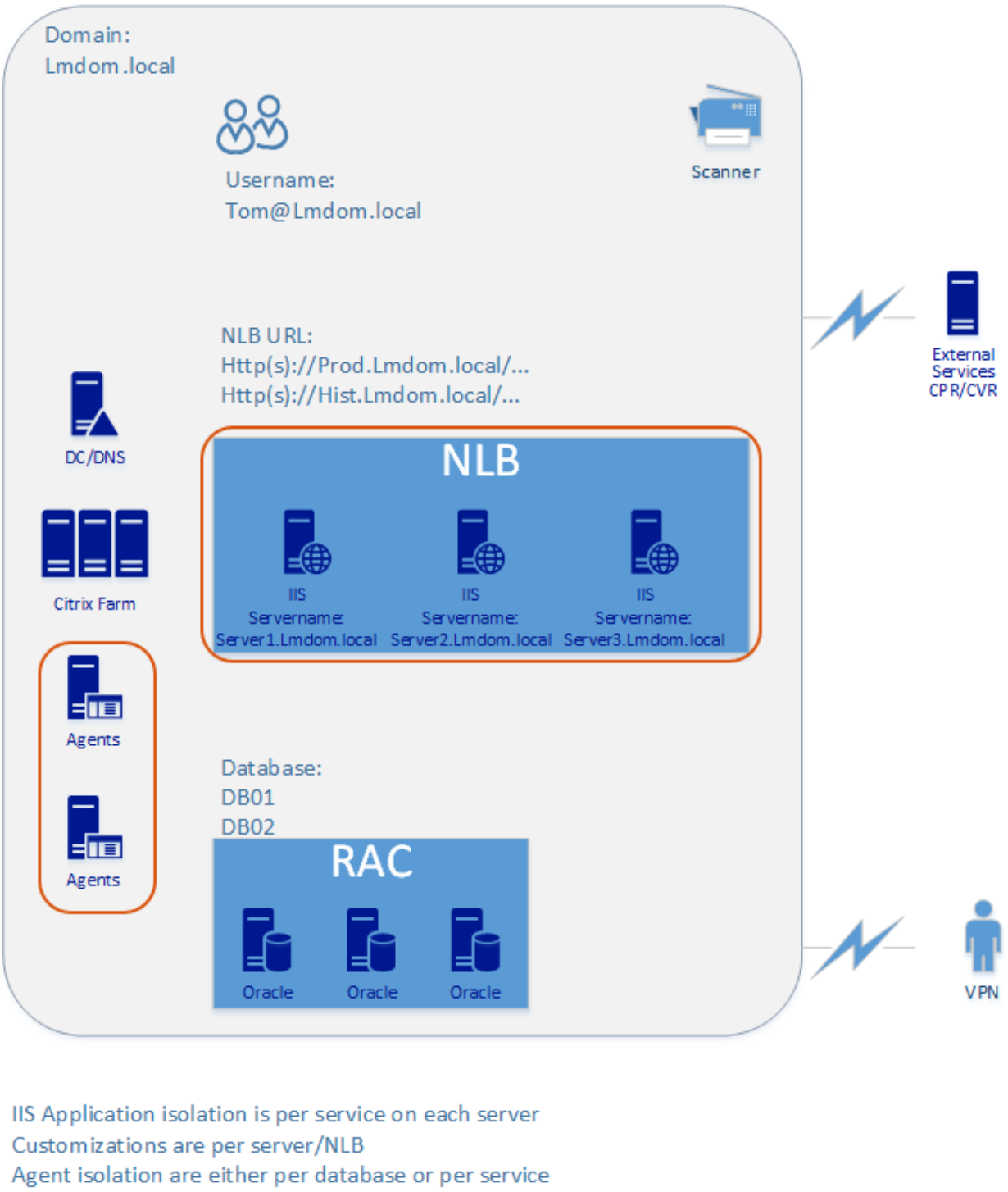
Scenario 2: Install on multiple servers

This scenario includes multiple servers and agent servers.

To preview documents in WorkZone Client, you need to install the following WorkZone products on each server:

- WorkZone Content Server (IIS)
- OData
- WorkZone Client
- WorkZone PDF Engine

To create PDF documents, you must install WorkZone PDF Crawler on one or more agent servers.



Perform database configuration

You only need to perform the database configuration once for every WorkZone database you are using.

1. Double-click the **KMD WorkZone PDF.exe** file. On the **Welcome to the KMD WorkZone PDF Installation Wizard** page, click **Next**.
2. On the **WorkZone PDF Products** page, click **Database Configuration**.
3. On the **License Agreement** page, you must read and accept the license agreement terms before you can continue the installation. Select the **I accept the terms of this license agreement** check box and then click **Next**.
4. On the **Database Configuration** page, select the WorkZone database and enter login credentials to access the data (Username and Password). Click **Next** to continue.
5. On the **Database Configuration** page, specify the location of the OData service, Crawler OAuth2 Client Id, and Crawler OAuth2 Client Secret, as the WorkZone PDF Crawler application uses the OData module to connect to WorkZone. Click **Next** to continue.
   The Crawler OAuth2 Client Id and Crawler OAuth2 Client Secret parameters can be defined as any strings allowed in the WorkZone Content Server OAuth2.
6. On the **Ready to perform Database Configuration** page, click **Configure**.

You can edit WorkZone PDF parameters in WorkZone Configurator, the WZPDF_CONFIGURATION table, or the Web.config file. See **Custom parameters** below.

Custom parameters

WorkZone PDF Engine parameters

Parameter	Description
Watermark	Specify the text to be used as the document watermark.
WatermarkStyle	Defines the default style of the watermark. This parameter must be in JSON format. You can specify color, transparency, and font as follows: • **Color:** Any valid html string format such as standard color name, hex

Parameter	Description
	value, and RGB colors. **Example:** Standard color name: Red Hex value: #FF0000 RGB: 255,0,0 • **Transparency:** Transparency ranges from 0 to 100 where 100 represents full opacity. • **Font:** The name of the font to be used for the watermark. You do not need to specify font size, the watermark will be sized to fit the page automatically. All the parameter arguments listed above are optional. Watermark example Define a watermark style using a red Verdana font with medium transparency. `{ Color: "Red", Transparency: "55", Font: "Verdana"}` The default setting is an empty string.
ActionsOnDocumentBeforeConversion	When a document is being converting to PDF, review information such as comments, tracked revisions (changes), notes, and annotations can be hidden or not on the final PDF document. You can define the setting for each specific document type and for each specific review information. To do this, edit and use the following JSON: { Pdf: { Annotations: 'Show'/'Hide'/'Flatten', Forms: 'Show'/'Flatten'}, Word: { Comments: 'Show'/'Hide', Revisions: 'Accept'/'Show'/'Reject' },

Parameter	Description
	where: • `Show` - The relating review information will be shown (included) to the final document. • `Hide` - The relating review information will be hidden (excluded) from the final document. • `Accept` - The tracked revisions (changes) will be applied and hidden on the final document. • `Reject` - The tracked revisions (changes) will be declined and hidden on the final document. • `Flatten` - The relating controls (text boxes, check boxes, annotations, etc.) will be included as regular content (text and images) to the final document. If you upgrade WorkZone PDF from 2019.2 version or earlier, be aware that the following backward compatibility will be applied automatically: **Old values** **New values**

Parameter	Description	

	true	{
		Pdf: { Annotations: 'Hide' },
		Word: { Comments: 'Hide', Revisions: 'Accept'},
		Excel: { Comments: 'Hide', Revisions: 'Accept' },
		PowerPoint: { Comments: 'Hide', Notes: 'Hide' }
		}

	false	{
		Pdf: { Annotations: 'Show' },
		Word: { Comments: 'Show', Revisions: 'Show' },
		Excel: { Comments: 'Show', Revisions: 'Show' },
		PowerPoint: { Comments: 'Show', Notes: 'Show' }
		}

	You can change the settings manually if it is relevant.	
FailIfOutOfBounds	If set to **False**, the document is converted even if the content exceeds the bounds of a	

Parameter	Description
	document. If set to **True**, the content fails to convert. The default setting is **False**. **Note:** Documents with the states **UL** (Locked), **ARK** (Archived), and **AFS** (Closed) will not be checked for content which is out of bounds even if the parameter is set to **True**. Documents with these states are locked in their final state regardless of content that exceeds the page bounds.
BypassBoundaryCheckForFiles	Specifies which file types are to be bypassed when boundaries of objects in the files are checked during PDF conversion. The syntax is a string of comma-separated file extensions, for example: pdf, xps, docx. The default file extension is pdf, meaning the check for out-of-bounds objects in pdf documents will be bypassed.
OutputPdfCompression	Compresses the PDF output to reduce its size. This parameter is particularly important as large documents may take a long time to download from a server. The default setting is **True**.
OutputPdfWebOptimization	Optimizes the PDF output for the web. This parameter is particularly important as regards large documents that may take a long time to download from a server. The default setting is **True**.

Parameter	Description
OutputPdfArchiving	Defines the output PDF format. Select **False** to convert to a PDF format for generic usage (PDF 1.7). Select **True** to convert to a PDF format that is used for long-term storage (PDF/A-3b). The default setting is **False**.

Header	Defines the content of the header.
	
	You can specify the header content as normal text, field values from the database, document metadata or by using the following Microsoft field codes:
	
	• **{Title}:** The document title.
	• **{Date}:** The current date aligned with the country date standard.
	• **{Page}:** The current page number in the document.
	• **{NumPages}:** The total amount of pages in the document.
	
	Custom header text example
	
	`<setting name="Header" serializeAs="String"><value> 'My Custom Header'</value></setting>`
	
	Field code header example
	
	`<setting name="Header" serializeAs="String"><value> {page}</value></setting>`

HeaderStyle	Defines the default style of the header that will be used if the style is not specified in the request.

Parameter	Description
	This parameter must be in JSON format. You can specify the formatting of the header, for example, bold or italic, and which font to use. All parameters are optional. The default setting is an empty string. Header style example Print the header in bold using Arial as font. `{ "Bold": true, "Font": "Arial"}`

Footer	Defines the content of the footer.
	You can specify the footer content as normal text, field values from the database, document metadata, or the following Microsoft field codes can be used:
	• **{Title}:** The document title.
	• **{Date}:** The current date based on defined culture settings.
	• **{Page}:** The current page number in the document.
	• **{NumPages}:** The total amount of pages in the document.
	Custom footer text example
	`<setting name="Footer" serializeAs="String"><value> 'My Custom Footer'</value></setting>`
	Field code footer example
	`<setting name="Footer" serializeAs="String"><value> " Page`

Parameter	Description
	`{page} of {NumPages}"</value></setting>`
FooterStyle	Defines the default style of the footer that will be used if the style is not specified in the request. This parameter must be in JSON format. You can specify the formatting of the header, for example, bold or italic, and which font to use. All parameters are optional. The default setting is an empty string. Footer style example Print the footer in bold using Arial as font. `{ "Bold": true, "Font": "Arial"}`
ConvertWithAttachments	Defines whether a document is converted with or without attachments. The default setting is **True**, which means that all document attachments are converted.
IncludeDocumentCoverPage	Specifies whether or not to create a separate cover page for each document in a multi-document report. The default setting is **False**, which means individual documents in a multi-document.
Target	Specify which WorkZone PDF Engine instance you want to apply custom parameters for. You are effectively naming the PDF Engine instance in order to uniquely identify it. Once an instance has been named, any Engine parameters specified in the data-

Parameter	Description
	base (WZPDF_CONFIGURATION table) for that specific instance will be applied to the instance. The Target parameter is a case-sensitive string with the default value PDFENGINE. The default value may be changed to any string value that corresponds to the value in the **Target** field in the WZPDF_ CONFIGURATION table. If you specify a Target parameter which does not exist in the WZPDF_ CONFIGURATION table, the request will fail with a 404 Not Found error and the error message: *The configuration for target"..." is not found.* You must uniquely name each PDF Engine instance (for example, RenderForProcess, RenderForMobile, etc.) you expect to use in the **Target** field of the WZPDF_ CONFIGURATION table. **Tip:** Create the required targets in the WZPDF_CONFIGURATION table before specifying Target parameters in order to have a list of valid PDF Engine instance names.
FailIfMissingFonts	Defines whether WorkZone must check availability of missing fonts in a document before its conversion to PDF. By default, the parameter is disabled, that is, the missing fonts are not checked. Note that WorkZone checks missing fonts on the IIS server only for par-

Parameter	Description
	ticular file types. See the list of file types in the **Font check** column in the Supported file types table in the Administrator's Guide for WorkZone PDF. > Important: During document conversion to PDF/A, missing fonts are always checked, regardless the value of `FailIfMissingFonts`. This behavior is aligned with the PDF/A specification.
FallbackFont	Defines a font that substitutes a missing font when a document is converted to PDF or PDF/A format.

Deploy reports

Standard reports

Standard reports for the KMD WorkZone product are not included in the standard installation of the KMD WorkZone product and are instead installed as part of the WorkZone installation.

WorkZone standard reports must be installed as a separate installation step as part of the Database Configuration installation step when installing WorkZone. During the installation of standard report templates, the **Report** table is created.

Custom reports

If you have created your own report templates for customized reporting requirements in your organization, you can deploy these custom report templates automatically when you set up the Database Configuration during installation of a new version of WorkZone or when updating your existing version.

To do this, you must create a folder called **Reports** in the same folder where the **KMD WorkZone PDF.exe** is located. Place all custom report templates that you want deployed during an installation or update in the **Reports** folder.

When the **Database Configuration** option is run during the installation process, any reports placed in the **Reports** folder will be automatically deployed to the WorkZone Client by the installation process.

> **Note:** Custom report templates in the **Reports** folder will overwrite any standard report templates.

Microsoft Power BI reports

KMDWorkZone supports Microsoft Power BI reports and the WorkZone installation process includes standard WorkZone Power BI (.PBIX) reports. The six standard BI reports are found in the **Power BI** sub-menu in the **Reports** menu of the WorkZone Client.

> **Note:** To utilize the Power BI reports, the Microsoft Power BI client must be installed on the local machine.

Deploy silently

To deploy report templates only, specify these parameters:

Parameter	Required?	Default value	Meaning
-dbconfig	Yes		Deploying templates mode.
-db	No	The first defined database (DSN) on the target server.	Specify database name.
-dbuser	No	SJSYSADM	Specify user name.

Parameter	Required?	Default value	Meaning
-dbpassword	Yes		Specify password.
-odata	No	The first defined OData URL on the target server.	URL to OData application.
-CrawlerClientId	No	WZPDF.CRAWLER	These parameters can be defined as any strings allowed in the WorkZone Content Server OAuth2.
-CrawlerClientSecret	Yes		

```
Example: "KMD WorkZone PDF.exe" -DbConfig -Db:db01 -dbuser:
[user] -dbpassword:[password] -OData:"ht-
tps://db01.lmdom.local/OData"
```

Install WorkZone PDF Engine

Install manually with standard settings

If you install WorkZone PDF Engine for working with other WorkZone products, you must select the **Real-time conversions** installation profile which is the default profile.

The following WorkZone features are automatically enabled by the **Real-time conversions** profile:

- Preview of documents in WorkZone Client.
- Print reports for WorkZone Client and WorkZone Process.

The **Real-time conversions** installation profile also:

- Installs WorkZone PDF Engine under the **WorkZone** web site.
- Identifies WorkZone PDF Engine by the URI `<WorkZone URL>/Render`, for example https://db01/render.
- Creates an application pool with the default name **WZRender**. You can rename the Application Pool Name if necessary.
- Uses Windows authentication.

Note: Custom parameters cannot be specified during installation when using the **Real-time conversions** profile. If you need to define custom parameters for the WorkZone PDF Engine, you must either select the **Custom** installation profile or wait until the installation has completed and then define any custom parameters after the installation.

See WorkZone PDF Engine custom parameters.

To install the WorkZone PDF Engine with standard settings:

1. Double-click the **KMD WorkZone PDF.exe** file. On the **Welcome to the KMDWorkZone Installation Wizard** page, click **Next**.
2. On the WorkZone **Products** page, click **WorkZone PDF Engine** to start the installation of WorkZone PDF Engine.
3. On the **WorkZone PDF Engine** page, click **Install**.
4. On the **Installation Profiles** page, select **Real-time conversions** to install the WorkZone PDF Engine with standard settings and then click **Select**.
5. On the **License Agreement** page, you must read and accept the license agreement terms before you can continue the installation. Select the **I accept the terms of this license agreement** check box and then click **Next**.
6. On the **Prerequisites** page, click **Verify** to ensure all prerequisites are present on the local machine and then click **Next**.
7. On the **WorkZone PDF Engine Settings** page, define the **Application Name**. You cannot define any other settings due to the selected **Real-time conversion installation** profile. Click **Next** to continue.

8. On the **WorkZone PDF Engine OData Settings** page, specify the location of the OData Service as well as user credentials for accessing the OData service. Click **Next** to continue.
9. On the **Ready to installWorkZone PDF Engine** page, click **Install** to start the installation.

If you want to specify your own default parameter values for the WorkZone PDF Engine application during the installation, you can specify these in the **Database Configuration** installation option or select to install WorkZone PDF Engine with customized settings. See Perform database configuration.

Install manually with customized settings

If you want to customize the WorkZone PDF Engine installation to match the specific needs of your organization, you must select the **Custom** installation profile.

If you want to change the custom parameter setup after installation, you can edit the parameters in the WorkZone PDF Engine Web.config file. The WorkZone PDF Engine Web.config file is located: `C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\Render`.

See WorkZone PDF Engine custom parameters.

To install the WorkZone PDF Engine with customized settings:

1. Double-click the **KMD WorkZone PDF.exe** file. On the **Welcome to the KMDWorkZone Installation Wizard** page, click **Next**.
2. On the WorkZone **Products** page, click **WorkZone PDF Engine** to start the installation of WorkZone PDF Engine.
3. On the **WorkZone PDF Engine** page, click **Install**.
4. On the **Installation Profiles** page, select **Custom** to install the WorkZone PDF Engine with customized settings and then click **Select**.
5. On the **License Agreement** page, you must accept the license agreement terms before you can continue the installation. Select the **I accept the terms of this license agreement** check box and then click **Next**.
6. On the **Prerequisites** page, click **Verify** to ensure all prerequisites are present on the local machine and then click **Next**

7. On the **WorkZone PDF Engine Settings** page, define the settings for the PDF Engine. The settings already contain the default values, but you can overwrite the settings if necessary.
   The **FQDN** field is automatically filled in with the current domain but you can change it, for example if you want to set up a test system to run in a different domain. In the **Host Headers** field, you can enter the host headers that you have created.
   Click **Next** to continue.
8. On the **WorkZone PDF Engine Parameters** page, specify the values of the parameters you want to customize.
   If you want to change the WorkZone PDF Engine parameters after installation, you can edit the parameters in the WorkZone PDF Engine Web.config file.
9. On the **Ready to install WorkZone PDF Engine** page, click **Install** to start the installation.

Install silently

To install WorkZone PDF Engine under a new site, follow this procedure:

1. Open the **Command prompt** window as administrator.
2. Type the path to the `KMD WorkZone PDF.exe` file.
3. Specify the product name `-engine`.
4. Specify parameters.

Parameter	Required?	Default value	Meaning
-i	Yes		Installation mode.
-profile	No	"Typical"	Installation profiles: • **Typical** - A predefined configuration. • **Custom** - Specify

Parameter	Required?	Default value	Meaning
			the application name under an existing web site, application pool name, authentication method, and WorkZone PDF Engine parameters.
-app	No	"Render"	Web application name.
-pool	No	"WzRender"	Application pool name for web application.
-auth	No	"Anonymous"	Authentication method for web application (Windows, Anonymous). **Note:** Can only be used with the **Custom** profile.
-params	No	`"Compress PDF output=True, Default footer style={}, Default header style={}, Hide review information=True, Optimize PDF output for the web=True, PDF output format=Default, Suppress content that exceeds page bound-`	List of custom parameters for PDF Engine.

Parameter	Required?	Default value	Meaning
		`s=False, Watermark style={}"`	
-Allowed CorsOrigin	No	*	Define which web client applications executed in a browser hosted on other domains will be able to perform CORS requests to the server. An origin for the **AllowedCorsOrigin** parameter[1] must be defined as: <scheme>://[<hostname>.]<host>[:<port>], for example Https://WZClient if WorkZone Client is hosted on Https://WZClient and the rest of WorkZone services are hosted on another domain, such as Https://WZServices. Origins are separated with semi-colons ";". When using Cross-Origin Resource Sharing (CORS) with WorkZone , this parameter should be set to the specific origins as most browsers will prevent passing credentials or tokens to the service when the wild card (*) is used as the origin.

Parameter	Required?	Default value	Meaning
			Using the wild card (*) origin means the PDF service is open for every origin. It is used when the wild card origin (*) is the only origin that is set in the configuration file or in the corresponding system environment variable, or the origin of the request is not found and the **AllowedCorsOrigins** parameter contains the wild card origin (*). **Example**: The following parameter in the Web Config file: <add key="allowCorsOrigin" value="*" /> will fail unless the wild card origin "*" is replaced with the specific origins of the web client to be accessed.
-AllowedCorsHeader	No	Origin;X-Requested-With;Content-Type;Accept;Accept-Language;OData;Authorization	Used in a response to OPTIONS preflight request. Indicates which headers can be used during the actual HTTP CORS request. The **AllowedCorsHeaders**[1]

Parameter	Required?	Default value	Meaning
			parameters corresponds to Access-Control-Allow-Header response header (ACAH) and acts as an answer to request's Access-Control-Request-Headers request header. The **AllowedCorsHeaders** parameter can be configured with: - "*" The Access-Control-Allow-Header will contain headers requested by the request as well as specific PDF headers. - specified headers (ACAH header will contain these headers as well as specific PDF headers). - both * and specified headers (ACAH will contain headers from the configuration and headers requested by the request as well as specific PDF headers).

[1] These parameters are also mapped to the following system environment variables on the server:

- WORKZONE_PDF_CORS_ALLOWEDORIGINS
- WORKZONE_PDF_CORS_ALLOWEDHEADERS

System environment variables take precedence over the parameters defined in the web.config files.

There is one additional common parameter, which you can use to extend the behavior of the installation:

-l	Log, which enables text log output that can be used to review and find issues during the installation, update, or uninstallation process.

Example: Typical installation

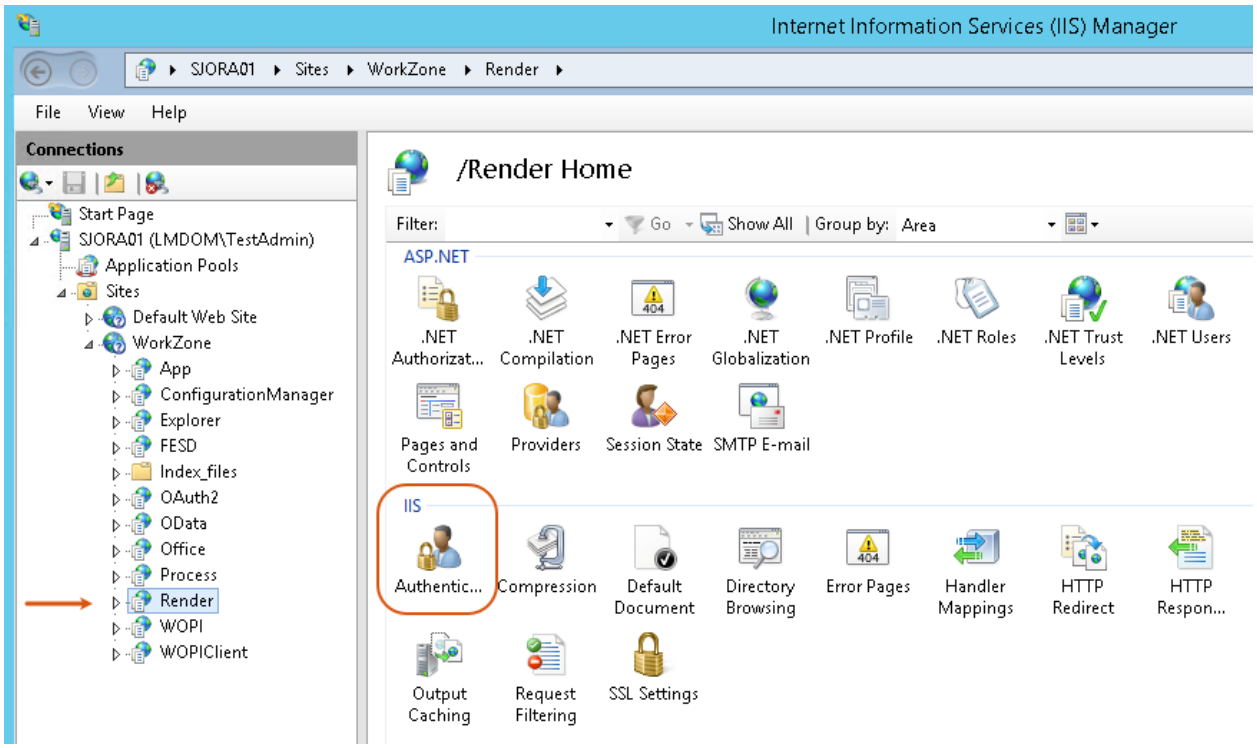
```
"KMD WorkZone PDF.exe" -Engine -i -profile:Typical -l:"c:\my-log.txt"
```

Example: Custom installation

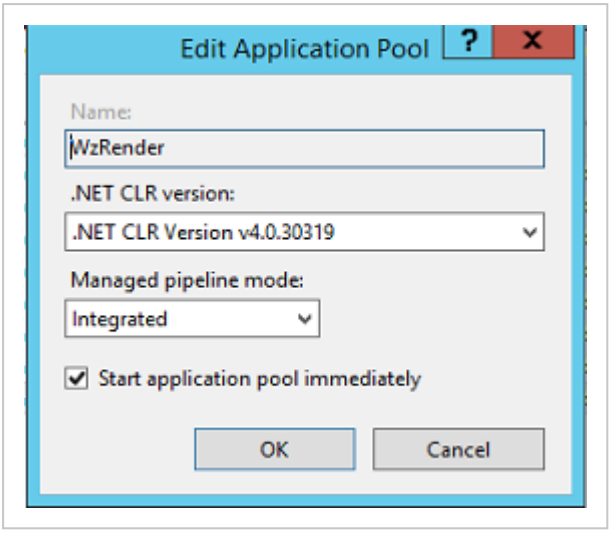
```
"KMD WorkZone PDF.exe" -Engine -i -profile:Custom -app:"Default web site/Pdf" -pool:WzRender -auth:Windows -params:"Hide review information=True, PDF output format=Default, Optimize pdf output for the web=True, Suppress content that exceeds page bounds=False" -l:"c:\mylog.txt"
```

Verify the installation

1. In Internet Information Services (IIS) Manager, select **Render**.



2. Double-click **Authentication**.
3. Verify that settings specified during installation are correct.
4. Navigate to **Application Pools** and double click on the WZRender application pool that was created during installation. The **Edit Application Pool** dialog box displays.
5. Under **.NET CLR Framework version**, verify that `.NET CLR Framework v.4.0.30319` for the application pool which is used for the WorkZone PDF Engine.



6. Click **OK**.
7. If you selected the **Custom** installation profile to use WorkZone PDF Engine with host headers, you can verify the binding between the web site and the appropriate host header. Select the web site under which the PDF service is installed, and then click **Bindings** in the **Actions** menu.

In the **Site Bindings** dialog box, verify that the bindings to the appropriate host headers are created.

Install WorkZone PDF Crawler

> Prerequisite: After the installation, you must enable WorkZone PDF Crawler in WorkZone Configurator. To do this, go to **Global > Feature settings > WorkZone PDF**, select **WorkZone PDF Crawler**, and click **Save**.

Install manually

1. Double-click the **KMD WorkZone PDF.exe** file. On the **Welcome to the KMDWorkZone Installation Wizard** page, click **Next**.
2. On the WorkZone **Products** page, click **WorkZone PDF Crawler** to start the installation of WorkZone PDF Crawler.

3. On the **WorkZone PDF Crawler** page, click **Install**.
4. On the **License Agreement** page, you must read and accept the license agreement terms before you can continue the installation. Select the **I accept the terms of this license agreement** check box and then click **Next**.
5. On the **WorkZone PDF Crawler OData Settings** page, specify the location of the OData service, Crawler OAuth2 Client Id, and Crawler OAuth2 Client Secret, as the WorkZone PDF Crawler application uses the OData module to connect to WorkZone. Click **Next** to continue.
   The Crawler OAuth2 Client Id and Crawler OAuth2 Client Secret parameters can be defined as any strings allowed in the WorkZone Content Server OAuth2.
6. On the **WorkZone PDF Crawler Credentials** page, specify the User Principal Name (UPN) and Password to be used to run the WorkZone PDF Crawler service. By default, the UPN is defined as *system* but you can change it to the user with the "Log on as a service" rights. Click **Next** to continue.
7. On the **Ready to installWorkZone PDF Crawler** page, click **Install** to start the installation.

Install silently

1. Open the **Command prompt** window as administrator.
2. Type the path to the KMD WorkZone PDF.exe file.
3. Specify the installation mode `-i`.
4. Specify the product name `-crawler`.
5. Specify parameters:

Parameter	Required	Default value	Meaning
-odata	no	The first defined OData URL on the target server	URL to OData application.

Parameter	Required	Default value	Meaning
-CrawlerClientId	no	WZPDF.CRAWLER	These parameters can be defined as any strings allowed in the WorkZone Content Server OAuth2.
-CrawlerClientSecret	yes		
-user	no	*system*	Name of the WorkZone PDF Crawler user with **Log on as a service** rights. The user is used to run the WorkZone PDF Crawler service. See Create WorkZone PDF user with the "Log on as a service" rights.
-password	yes, if the user is not *system*		The password of the Crawler user specified for `-user` parameter.
-l	no	The TEMP folder of the current user under which the installation is running	Log, which enables text log output that can be used to review and find issues during the installation, update, or uninstallation process.

Example:

```
"KMD WorkZone PDF.exe" -crawler -i -odata:"https://db01/OData" -CrawlerClientId:WZPDF.CRAWLER -CrawlerClientSecret:[secret] -user:[user] -password:[password] -l:"C:\Logs\Crawler.log"
```

To install more than one instance of PDF Crawler you need to run the installation command for every instance.

Configure WorkZone PDF

Configure WorkZone PDF parameters

It is recommended to perform further configuration in WorkZone Configurator. See WorkZone PDF settings in the WorkZone Configurator Administrator guide.

Configure WorkZone PDF Engine

> **Tip:** You can find list of parameters and their descriptions in the WorkZone PDF Engine parameters table.

During installation, you can define WorkZone PDF Engine custom parameters in:

- in WorkZone Configurator – preferable in the WorkZone environment
- in the Web.config file
- as API calls

After installation, you can edit the parameters:

- in WorkZone Configurator – preferable in the WorkZone environment
- in the Web.config file.

The WorkZone PDF Engine Web.config file is located: `C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone\Render`.

You can find API reference documentation under the WorkZone PDF Engine under /Help uri, for example, https://db01/Render/Help.

Any changes to the WorkZone PDF Engine parameter settings will take effect immediately.

Parameter priorities

The following list illustrates the priority ranking of each WorkZone PDF Engine parameter, with the highest ranked parameter placed first.

1. **Body**: Parameters specified in the body of the request.
2. **HTTPS Header**: Parameters specified in the request header of the API call.
3. **Database settings**: WorkZone PDF Engine settings specified by using the WorkZone Configurator or by using an SQL tool, for example Oracle's SQL Developer to update settings directly into the database in the **WZPDF_CONFIGURATION** table.
4. **Web.config settings**: Settings specified in the Web.config file.
5. **Installation default values**: the settings specified when the WorkZone PDF Engine was initially installed.

Custom parameters by instance

You can define parameters for each instance of the WorkZone PDF Engine, enabling you to set different parameters for the various usages you might invoke for the WorkZone PDF Engine, for example, defining parameters for creating pdf documents through the PDF Engine and then defining parameters for the same PDF Engine but different instance when used by the WorkZone SmartPost module.

Create parameter settings for PDF Engine instances

Since WorkZone PDF Engine custom parameter settings are stored in the WZPDF_CONFIGURATION table, you should first create the parameter settings in the WZPDF_CONFIGURATION table for each instance you expect to use.

Creating the parameter settings first will give you a list of valid PDF Engine instances as well as their unique names, making it easier to specify which instance to invoke in the PDF Engine Web.config file later.

Entries in the WZPDF_CONFIGURATION table can be made using an SQL tool, such as Oracle's SQL Developer distributed with the WorkZone product.

Example: Create parameter settings for SmartPost PDF Engine instance

In this example, a new set of parameter settings is created in the WZPDF_CONFIGURATION table for the PDF Engine instance named "SmartPost".

```
INSERT INTO WZPDF_CONFIGURATION(TARGET, NAME, CUSTOM_VALUE)
VALUES('SmartPost', 'Watermark', 'PROTECTED COPY');
```

Unique instance names

You must uniquely name each PDF Engine instance (for example, RenderForProcess, RenderForMobile, etc.) you expect to use in the **Target** field of the WZPDF_CONFIGURATION table.

Once you have created the PDF Engine instances you want to use and defined the custom parameters for each individual instance, these parameters will be applied to the invoked instance.

Default instances

The WZPDF_CONFIGURATION table contains one named instance with the default value: PDFENGINE. You can specify as many instances in the WZPDF_CONFIGURATION table as you need.

Configure WorkZone PDF Crawler

You can set up custom parameters at the time of installation, see Install or update database configuration settings. After the installation, you can set up custom parameters through WorkZone Configurator, see Configure WorkZone PDF.

Note: If you set custom parameters via WorkZone Configurator, the changes will take effect in the next service iteration. A regular service iteration takes a few minutes, but it depends on the number of files, their size, and different settings.

Alternatively, you can define the configuration settings directly in the **WZPDF_CONFIGURATION** table using SQL scripts or by using an SQL tool such as Oracle's SQL Developer. Parameters will be applied to all instances of the WorkZone PDF Crawler.

Parameter	Description
ProcessingRetries	Specifies how many times WorkZone PDF Crawler tries to convert a document. The parameter is used when document conversion exceeds `ProcessingTimeout` or when you have installed multiple instances of WorkZone PDF Crawler and two crawlers try to convert the same document at the same time. In this case, WorkZone PDF Crawler may pause and then try to convert the document again. The default value is **3**.
ProcessingTimeout	Specifies a time-out for conversion. When time-out is exceeded, an error message is written to the **DVS_RENDER_MESSAGE** table. The default value is **5** minutes.

Define HTTP redirect rules

In order to support offloading and different scalability scenarios, you can install the WorkZone PDF Engine on separate web servers and then create redirect rules from one server to another or to a farm of servers, each with a WorkZone PDF Engine installed.

The redirect rules can be defined on the web server using Microsoft Internet Information Services (IIS) configuration settings.

For more information on defining redirect rules, see HTTP redirects.

Troubleshooting

> **Note:** These steps are not interdependent and can be performed in any order.

General troubleshooting flow:

Issue	DB Config	PDF Engine	PDF Crawler
Any issues	Check the Microsoft Windows **Event Viewer** form. See The Event Viewer.		
Installation	Run silent installation with logging enabled. See Install silently.		

Issue	DB Config	PDF Engine	PDF Crawler
fails			
Database is not accessible	Check names for TSN and DNS.		
PDF Engine web service is not accessible (error 500)		Verify the installation in IIS.	
Database errors	Check the tables: • WZPDF_UNRENDERABLE • WZPDF_CONFIGURATION_INFO • WZPDF_CONFIGURATION	Check the tables: • REPORT • REPORT_NAME • REPORT_DESCRIPTION • REPORT_RECORD • REPORT_REPORT	Check the tables: • Perform a select from the **dvs_render_info** table for the needed document. • Check that the policy is valid and enabled (`enabled = "J"`) in the **dvs_policy** table for the needed document.
You get an unexpected result		Check the corresponding website's settings in the Administrator's Guide for	Check the corresponding Crawler settings in the

Issue	DB Config	PDF Engine	PDF Crawler
		WorkZone Configurator.	Administrator's Guide for WorkZone Configurator.
Access errors	Check whether database configuration settings are correct. See Perform database configuration.	Verify the authentication settings in IIS. See Verify the installation.	• Enable logging in WorkZone PDF Crawler. See WorkZone PDF Crawler logs. Analyze the logs. • Check the rights of the user who runs the service.
A particular document cannot be converted		1. Open the file that failed to be converted and ensure that it's not damaged. 2. Try to perform a manual PDF conversion for a dif-	Enable logging in WorkZone PDF Crawler. See WorkZone PDF Crawler logs. Analyze the logs.

Issue	DB Config	PDF Engine	PDF Crawler
		ferent file, for example, convert *.txt to *.pdf.	
Other issues	If troubleshooting does not solve the issue, please create a support case with KMD support and include error messages, log files, or document files depending on the issue.		

See also:

Troubleshooting in the WorkZone PDF Administrator Guide.

Install WorkZone I/O Manager

WorkZone I/O Manager is based on the 3rd party technology Lasernet from Formpipe. Lasernet is embedded in the WorkZone platform, allowing you to configure a variety of input and output management aspects with WorkZone.

See **Lasernet - Installation** for step-by-step instructions on how to install Lasernet 9.

A typical setup and integration of WorkZone I/O Manager with WorkZone includes the following tasks:

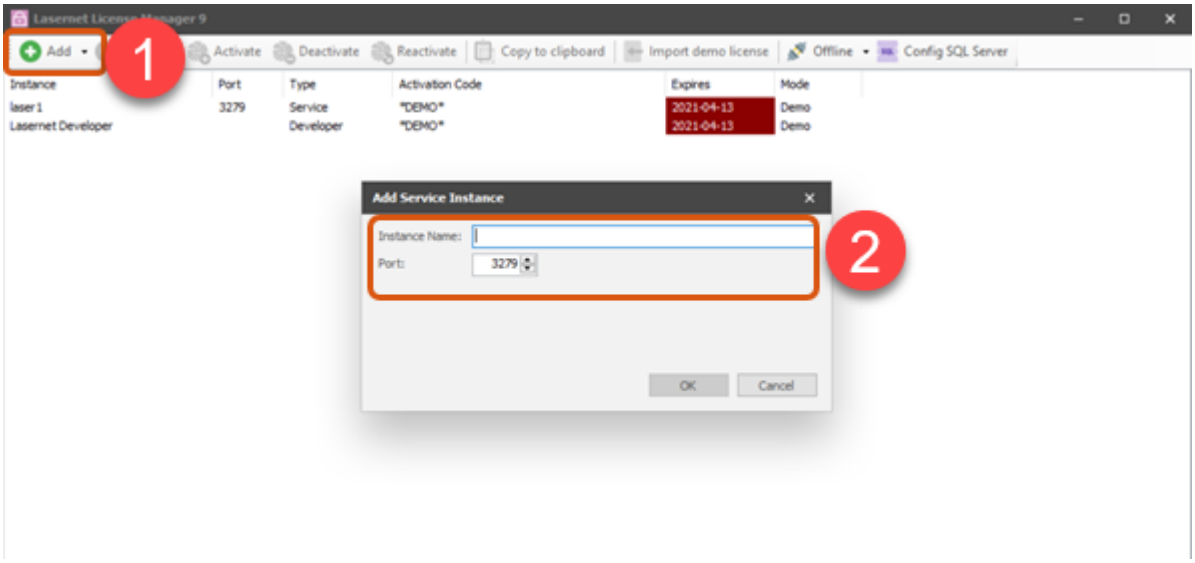
- Add license
- Set up Developer access
- Configure web server
- Set up web server (developer side)
- Set up web server tasks
- Create new modifiers (via HTTP request)
- Create new modifiers (via scripts)
- Save changes (create a commit)
- Start a workflow
- Add a scheduler

Add license for WorkZone I/O Manager

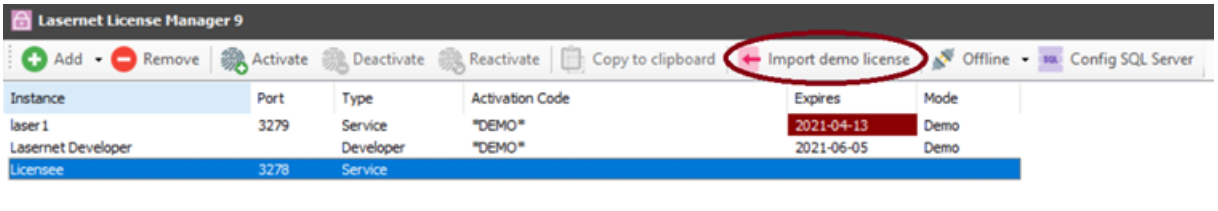
WorkZone I/O Manager requires a license.

Add license

1. Under **Lasernet** general applications, click **Lasernet License Manager.**
2. Click **Add**.
3. In the **Add Service Instance** dialog, specify **Instance name** and **Port** (if default value is not correct for your usage).



4. Click **OK**. The new service instance should appear on the list.
5. Select your newly created service instance, and click **Import demo license**.



6. Import license from the disk drive, and click **Activate**.
7. If license is correct, the service instance will be displayed as activated.

See also:

- Set up and configure WorkZone I/O Manager
- Additional common tasks with WorkZone I/O Manager

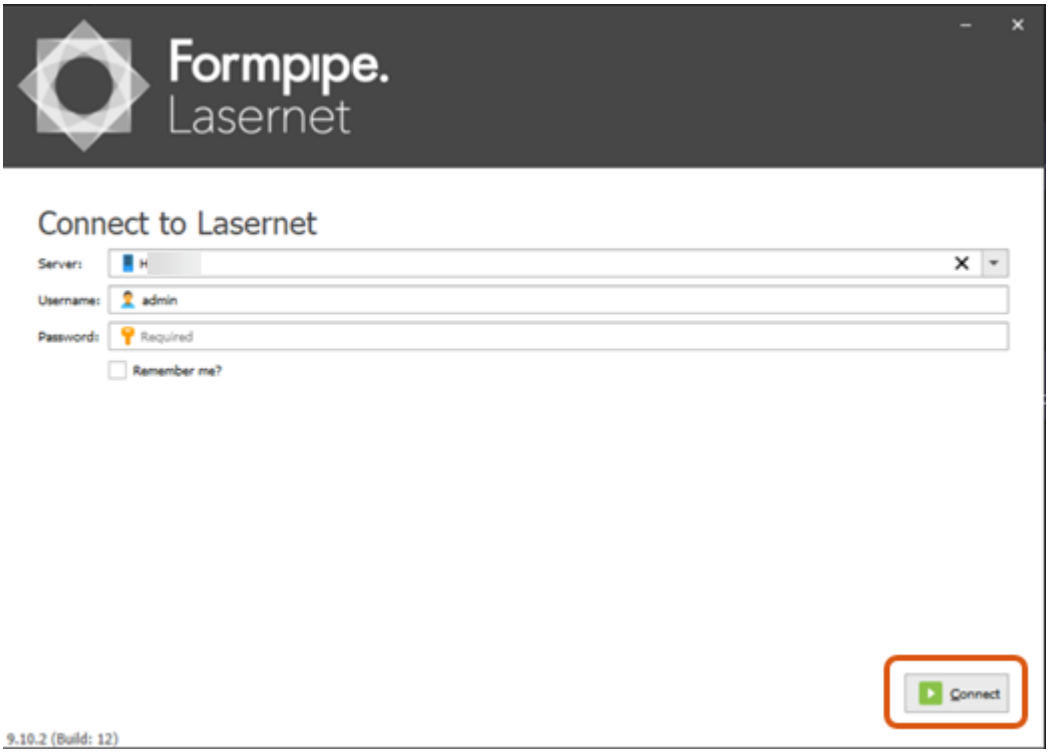
Set up and configure WorkZone I/O Manager

Set up Developer access

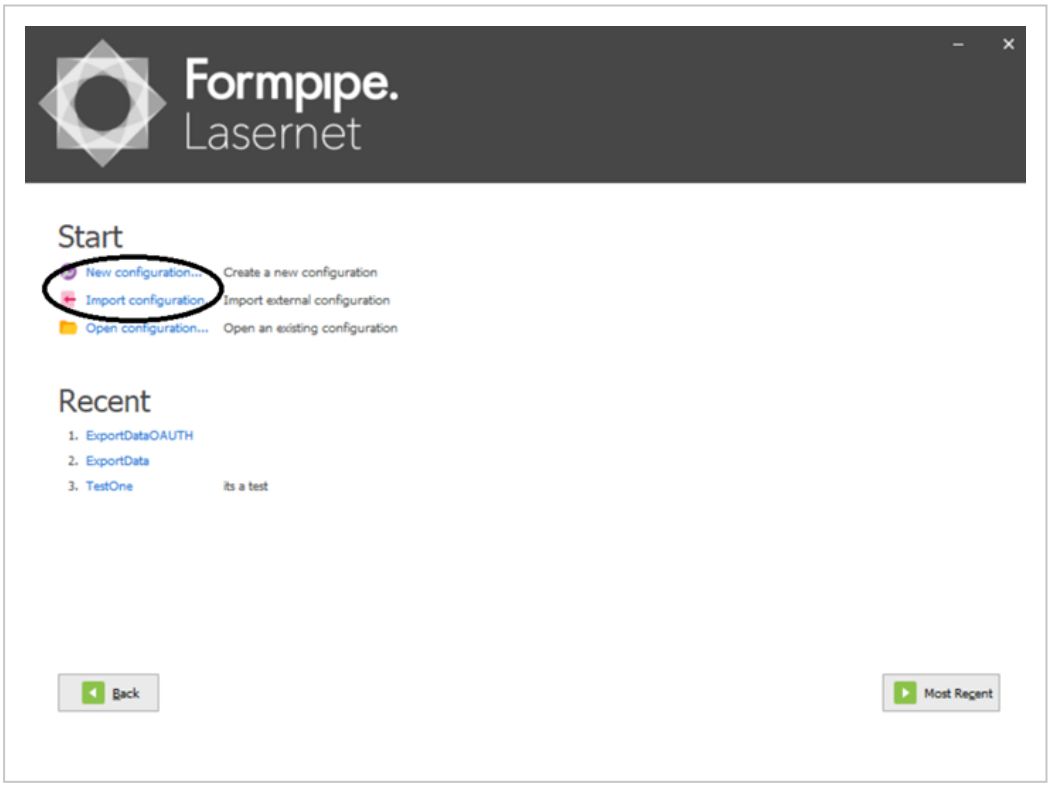
In the Developer application, you can set up your WorkZone I/O Manager processes, workflows and servers.

1. Under Lasernet general applications, select **Developer.** For the first time, you will need to log in as the default user with empty password. After that, you can change your credentials.

2. Connect to Lasernet.



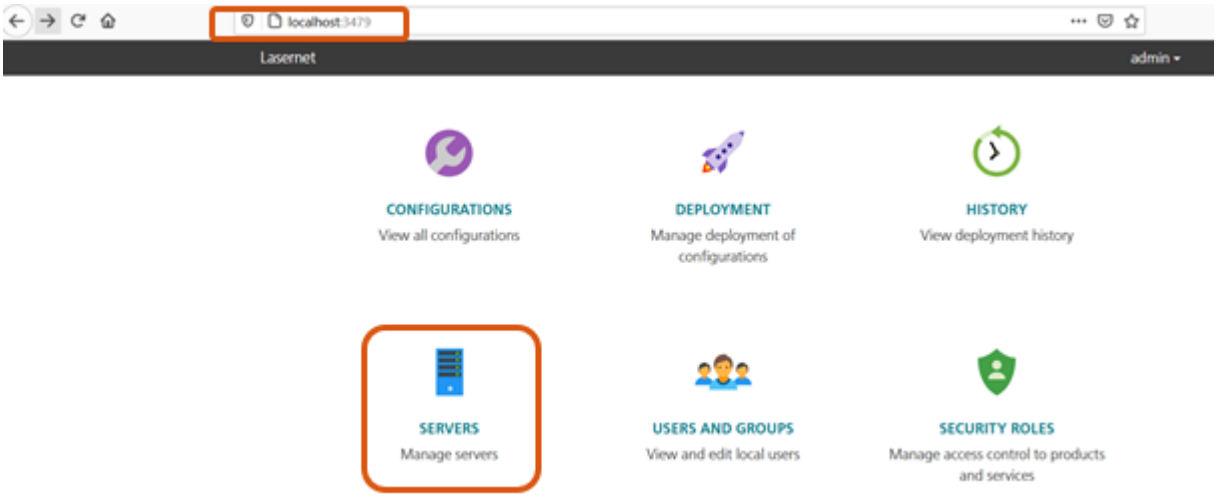
3. Create a new configuration or import an already existing one.



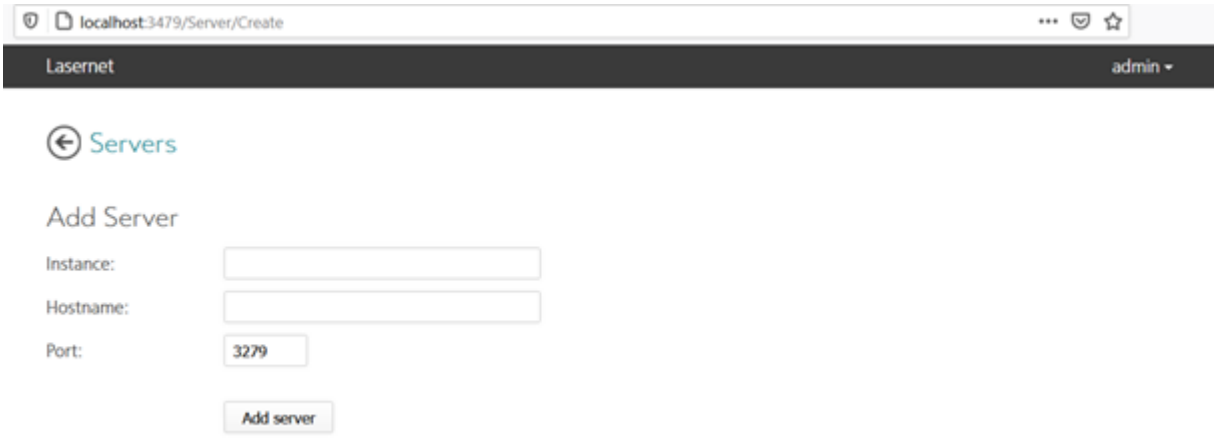
Configure web server

For a new configuration, you will need to set up web server.

1. Enter the `http://localhost:3479/` URL, where `3479` is the default port.
2. Log in, and click **SERVERS**.



3. Click **Add** to add a new server.

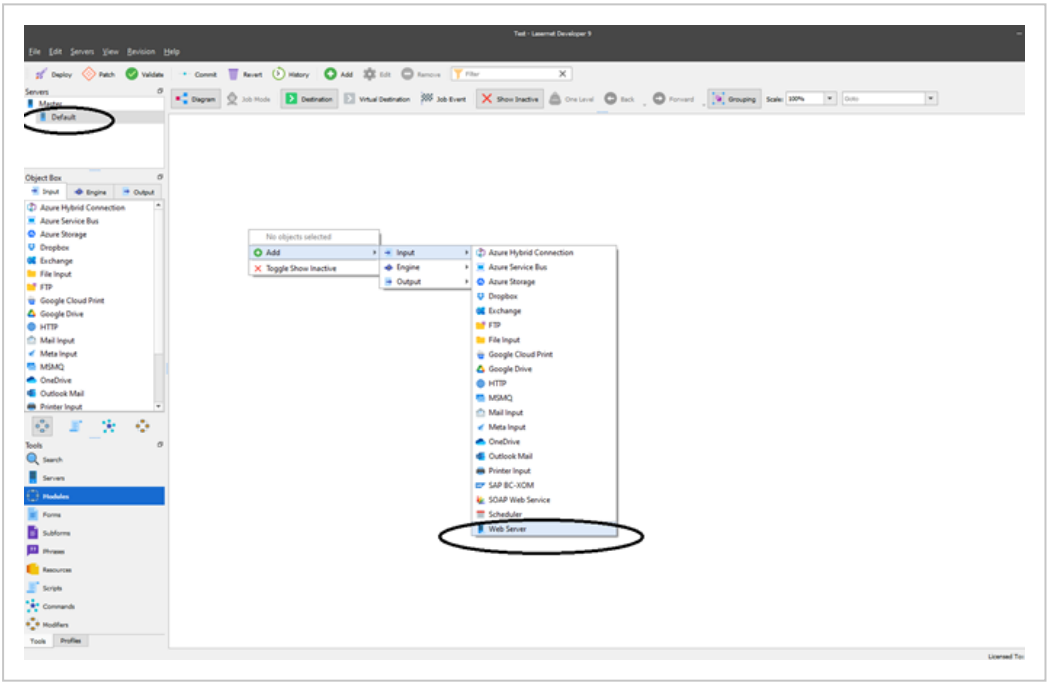


- **Instance** should be the name of your web server
- **Hostname** can be set as **localhost** in proof of concept (PoC) usage.
- **Port** is set to `3279` by default.

Set up web server (developer side)

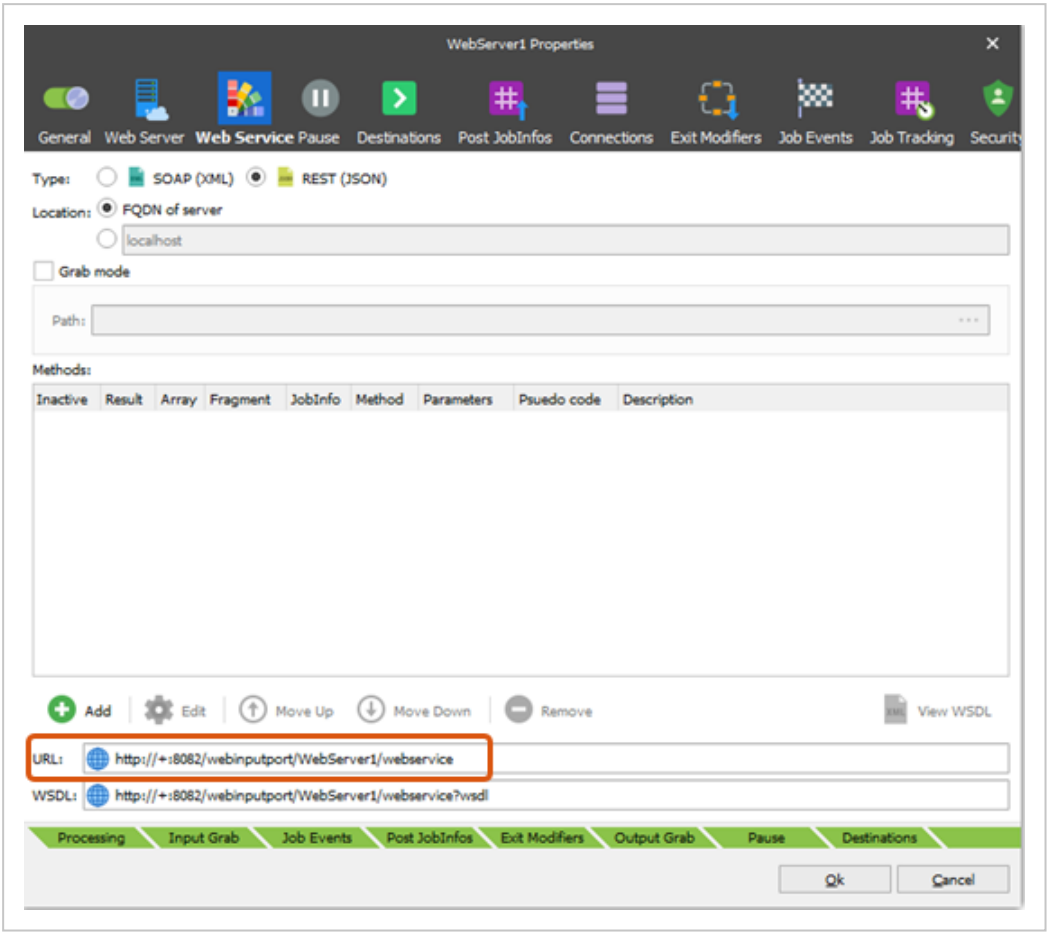
For a new configuration, you will need to set up the web server and workflows in the **Developer** app.

1. In the **Developer** app, click **New configuration**.
2. Enter **Configuration Name** and **Description**, and click **OK**.
3. On the navigation panel, under **Servers** (top left corner of the screen), click your web server name.
4. Click **Modules** on the bottom left side of the screen.
5. Right-click the blank space in the center of the screen, and select **Add** > **Input** > **Web Server**.

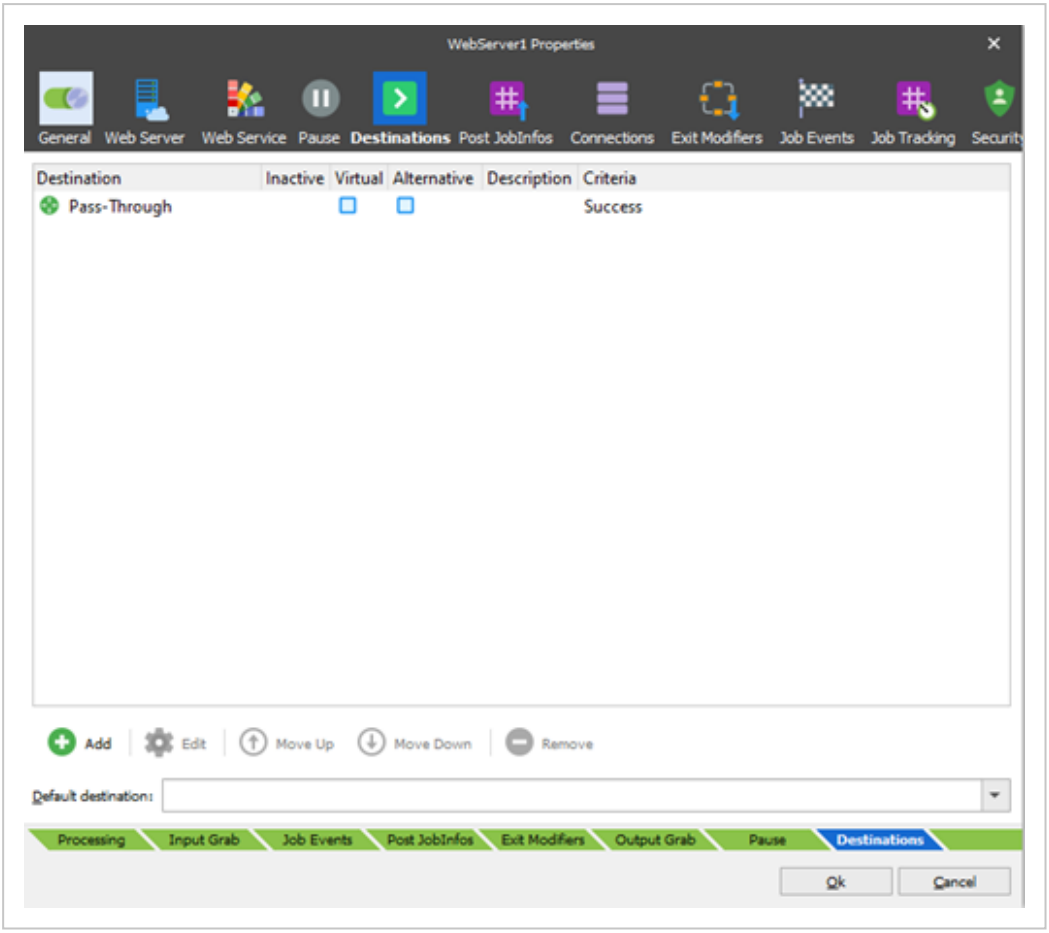


6. Configure your web server properties:
    - **General** tab: you can leave the default values
    - **Web Server** tab: specify the **Listen port**

- **Web Service** tab: specify the **URL** for service



- **Destinations** tab: add task which should be triggered upon calling the web service. In the provided example, it is `Pass-Through` task.

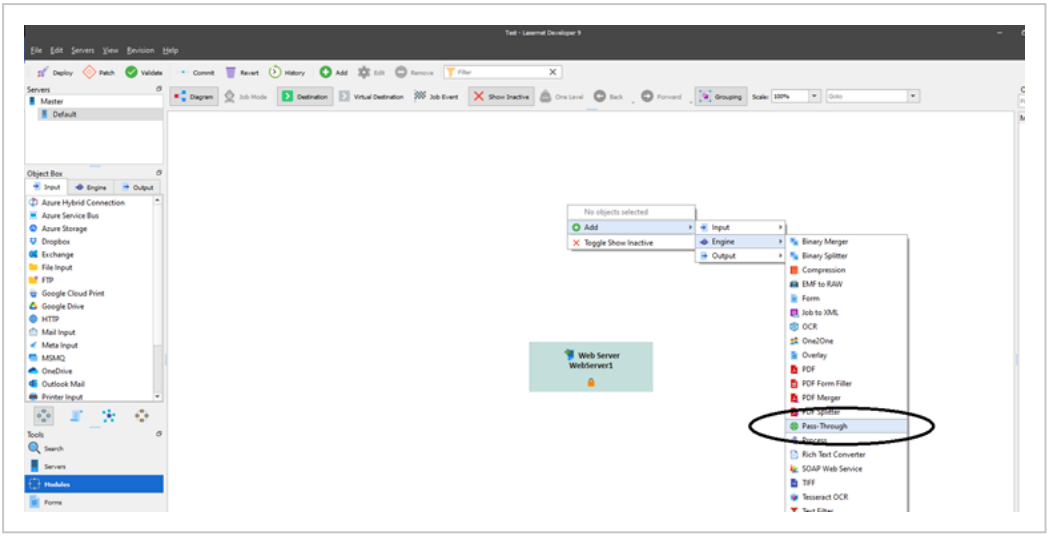


7. Click **OK** to create a new web server.

Set up web server tasks

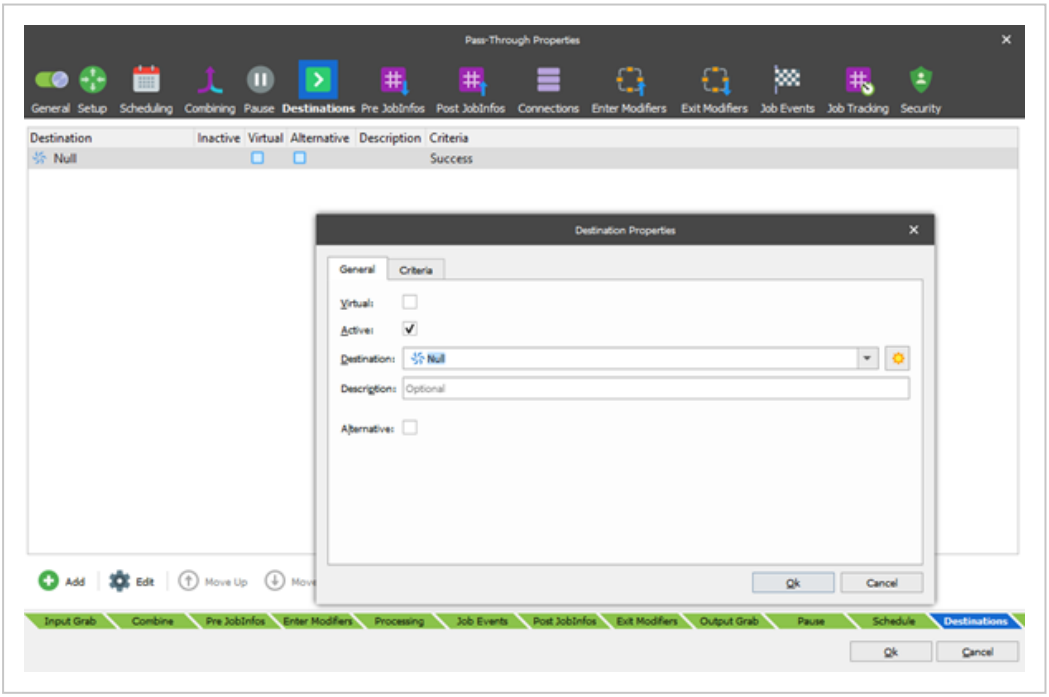
Now you need to set up tasks which can be triggered from your web server.

1. In the **Developer** app, on the navigation panel under **Servers** (top left corner of the screen), click your web server name.
2. Click **Modules** (on the bottom left side).
3. Right-click the blank space in the center of the screen, and select **Add** > **Engine** > **Pass-Through**.

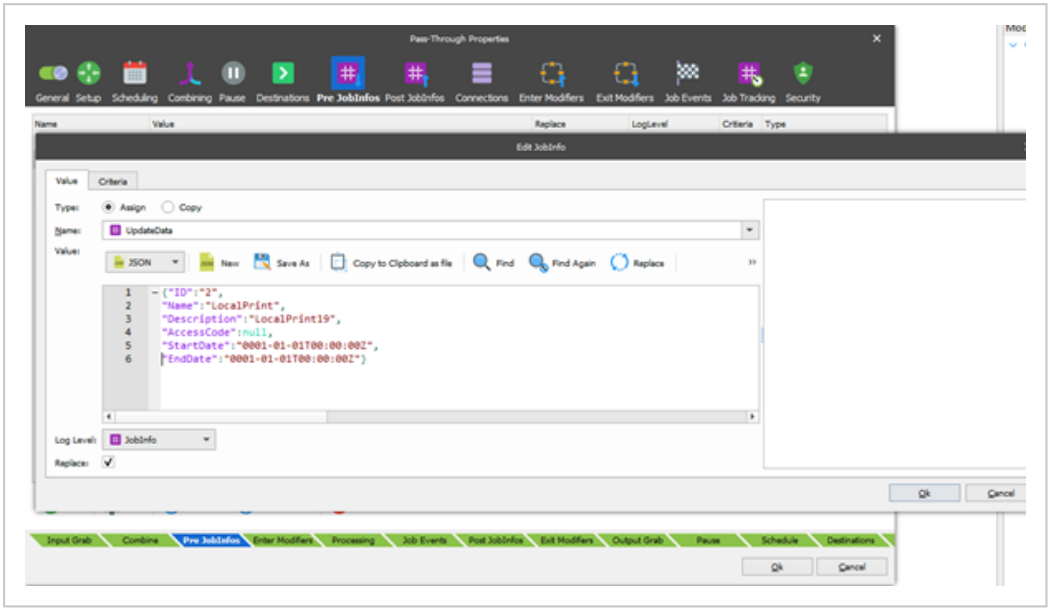


Pass-Through is the most important task, as it will manage your scripts and requests in the specified order. For example, inside the **Pass-Through** task you can define, that first you will trigger the `Get` request (to get the data from external application), and then trigger the JavaScript script which will get this data and update the body for the next step in a `Post` (update) request.

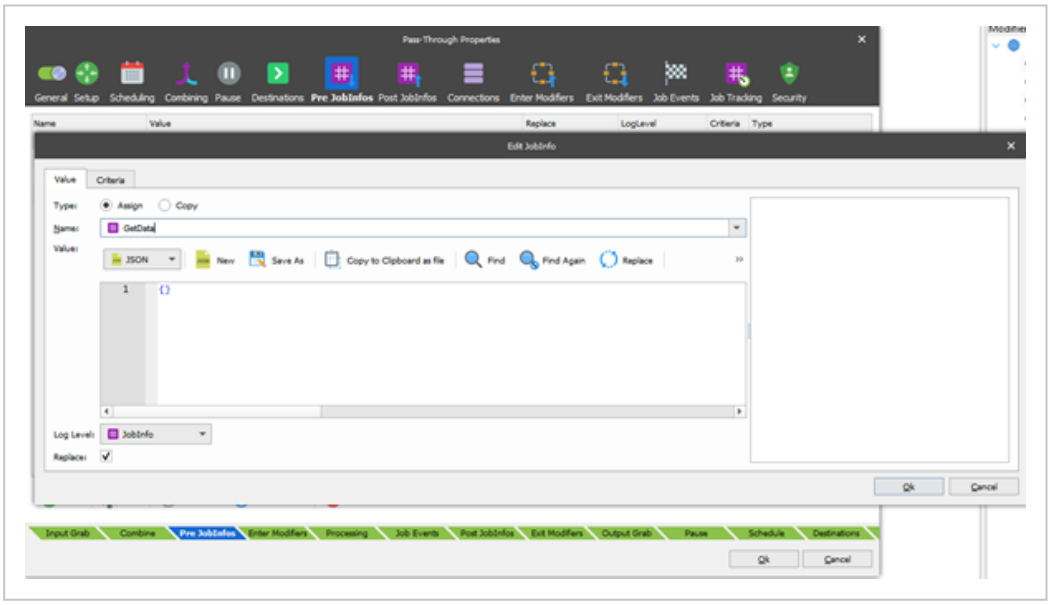
4. Specify the task name.
5. On the **Destinations** tab, select **Add**.
6. Set **Destination** as **Null**.



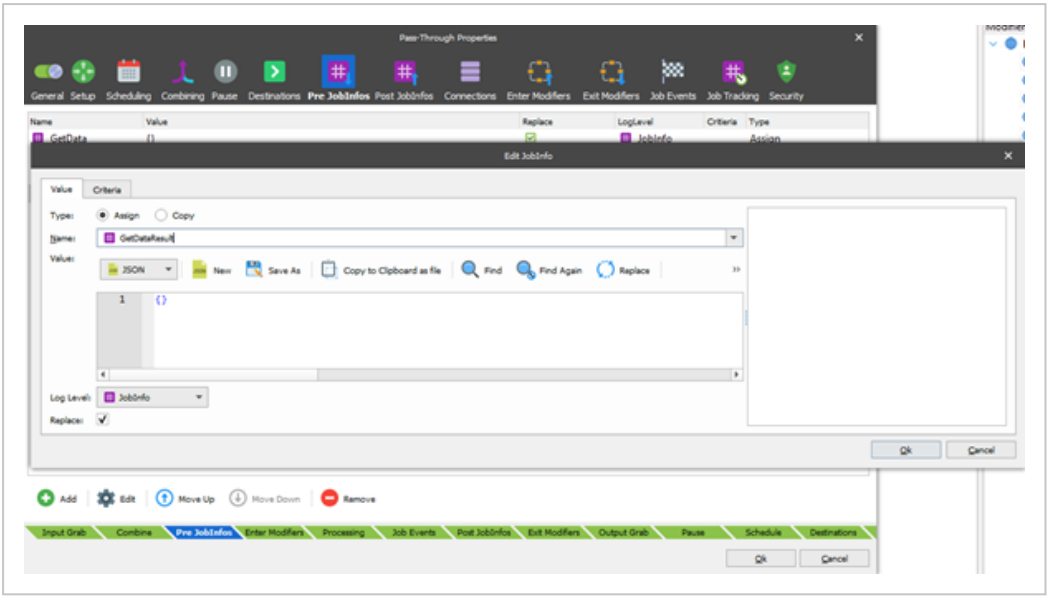
7. The **Pass-Through** task can also send requests using specific initial data placeholders called JobInfos. You can create initial one on the **Pre JobInfos** tab: click **Add**, and then provide **Name** and body example for **Value** as shown below:



- You can also add empty JobInfos for get requests which will not send any body.



8. Similar to GetData, add GetDataResult JobInfos.



You can leave the **Post JobInfos** empty for now.

See also:

Additional common tasks with WorkZone I/O Manager

Additional common tasks with WorkZone I/O Manager

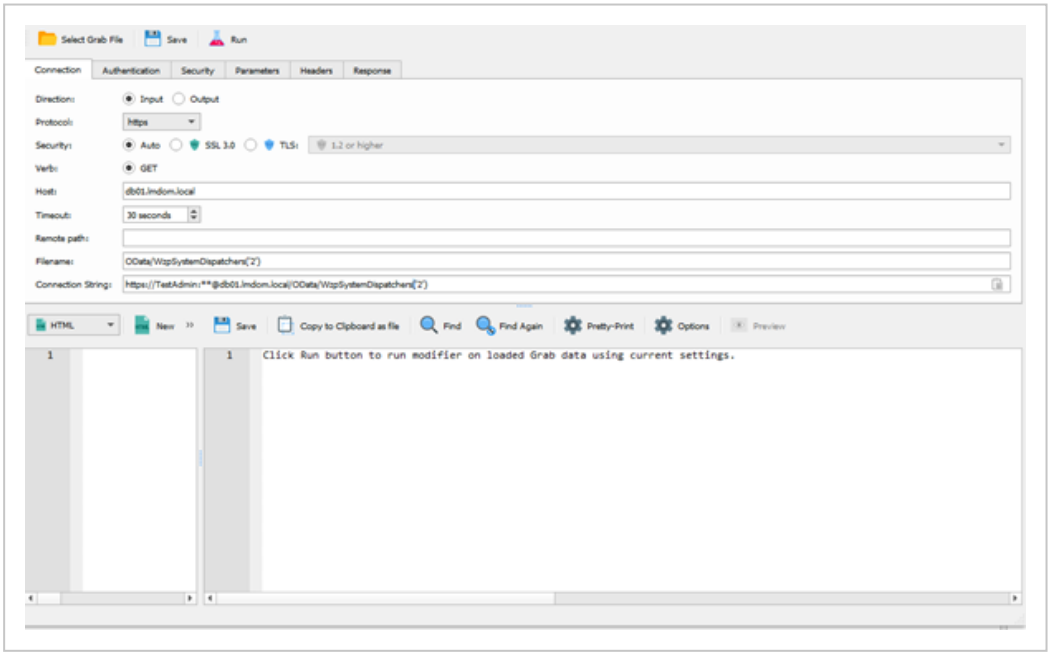
Create new modifiers (via HTTP request)

You can create request templates, using the HTTP modifier.

1. In the **Developer** app, on the navigation panel under **Servers** (top left corner of the screen), click your web server name.
2. Click **Modules** (on the bottom left side).
3. Right-click the blank space in the center of the screen, and select **Add** > **Input** > **HTTP**.

4. Configure properties of your request:

    - **General** tab: provide **Name**.
    - **Connection** tab:
        - **Protocol**: select **http**.
        - **Verb**: should be equal to the request method
        - **Host**: provide hostname (in the example below, it is `db01.lmdom.local`)
        - **Timeout**: can be set as default
        - **Remote path:** can be left blank
        - **Filename**: should be partial path combined with the hostname (in our example, it is `OData\WzpSystemDispatchers('2')`)
        - **Connection string**: provide string used for ntlm authentication (on the example below, it is `https://user-name:-pass-word@d-b01.lmdom.local/OData/WzpSystemDispatchers('2')`)

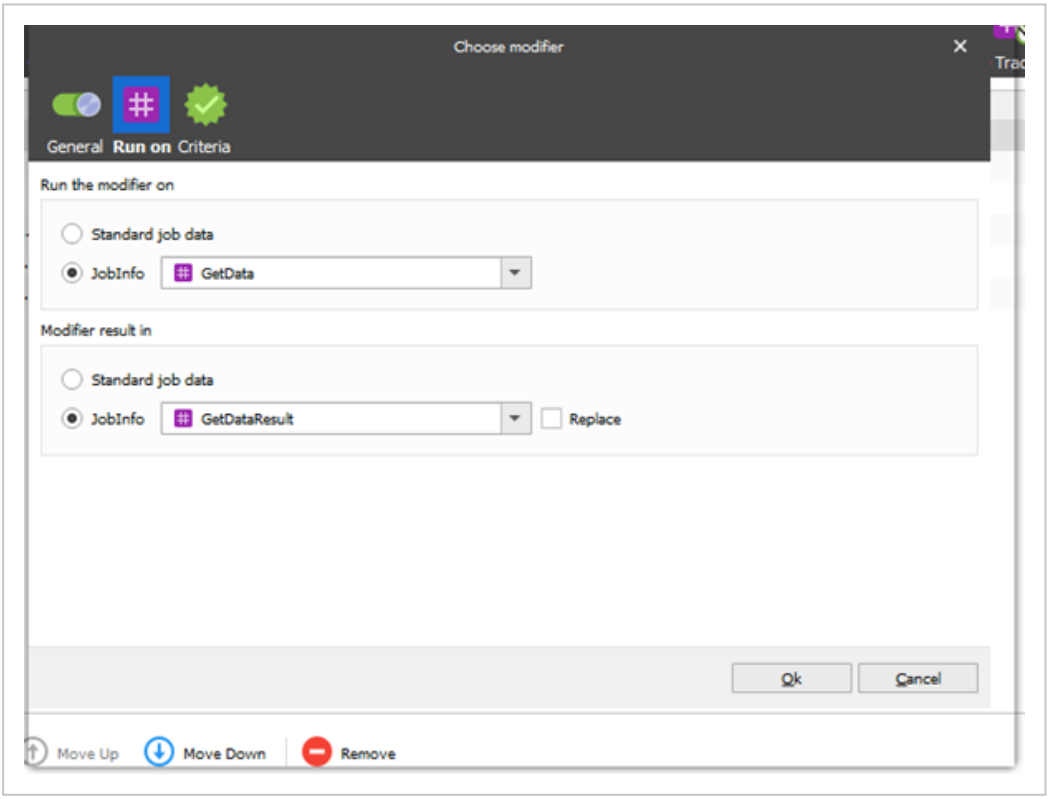


- **Authentication** tab: provide username, password and domain information.
- **Response** tab: select **JobData**.

5. Now you can add your HTTP modifier to the Pass-Through task. Double-click on the Pass-Through task, select the **Enter modifiers** tab and click **Add**. The **Choose modifier** dialog box will be displayed.
6. Specify the following details:

   - **General** tab: Select your HTTP modifier from the **Name** droplist.
   - **Run on** tab:

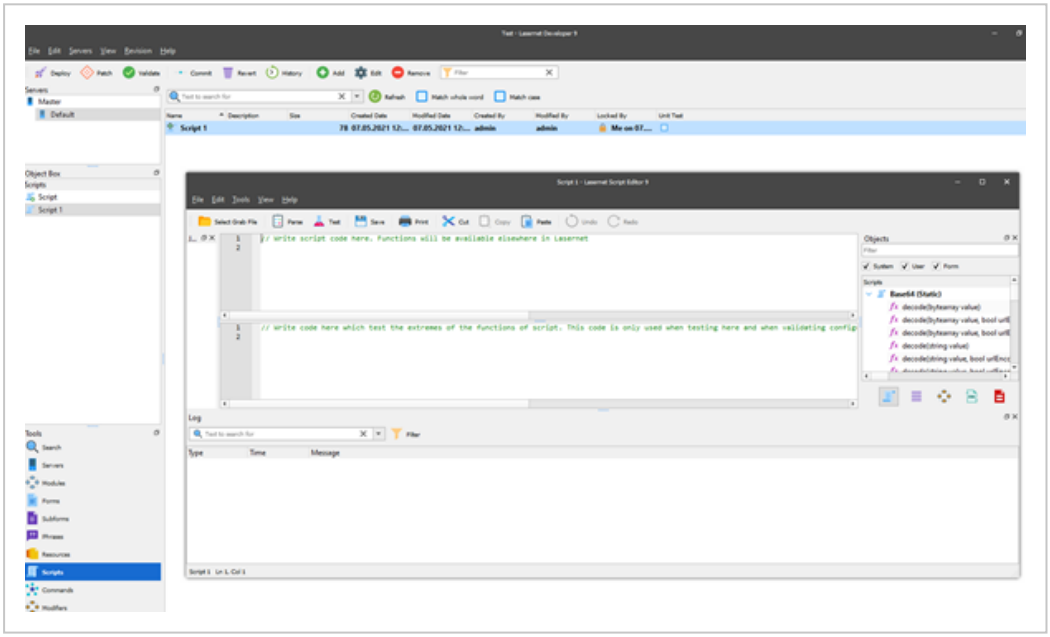
     - Under **Run the modifier on**, select **JobInfo**, and enter `GetData` as name.
     - Under **Modifier result in**, select **JobInfo** and enter `GetDataResult` as name.



Create new modifiers (via scripts)

You can also add scripts to manage your requests and responses.

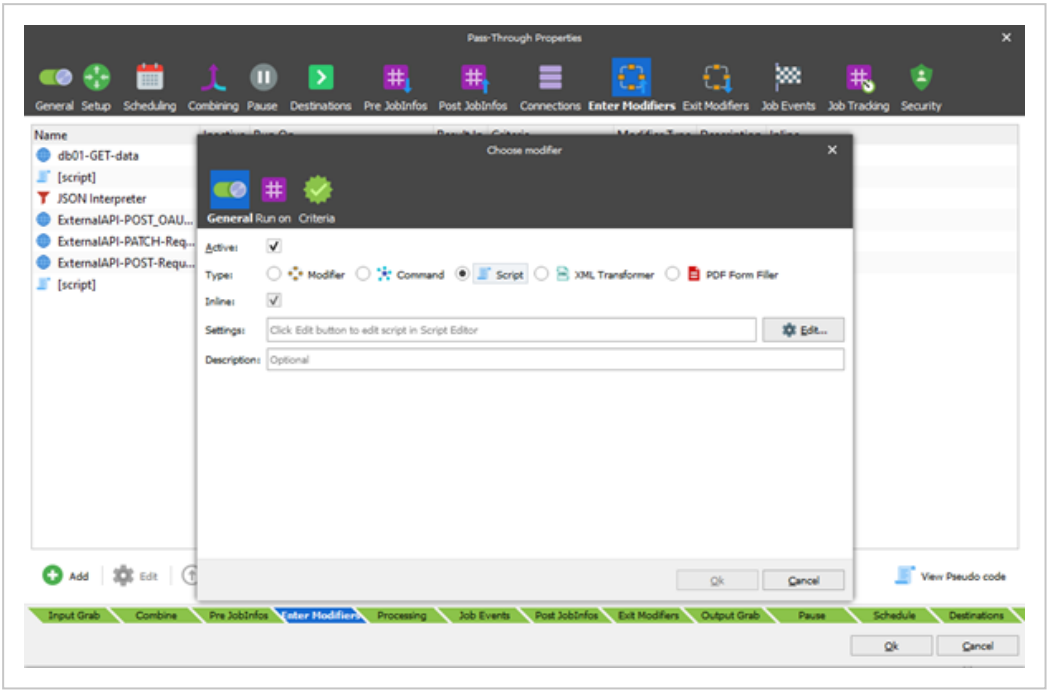
1. In the **Developer** app, on the navigation panel, select **Scripts** (bottom left corner of the screen).
2. Right-click the blank space in the center of the screen, and select **Add**.
3. Enter the name of your script, and click **OK**.
4. Select your created script (on the left pane), and click **Edit**.
5. Add the needed JavaScript code inside the script, and click **Save**.



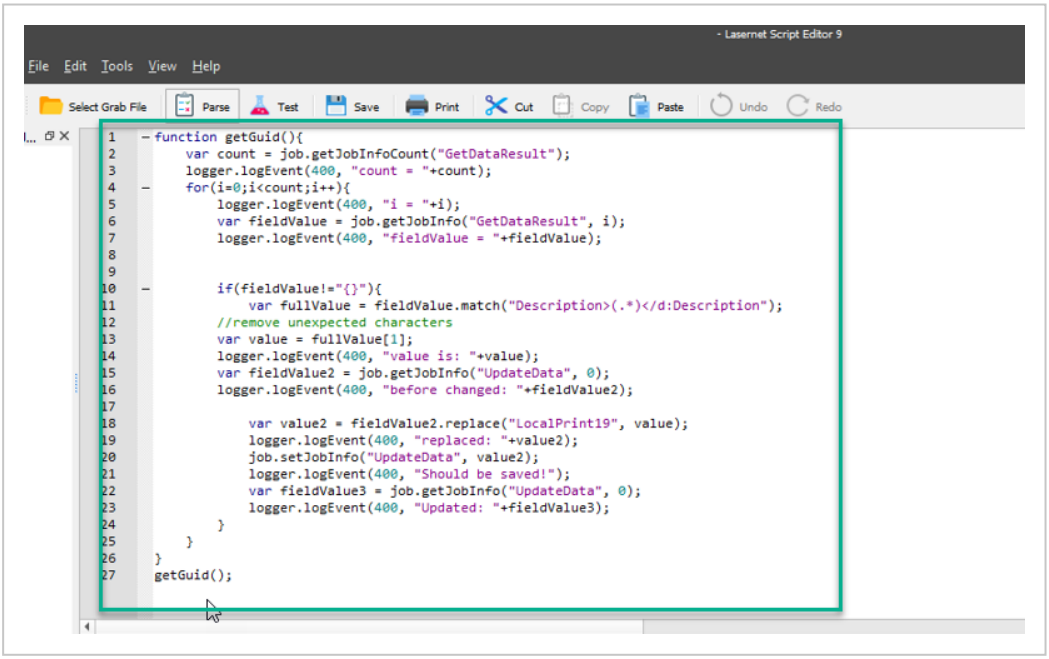
> Tip: Click **Test** to check that your code is correct and can be compiled.

6. You can also add your script to the **Pass-Through** task:
    a. In the **Developer** app, on the navigation panel under **Servers** (top left corner of the screen), click your web server name.
    b. Click **Modules** (on the bottom left side).
    c. Double-click your Pass-Through task, then select **Enter Modifiers** > **Add.**

d. Under **Type**, select **Script**, and select your script's name. Now you can open and edit your script as needed.



For HTTP modifier, which uses `GetData` and `GetDataresult` JobInfos, you can use the following script:



It will send the request with empty GetData and try to take response data from `GetDataResult`:

```
var fieldValue = job.getJobInfo("GetDataResult",
i);
```

Then it will try to find specific value from the response data:

```
var fullValue = fieldValue.match("Description>
(.*)</d:Description");
```

```
var value = fullValue[1];
```

If found, it will be send to **UpdateData** JobInfo using code:

```
var fieldValue2 = job.getJobInfo("UpdateData",
0);
```

```
var value2 = fieldValue2.replace("LocalPrint19",
value);
```

```
job.setJobInfo("UpdateData", value2);
```

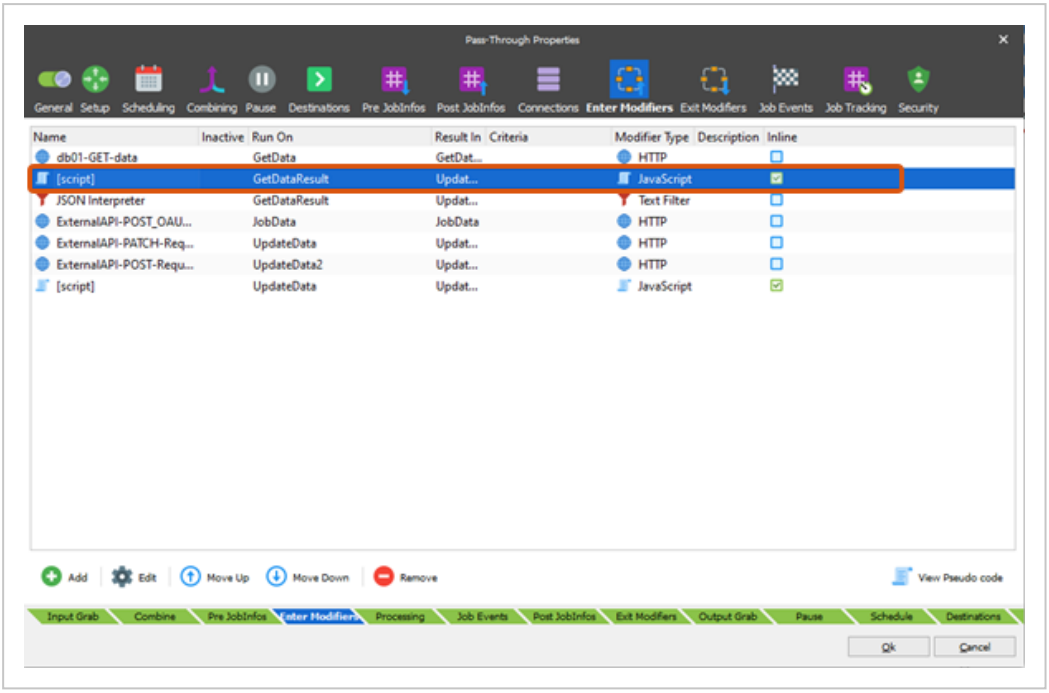
And in the end the script will also verify if the data is present:

```
var fieldValue3 = job.getJobInfo("UpdateData",
0);
```

```
logger.logEvent(400, "Updated: "+fieldValue3);
```

All infos will be saved to your logs (on the **Monitor** tab).

e. On the **Enter Modifier** tab, place your script to be triggered as a second subtask.



f. Optionally, you can add a third subtask such as HTTP modifier, which will use updated `UpdateData` JobInfo as a default body and can be used for external API.

g. Click **Ok**.

Save changes (create a commit)

1. To save your changes, click **Commit**. A new window will appear with the list of all your changes.
2. Optionally, enter the commit info message.
3. Click **OK** to save the selected changes in your setup.
4. Under `http://localhost:3479/Deployment`, click on your web server instance to see all of your changes.
5. To deploy only specific changes, click **Deploy** next to this commit (their state will

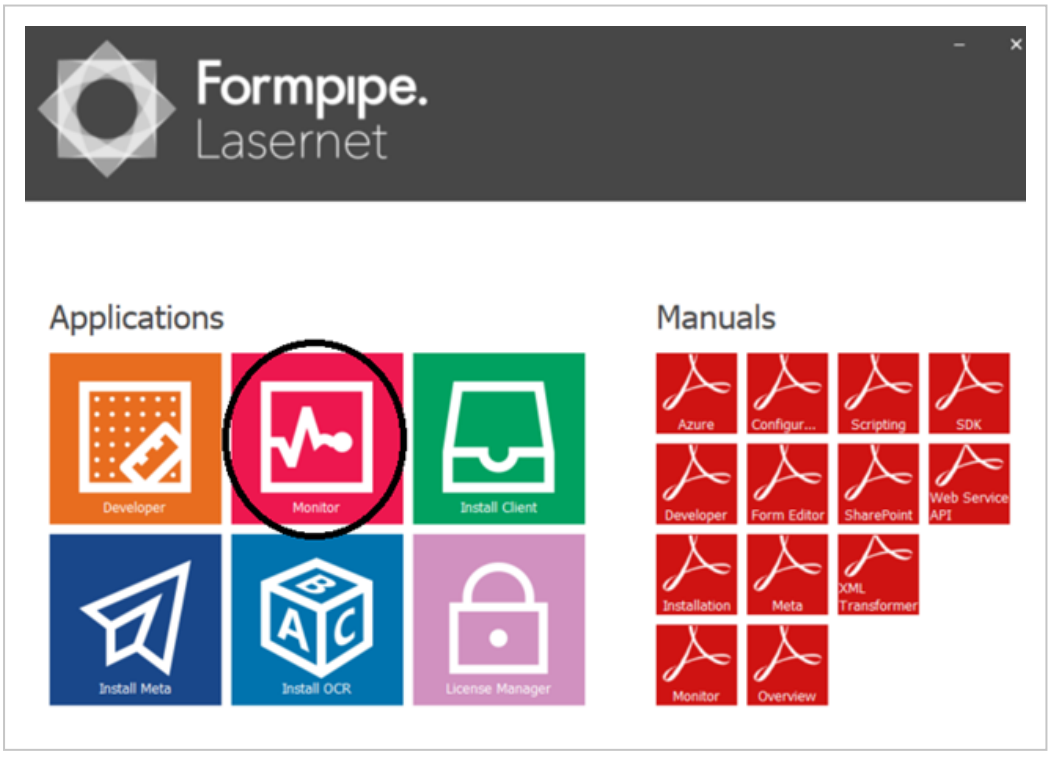
change to **Active** then).

Start a workflow

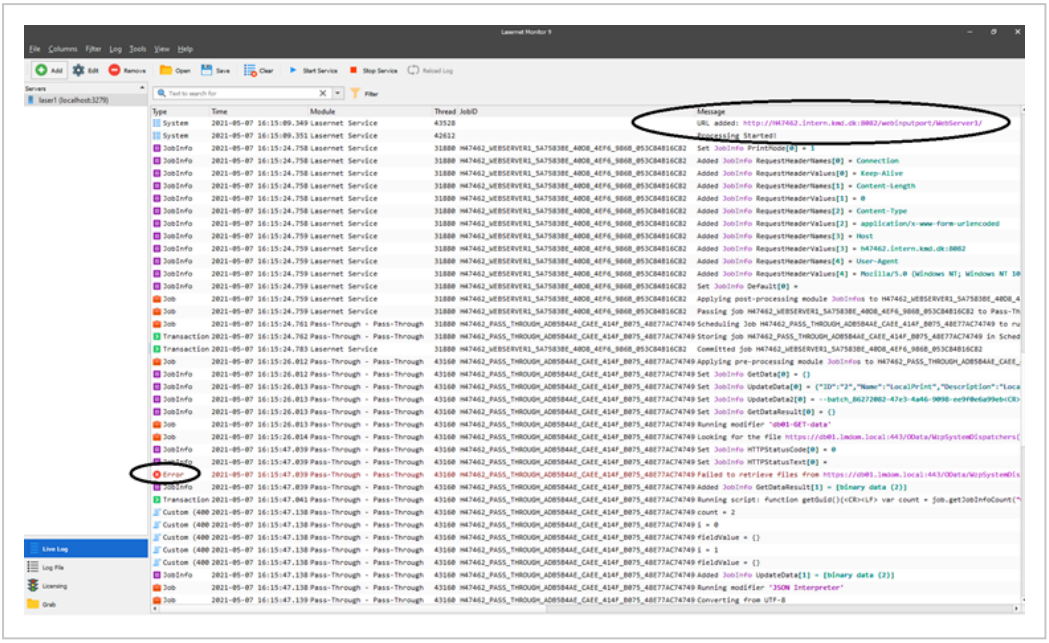
Once your changes are saved and workflow is ready, you can start web server by the request in Powershell:

```
Invoke-WebRequest -Uri http://(ifLocal-
hostPleaseUseComputerName):8082/webinputport/WebServer1/ -Method
POST
```

The web server will be started and will trigger the **Pass-Through** task. Now you can navigate to the **Monitor** application.



Here you can check if the web server is started and if there are any errors or warnings.



On the screenshot above, the **Pass-Through** gets request as one of its sub tasks, but the `https://db01.lmdom.local:443/OData/WzpSystemDispatchers/...` webpage is not responding.

You can also see here output and other information for your **Script** sub task.

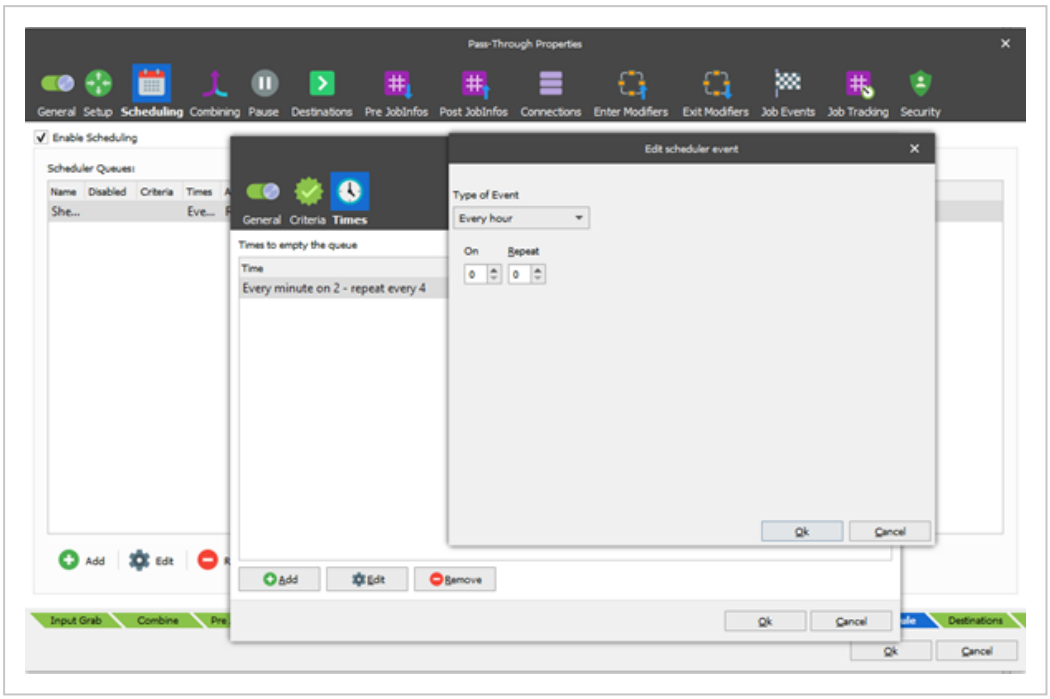
> **Important:**
>
> Your license must be valid. Otherwise you will not be able to start the web server via a Powershell request. You can check your license via **Lasernet** > **License Manager**, or **Lasernet** > **Lasernet Monitor** > **Licensing**.

Add a scheduler

If you want to repeat the Pass-Through tasks after some intervals, you can do that by configuring a scheduler.

1. Select the **Pass-Through** task > **Scheduling** > **Add** > **General**.
2. Enable the **Re-schedule** option to repeat the task all the time.
3. Select the **Times** tab, and click **Add**.

4. Specify how often to repeat the task. For example, start every hour and repeat every 10 minutes.



5. Save and commit your changes.

> **Important:** Remember to restart the service after each commit.
>
> Deploy your changes on `loc-alhost:3479/Deployment/Details/OurServerName` page and then trigger the web server as described in Start a workflow.

See also:

Set up and configure WorkZone I/O Manager

Active Directory

Set up configurations in WorkZone Configuration Management

Configuration of security codes

In WorkZone Configuration Management in the **Registry Security** module you must pre-configure the security system and assign permissions to each level of security.

The WorkZone Security System is based on 9 security codes: `1`, `2`, `3`, `4`, `5`, `6`, `7`, `8`, and `9`. For each of these security codes, you must configure a set of permissions for every register and table of the system.

The security code must reflect the permissions for a user regarding the database content.

The permissions define whether the user is allowed to search, update, insert, delete, lock, and unlock a certain type of database item, that is, a case or a relation.

The permissions of each security code can be configured to reflect the demands of specific groups of users. When a user logs on, the security code assigned to the user defines what the user is allowed to do.

Assigning security codes to users is done in **Active Directory Users and Computers** (AD). After creating a WorkZone user in Active Directory, the user must be added a distribution group, representing one of the 9 security codes.

When the users are replicated to the WorkZone Content Server database, each user is automatically allocated the correct security code and the corresponding permissions for registers and tables in the database.

Each security code can be customized to reflect the organization's specific requirements and processes, but many employ the security codes as they are defined out-of-the box.

The three most commonly used security codes are:

Security Code	Description
1	This security level contains only Read access to tables and sub-tables. Users assigned this security level may only read entries from the WorkZone database and cannot create, update or delete records. The security level can be assigned to users that only require information and not

Security Code	Description
	editing rights.
6	This security level contains some Create, Read, Update and Delete rights at a level corresponding to the expected access requirements of a user working as a typical case-worker. The security level is typically assigned to users performing normal operations in WorkZone such as case-work, document handling and contact management.
9	This security level contains Create, Read, Update and Delete rights to all tables and sub-tables in WorkZone. The security level is usually assigned to System Administrators who should be able to perform all kinds of actions on the WorkZone databases.

Configuration of contact types

In WorkZone Configuration Management in the **Basic data** > **Addressee** module, you need to pre-configure the following three mandatory contact types:

- Contact type `A`, which is used to contain the replicated Organizational units created in Active Directory.
- Contact type `M`, which is used to contain the replicated user as created in Active Directory for the purpose of a **Case Handler** register.
- Contact type `U`, which is used to contain the replicated committees as created in Active Directory.

You must create all the contact types listed above with **Auto ID** set to `N` while the maximal length of **Name Code Length** must be 30 characters.

Configuration of custom labels

In WorkZone Configuration Management in the **Basic data** > **Custom label module**, you must pre-configure a mandatory contact role for members of a committee.

- Create a contact reference named **Member** under the **NP** label type.

Later on in the process you must add this role/contact reference to committees in the Active Directory Connector.

Configuration of code visibility

In WorkZone Configuration Management in the **Operation** > **Owner** module, you can change the default configuration of access code visibility. By default, both user access codes (that is, employee user codes) and unit access codes (that is, organizational unit access codes) are visible.

To deny the use of either one, select the **Hide** check box near each type in the **Access code visibility** section.

After this, the users will be able to choose only from group access codes.

SJ Active Directory Connector

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

You can access the application from the KMD program folder. Run the `sjActiveDirectoryReplication` application as administrator.

SJ Active Directory Connector facilitates the transfer (replication) of data from Active Directory to WorkZone Content Server. 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 Content Server database.

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

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

User account permissions

User account

The name of the user account used to run the Active Directory Connector is not important, however, it is essential that the user account, including its password, is present and known to the database and 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 SJ Active Directory Connector(`sjActiveDirectoryReplication.exe`), the **ScanJour 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.

> **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 used user account has the necessary permissions to create the following objects in AD:

- Organizational unitwith 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.

These 11 groups can be created by the wizard by clicking the **Create** button in the **Active Directory Connector** wizard. See Pre-configure using 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 which has the following rights:

- **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 Windows Registry:

```
HKLM\SOFTWARE\SCANJOUR\SJAD
```

```
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application
```

Pre-configure using the wizard

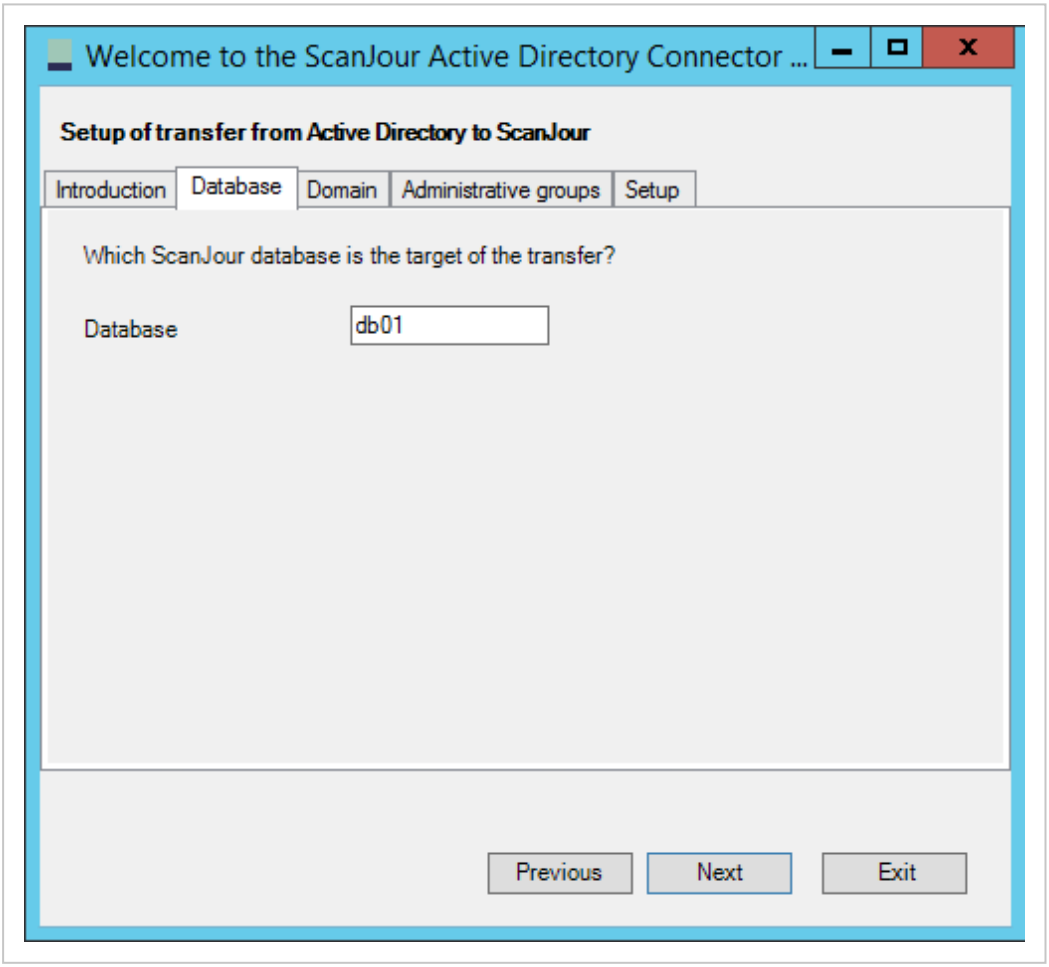
The wizard guides you through the following steps during the pre-configuration of Active Directory Connector:

- 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.

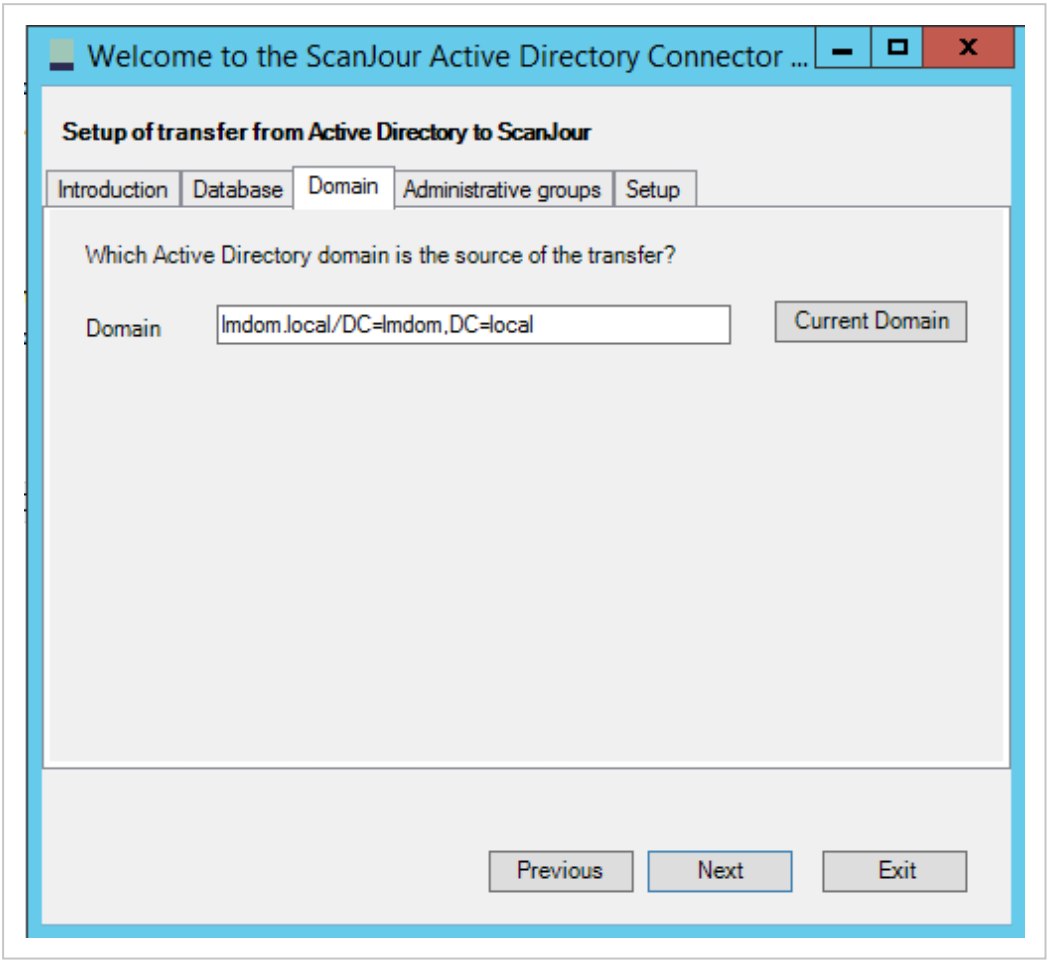
- Creation of a desktop shortcut to Active Directory Connector for easy maintenance access.
- Configuration of a scheduled task which periodically automatically secures alignment of data.

Preconfiguration wizard

1. In the WorkZone Content Server program folder `C:\ProgramFiles (x86)\KMD\WorkZone\Program`, double-click the `sjActiveDirectoryReplication.exe` file to start the Active Directory Connector Wizard.
2. Click **Next**.
3. On the **Database** tab, type the name of your database.
4. Click **Next**.

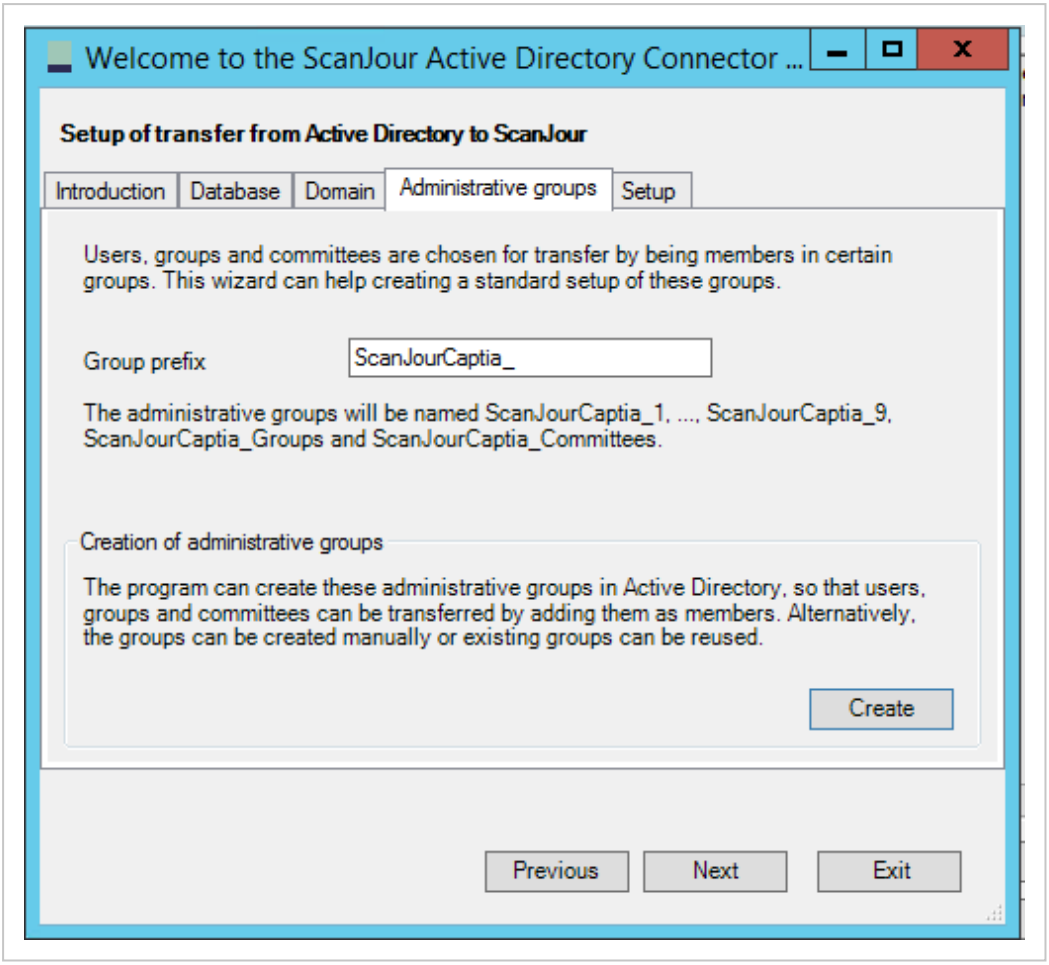


5. On the **Domain** tab, click **Current Domain** to insert the name of the current domain, or enter the name of your server domain in the **Domain** field. Click **Next**.



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 - `ScanJourCaptia<database name>`.

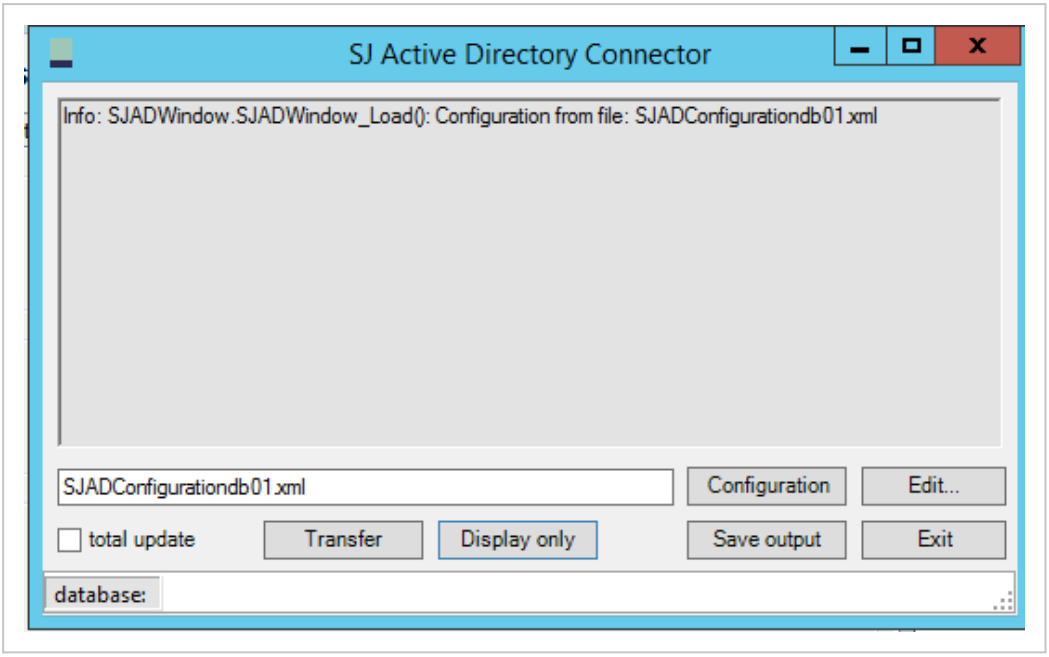
   To enhance legibility, it is recommended that you add a separating character such as a dash after the `<database name>`.



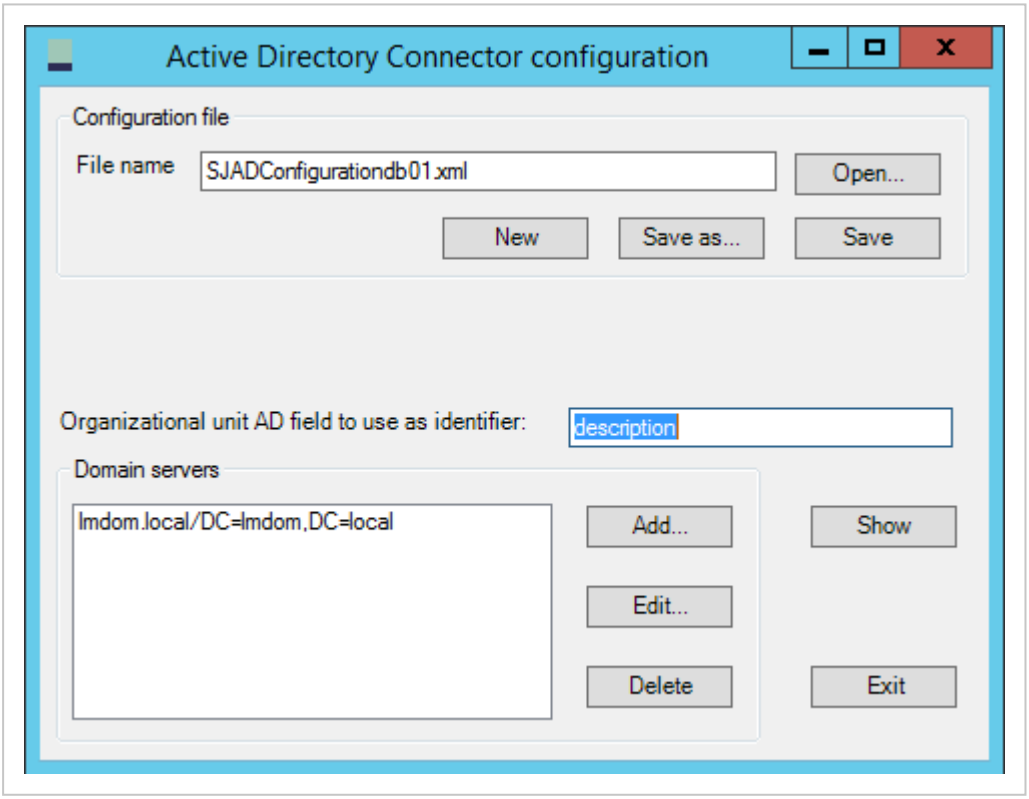
7. Click **Create**.
8. In the **Creating groups in AD** dialog box, click **OK**. The groups are created in the `ScanJourCaptiaAdministration` entry in the AD. You can rename the entry.
9. Click **Next**.
10. On the **Setup** tab, in the **Run in interactive mode** section, click **Run now** to create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

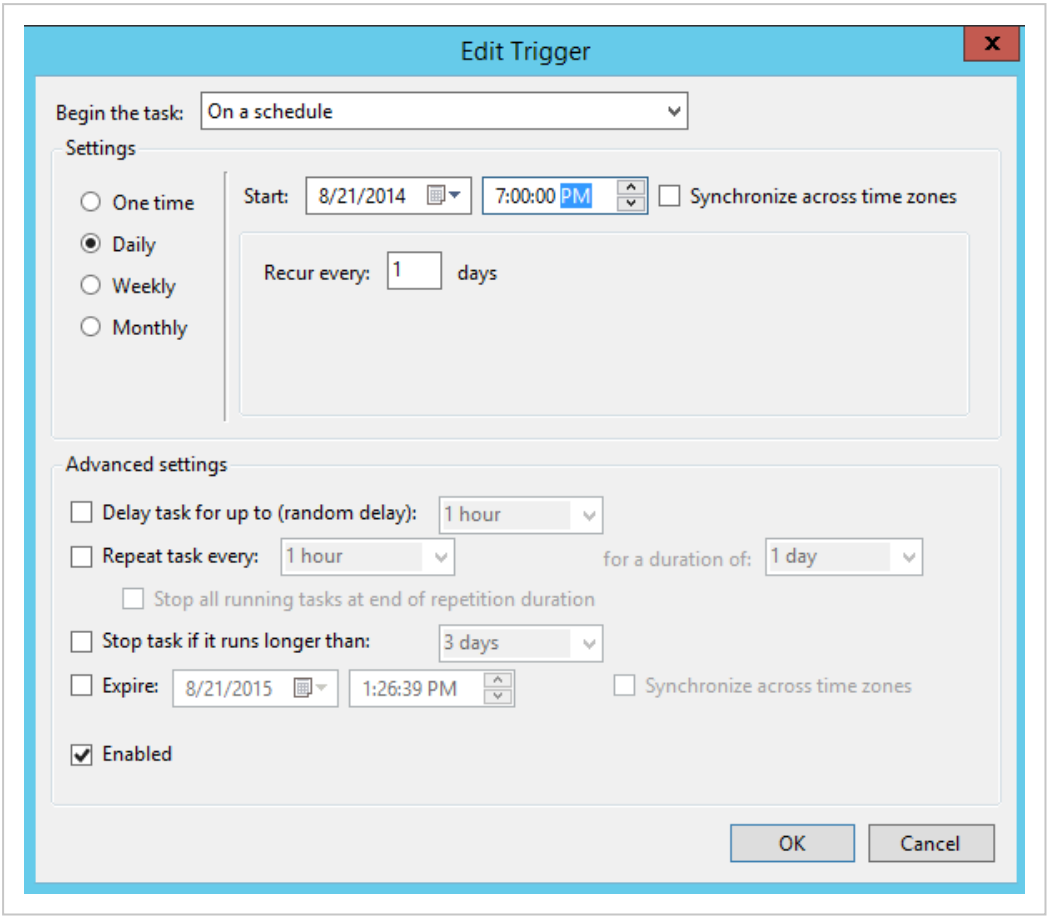
13. Click **Exit**.
14. In the **Run in interactive mode** section of the **SJ Active Directory Connector** wizard, click **Create shortcut**.

    A desktop shortcut icon linking to the Active Directory Connector for easy access is placed on your desktop with the title `sjad<database name>`, for example, `sjadtiltest`.

Create a scheduled task transfer

1. Start SJ Active Directory Connector.
2. In the **SJ Active 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 `SjADreplication<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.

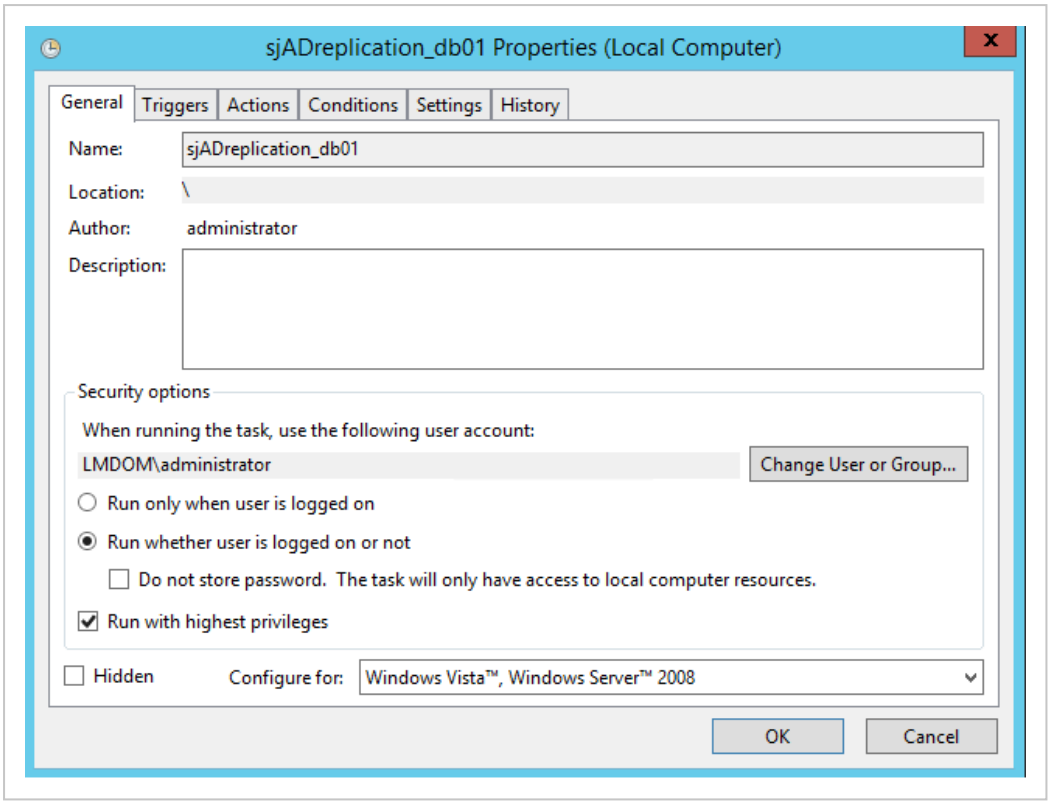


Note: It is recommended that you disable the task until you have finished your AD configuration. To do this, clear the **Enabled** check box in the **Edit Trigger** dialog box.

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.



Access Active Directory

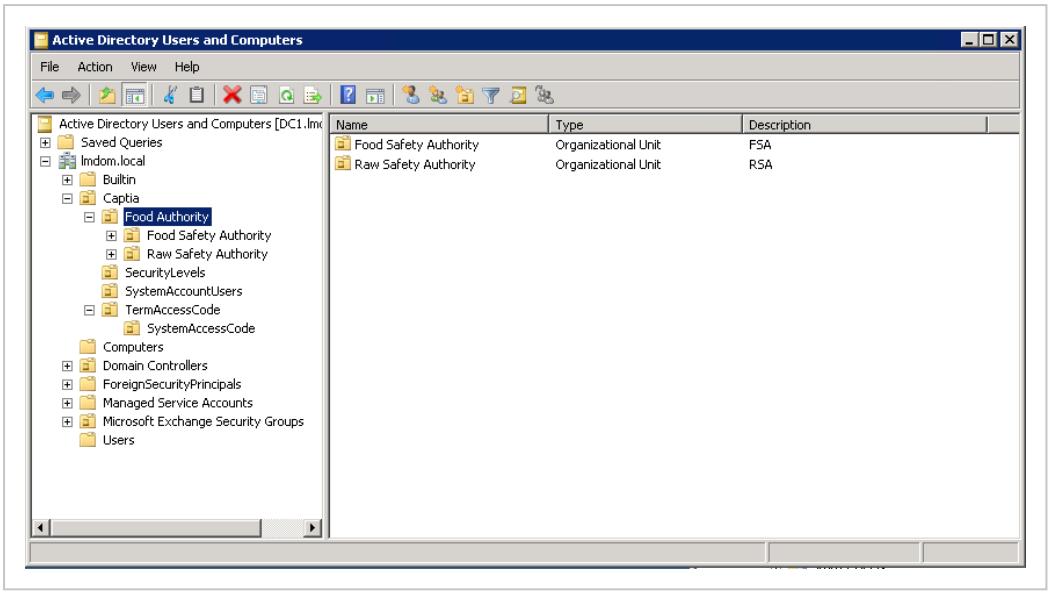
Open **Active Directory Users and Computers** to do the following:

- Create hierarchical structure of Organizational units.
- Create new users and maintain existing users.
- Maintain distribution groups and memberships.
- Create and maintain memberships of security groups.

  Group access codes and committees.

Open Active Directory

To access Active Directory, click **Start** > **Administrative tools** > **Active Directory Users And Computers** to access the Active Directory tree.



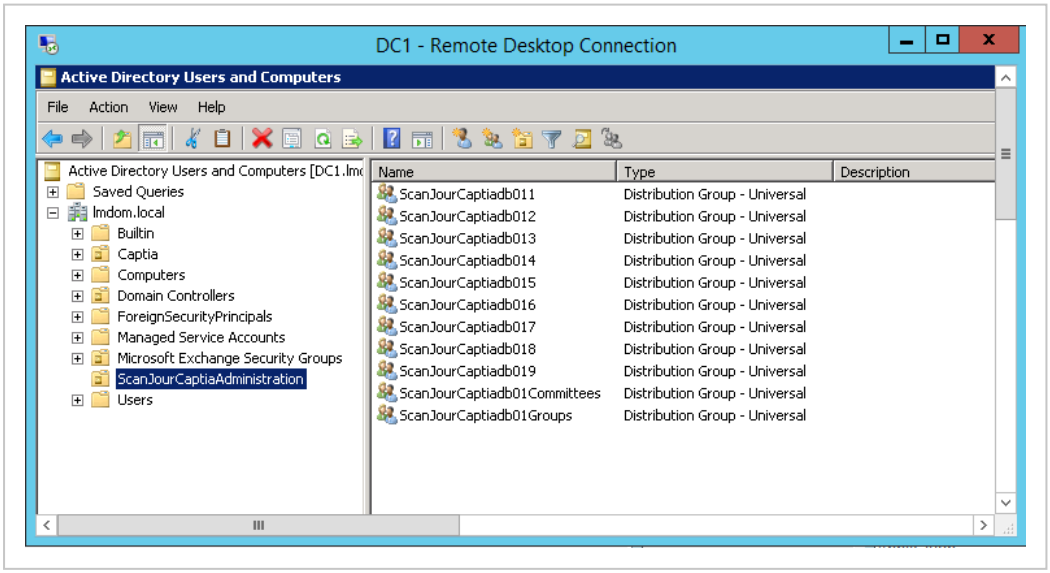
Distribution groups

The `ScanJourCaptiaAdministration` entry in the Active Directory tree contains 11 distribution groups that are pre-configured by the SJ Active Directory Connector wizard.

These distribution groups together with the configuration.xml file are the basis for alignment between Active Directory and WorkZone Content Server and the secure transfer of data.

The re-configuration of the database through WorkZone Configuration Management, that is, security groups, custom labels, and contact types, secures the receipt of transferred data.

The folder that contains the distribution groups is shown below:



> **Example**: A user who is a member of the distribution group `ScanJourCaptia_6` in Active Directory becomes a Log-on user and an employee with security level `6` in WorkZone Content Server.

The basic edit and delete permissions of the security levels are defined in WorkZone Configuration Management.

Create users in Active Directory

In an Organizational unit, you can create each user according to their administrative unit in WorkZone Content Server.

> **Note:** Even though you may already have users in your Active Directory, they must be located in the users' organizational OU and not in a separate user catalog. Move your users to the Organizational unit where they belong to comply with WorkZone Content Server default configuration.

1. Open **Active directory Users and computers**. In the Active Directory tree, right-click the Organizational unit you want to add a user to. From the menu, select **New > User**.
2. The **New Object - User** dialog box is displayed.

   Specify the following required values:

   - **First name**
   - **Last name**
   - **User logon name**

   The following values are filled in automatically:

   - **Full name**
   - **User logon name (pre-Windows 2000)**

> **Note:** Some restrictions regarding characters and length apply, as well as **User logon name (pre-Windows 2000)** restrictions. See User name restrictions.

3. Click **Next**.
4. Specify the following values:
    - **Password**
    - **Confirm password**
5. Click **Next**, then click **Finish** to create the user.
6. Right-click the user you have just created and select **Properties**.
7. In the **<user name> Properties** dialog box on the **General** tab, the following fields can be filled in or edited in a default configuration. (✓) indicates that the text box is already filled in, but may be edited:
    - First name (✓)
    - Last name (✓)
    - Description
    - Telephone number
    - E-mail

    Click the **Address** tab.
8. On the **Address** tab the following text boxes can be filled in or edited in a default configuration. (✓) indicates the text box is already filled in but may be edited:
    - Street
    - Zip/postal code
    - Country/region
9. Add the user to a distribution group. For more information, see Apply security groups to users

Apply security groups to users

Distribute user security code membership

If you transfer data from Active Directory to WorkZone Content Server as defined in previous sections, only the registered Organizational units would be transferred.

To transfer the users and user details, you must include them in one of nine distribution groups, which secure the alignment of a corresponding security level.

```
ScanJourCaptia<database name>-<security code>
```

Note: The distribution groups can be found in the AD tree under the `ScanJourCaptiaAdministration` entry.

See Access Active Directory for more details.

1. In the AD tree with a list of users that you have created, right-click the user and select **Properties**.
2. In the **<user name> Properties** dialog box, click the **Member of** tab.
3. Click **Add**. The **Select groups** dialog box appears.
4. In the **Enter the object names to select** field, start typing the name of the distribution group into which you want to include the user and click **Check Names**. The **Multiple Names Found** dialog box is displayed.
5. Select the distribution group.
6. Click **OK**.
7. Click **OK** in the following dialog boxes to verify the membership of the user.

Log-on users and employees in WorkZone Content Server

When data is transferred from AD to WorkZone Content Server, each user becomes:

- A log-on user in the WorkZone Content Server **User** register. In a default configuration, user log-on name is transferred to user name in WorkZone Content Server

and is equal to the user ID.

- An employee in the WorkZone Content Server **Employee** register. It can be used in the user interface list such as the **Case handler** list.

Create or copy users

Another way to create a user is to copy a user who already has the memberships you want the new user to have, for example, security code `6` and required access codes. You can change the default settings of the new user as needed.

Discontinue users

Before discontinuing a user in Active Directory, it is essential to investigate whether the user has used user access codes.

If the user has applied user access codes to cases, documents, or contacts, you can use the **Lost and Found** functionality to uncover cases, documents or contacts that normally do not appear in searches because they are owned by the discontinued user.

When the user has been deactivated in AD and a transfer has taken place (either manually or as a scheduled task), you should be aware of the following:

- Discontinued users remain in the WorkZone Content Server **User** register but they do not have any permissions. The security code of the user is `0` now, which means that the user has no access to the database.
- Discontinued users continue to be employees in **Employee** register and are therefore still owners of terminated cases or archived documents.
- The user access codes of the deactivated users have been terminated.

Change the Organizational unit for the user

When a user is moved from one Organizational unitto another in the Active Directory tree, this only affects the unit access codes of the moved user. However, you should be aware of the following:

- A changed Organizational unit will affect all cases, documents, and addressees where the user has applied unit access codes. These can no longer be viewed by the

case handler, only by members of the former case handler's responsible unit.

- The items will not appear in **Lost and Found** for the reason that the rest of the members of the unit in question can still view it.
- All the items of the moved user will need to have the **Responsible Unit** field updated: either manually per item or multi-edited by a user with the system access code `MULTIEDIT`.

Distribution groups: Groups and committees

The purpose of groups and committees is to enable you to unite users across the organization regarding:

- Shared **group access codes** regardless of Organizational unit.

  An Active Directory group (global security group) which is a member of the distribution group `ScanJourCaptia<database name>Groups`.

- Shared **Committees**.

  An Active Directory group (global security group) which is a member of the distribution group `ScanJourCaptia<database name>Committees`.

Organization

An Active Directory group can be a member of both distribution groups.

> **Example**: A committee called *Agenda* may be a group access code to protect the work of the committee Agenda.

However, when you organize your Active Directory tree, it is recommended that you consider creating two individual Organizational units under the domain that the WorkZone Active Directory groups are part of, to separate them from other Active Directory groups in your general Active Directory tree:

1. One that contains group access codes, for example, *SJ access codes.*
2. And one that contains committees, for example, *SJ Committees.*

System access codes

Some Active Directory groups are mandatory, such as the system access codes that are automatically generated by a script when WorkZone Content Server is initialized.

Corporate access codes

If you selected the installation with corporate access code, see Corporate access code for details.

Group access codes

> **Prerequisite:** The above mentioned organization of your WorkZone Content Server Active Directory tree should be implemented.

If you still need to create your WorkZone Content Server access code Organizational unit, see Create an organizational unit, steps 1 and 2 for more details.

Create a group access code

1. Open **Active directory Users and computers**.
2. In the AD tree, right-click the Organizational unit in which you want to organize your group access codes, (for example, *SJ access codes* in the AD tree) and select **New** > **Group**. The **New Object – Group** dialog box is displayed.
3. In the **Group name** text box, enter the name of the group, for example, *CONFIDE1*. The **pre-Windows 2000** field is automatically filled in.

   Your entry is not case-sensitive but must be within the length specified in WorkZone Configuration Management – max 30 characters. Other important restrictions regarding characters apply as well. For more information, see Group name restrictions.
4. Leave **Group scope** and **Group type** as they are. Click **OK**.

5. Right-click the group you have just created, for example, *CONFIDE1* and select **Properties**.
6. On the **General** tab in the **<group name> Properties** dialog box, click **Add**.
7. Leave the **Description** field empty.
8. On the **Members** tab, click **Add**. You can add both individual users and groups (of users), that is, group access codes as members, see Add a Group access code as a member of a group access code below.
9. In the **Select Users, Contacts or Computers** dialog box, start typing the name of the user or users you wish to make members. Click **Check Names**:

    - If there is only one match, the name appears directly in the **Enter the object names to select** text box area;
    - If there are multiple matches, the **Multiple Names** dialog box is shown. In the **Multiple Names** dialog box you can:

        - Select the name you are looking for;
        - Select more than one name - press the **Ctrl** key while selecting.

    Click **OK**.

    If you know from the start you are looking for several users you can separate entries with semicolon - `hen;pel;elp`.

10. After the name (or all the names you have selected) in step 8 appear in the **Select Users, Contacts or Computers** dialog box in the **Enter the object names to select** field, click **OK**.
11. In the **<group name> Properties** dialog box, the added members are listed. Click **OK**.

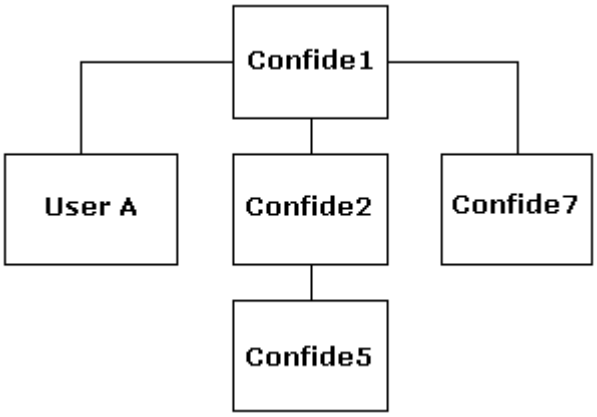
Add a Group access code as a member of a group access code

You can add groups of users, that is, group access codes as members of group access codes. In this way, you can make a whole batch of users into members of a group access code at the same time.

Example

You have a group access code, for instance, *Confide1*. Now you want to populate it. First you add an individual user – *User A*. Then you want to add groups of users. To do this, you can add the group access codes *Confide2* and *Confide7*. In this way you add all the members of *Confide2* and *Confide7* at the same time. Group access code *Confide5* is already a member of *Confide2*. Therefore, the members of *Confide5* are also members of *Confide1*.

See the diagram below.



Prepare the group access code for transfer

If you transferred data from Active Directory to WorkZone Content Server at this point, your group access code `CONFIDE1` would not be transferred. It will be another global security group in your general Active Directory tree.

> **Prerequisite:** To complete creating the group access code, it is important that you make it a member of the distribution group: `ScanJourCaptia<database name>-<Groups>`. This is the tag that makes it recognizable to the configuration file.

1. Access **Active directory Users and computers**. The Active Directory tree is displayed.
2. Click the `ScanJourCaptiaAdministration` Organizational unit to open it.
3. Right-click the `ScanJourCaptia<database name>-<Groups>` distribution group and select **Properties**.
4. In the **<database name>-<Groups>** dialog box, click the **Members** tab and then click **Add**.

5. Enter the group access code name or part of it. For example, *CONFIDE1*.
6. Click **Check Names**.
7. Select group.
8. Click **OK**.
9. Click **OK** in the following dialog boxes to verify the membership.

After SJ Active Directory Connector transfer

When the next transfer has been performed (either manually or as a scheduled task), the group access code, for example, *CONFIDE1,* has been added to the profiles of its members in WorkZone Content Server.

The added group access code now allows its members to:

- Apply this access code to items.
- Access items protected by this access code.

Create a committee

> **Prerequisite:** The organization of your WorkZone Content Server Active Directory tree must has be implemented before you create a committee.
>
> If you still need to create your WorkZone Content Server committee Organizational unit, see Create an organizational unit.

1. Access **Active directory Users and computers**. The Active Directory tree is displayed.
2. Right-click the Organizational unit in which you want to organize your group access codes used as committees. For example, *SJ Committee*.
3. From the menu select **New** > **Group**. The **New Object – Group** dialog box is displayed.
4. In the **Group name** field, enter the name of the group. For example, *AGENDA*. Your entry is not case-sensitive, but must be within the length specified in WorkZone Configuration Management – maximum of 30 characters. Other

important restrictions regarding characters apply, see Committee name restrictions.
The **pre-Windows 2000** field is automatically filled in.

5. Leave **Group scope** and **Group type** as they are and click **OK**.
6. Right-click the group you just created, for example, *AGENDA* and select **Properties**.
7. In the **<group name> Properties** dialog box on the **General** tab, click **Add**
8. Leave the **Description** field blank.
9. Click the **Members** tab.
10. Click **Add**.
11. In the **Select Users, Contacts or Computers** dialog box, enter part of the name of the user or users, whom you want to make members.
    If you know from the start you are looking for several users you can separate entries with semicolon - `hen;pel;elp`.
12. Click **Check Names**:

    - If there is only one match, the name appears directly in the **Enter the object names to select** field.
    - If there are multiple matches, the **Multiple Names** dialog box is displayed.

    In the **Multiple Names** dialog box you can:

    - Select the name you are looking for.
    - Select more than one name by holding the **Ctrl** key while selecting.

    Click **OK**.

13. After the name (or all the names you have selected in step 10) appears in the **Select Users, Contacts or Computers** dialog box in the **Enter the object names to select:** field, click **OK**. The **<group name> Properties** dialog box with the added members is displayed.
14. Click **OK** to verify.

Prepare the committee for transfer

To complete creating the group access code for the committee, it must become a member of the distribution group `ScanJourCaptia<database name>-<Committees>`. This is the tag that makes it recognizable to the configuration file.

1. With the **Active Directory Users and computers** accessed and the AD tree displayed, click the `ScanJourCaptiaAdministration` Organizational unit to open it in the right pane.
2. Right-click the distribution group: `ScanJourCaptia<database name>-<Committees>`.
3. Select **Properties**.
4. In the **<database name>-<Committees>** dialog box, click the **Members** tab, and then click **Add**.
5. Enter the committee name, for example, *AGENDA*, and click **Check Names**.
6. Click **OK**.
7. Click **OK** in the following dialog boxes to verify the membership.

After SJ Active Directory Connector transfer

When the next transfer has taken place (either manually or as a scheduled task):

- The committee, for example, *AGENDA*, has been created in WorkZone **Addressee** register under the contact type `U` and the addressee code, for example, *AGENDA*.
- Members of the committee, for example, *AGENDA*, have been added as contact references to a contact group named *AGENDA* in WorkZone Content Server.

Transfer data

When you have configured your WorkZone Active Directory system according to the steps of this guide, you must start a trial transfer.

In the **SJ Active Directory Connector** window, click **Display Only** to log errors in the setup in Active Directory, see Monitor the transfer .

Initialize transfer of data

When you have corrected the errors that occurred in the trial, you are ready to start the actual transfer.

When you click the **Transfer** button in SJ Active Directory Connector data is transferred from Active Directory to the WorkZone Content Server database according to the alignment described in the configuration file.

Re-enable the scheduled transfer task

After the transfer has been completed successfully, you must re-enable the scheduled transfer task.

This task will now handle the alignment of data changes and new creations between Active Directory and WorkZone Content Server.

See also:

Create a scheduled task transfer

Creating organizational units in Active Directory

Organizational Unit Organizational unit structure

Organizational units are essential to the WorkZone Active Directory structure. The hierarchical structure of your organization must be mapped to your Organizational units in the Active Directory tree.

In a standard WorkZone Content Server installation, all units and unit dependencies are maintained in Active Directory.

However, some organizations have chosen customized installations that draw on data regarding units from sources other than Active Directory for a number of reasons. Some have chosen a direct integration and maintain the entire hierarchical structure from outside Active Directory while others feed a shadow Active Directory-structure.

Three common Organizational unit Scenarios

Below is a description of the three most common scenarios regarding Organizational units:

- **The Organizational units must be created from scratch**

  The organization does not have its Organizational unit or users in Active Directory. The Organizational unit structure must be implemented and each Organizational unit must be created in Active Directory.

- **The Organizational units need restructuring**

  The organization has implemented Active Directory and has created Organizational units and users but not in a hierarchy and the Organizational unit-structure needs these to comply with Active Directory.

  The task is to make sure that all the necessary Organizational units are structured in a hierarchy that takes the organization's unit access codes into account, since the user's Organizational unit membership determines which unit access codes are available to each user (recursively from sub-Organizational unit to main Organizational unit).

- **The OUs need not be transferred**

  The organization has implemented Active Directory and has created Organizational units but does not want to change their structure to fit the Active Directory. The organization can choose a transfer that excludes Organizational units but includes users and security groups.

  To do this, the configuration file must be customized and the user to unit relationship must be established in an alternate way. Maintenance of the units' register then needs to be established through integration to a system where this is feasible.

  A solution like this may be vulnerable due to the timing between transfers from two or three different sources.

This guide is based on the situation **The Organizational units must be created from scratch** above. That is, Organizational units, users, and security groups (group access codes and committees) must be implemented.

Create an organizational unit

Create an Organizational unit

Perform the following steps to create an Organizational unit in Active Directory.

1. Open **Active directory Users and computers**. In the Active Directory tree, right-click the **domain name** at the top of the tree and click **New** > **Organizational unit**. The **New Object – Organizational** dialog box appears.
2. In the **Name** field, enter the full name of the Organizational unit, for example, `Library`.

   Create an Organizational unit at the top of your organization, for example, `<name of the top of your organization>` with each sub entry inside the top Organizational unit. In this example, `Library` is the top one. `Circulation`, `Reading Room`, and `Administration` are child Organizational units to `Library`.

1. Click **OK** to add the entry. Right-click the created Organizational unit and click **Properties**.
2. The *<name of the top of your organization>* **Properties** dialog box appears, in this example `Library`. In the **Description** text box, enter the abbreviation of the library, for example, `LIBR`. Click **OK**.

   The abbreviation is name code of the library and a part of its ID in the **Units** register in WorkZone Content Server. [1]

   For more details about the transfer of additional information from Organizational units, see section Field data concerning Organizational units.
3. Create the additional Organizational units of your organization's hierarchy one by one.
4. Right-click *<name of the top of your organization>* for example, `Library` and

select **New > Organizational unit** to create the next Organizational unit.

5. Perform the steps 2 and 3 again.

[1] Some restrictions regarding characters and length may apply. For more information, see Organizational unit name restrictions.

Register Organizational units in SJ Active Directory Connector

Configuration of Organizational units

To perform the transfer and alignment of Organizational unit data, SJ Active Directory Connector needs to register Organizational units that belong to the Active Directory. If it is not registered, the configuration file will not work correctly.

Register Organizational units in SJ Active Directory Connector

1. Start SJ Active Directory Connector.
2. The **SJ Active Directory Connector** window appears. Click **Edit**.
3. The **Active Directory Connector Configuration** window appears. In the **Domain server** section, click **Edit**.
4. The **Domain Server** dialog box appears. In the **Units** section, click **Add**. The **Unit** dialog box is displayed.
5. In the **Full name** list, select an Organizational unit at the top of your Organizational unit hierarchy, for example, `Library`.

   If two or more Organizational units have the same full name, they are distinguished by their **Distinguished name** in the relevant dialog box.

   For instance, two Organizational units in different departments are both called SEC, that is, Secretariat. In Active Directory they are displayed in the following way:

   ```
   SEC <DN : OU=SEC,OU=DEP1,DC=udvad,DC=local>
   SEC <DN : OU=SEC,OU=DEP2,DC=udvad,DC=local>
   ```

   Where SEC is the name and the following string is the distinguished name - DN.

   Select the **Recursive** check box. The child Organizational units of the selected OU will be transferred as well.

   You only need to select **Recursive** once, because all future child Organizational units are instantly known to the SJ Active Directory Connector.

   Click **OK**.
6. The **Domain Server** dialog box appears. Click **OK** to exit.
7. In the **Configuration file** section of the **Active Directory Connector Configuration** window, click **Save** to commit your recent changes to the configuration file. Click **Exit**.
8. The **SJ Active Directory Connector** window appears. Click **Exit** to finish.

Create group organizational units

1. Open **Active directory Users and computers** and the AD tree is displayed. Right-click the OU in which you wish to organize your group access codes, (for example, `SJ_OU_GROUPS` in the AD tree) and select **New** > **Group**. The **New Object – Organizational** dialog box appears.
2. In the **Group name** field, enter the name code of the department, for example LIBR.

   > **Note:** Your entry must be in upper case and within the length specified in WorkZone Configuration Management – max 30 characters.

   The **Group name (Pre-Windows 2000)** field is automatically filled in.

   Leave **Group scope** and **Group type** as they are and click **OK**.
3. Right-click the group you just created, for example `LIBR`, and select **Properties**.
4. On the **General** tab, change the description to the name of the OU in the **Description** field, and change the **E-mail** to either `OVERMYN`, `MYNDIGHE`, `AFDELING`, or `KONTOR`.

> **Tip:** You have only to fill out the **E-mail** field if you have an installation with corporate access code.

- `OVERMYN`, if the organizational unit belongs to the executive authority level (Danish: overmyndighed).
- `MYNDIGHE`, if the organizational unit belongs to the authority/department level (Danish: myndighed).
- `AFDELING`, if the organizational unit belongs to the section level (Danish: afdeling).
- `KONTOR`, if the organizational unit belongs to the office level (Danish: kontor).

It is possible to use another field than the **E-mail** field. You can change it in the configuration file.

5. Click the **Members** tab.
6. Click **Add**. You can add:

   - One or more groups representing Organizational units
   - One or more users

   It is possible to have an Organizational unit and a user as members in more than one Organizational unit group, BUT the Organizational unit/User structure in WorkZone Content Server only allows that an Organizational unit group and a user are members of one Organizational unit group. Equally, there should not be any circular references between Organizational unit groups.

7. In the **Select, Users, Contacts, Computers, or Groups** dialog box, enter the name or part of the name and click **Check Names**.

   - If there is only one match, the name appears directly in the **Enter the object names to select** text box area.
   - If there are multiple matches, the **Multiple Names** dialog box is shown.

In the **Multiple Names** dialog box you can:

- Select the name you were looking for.
- Press the `Ctrl` key while you select more than one name.

> **Tip:** Alternatively, if you know from the start you are looking for several users, you can separate entries with semicolon - `hen;pel;elp`.

8. Click **OK** when the name (or all the names you have selected) in step 7 appear in the **Select Users, Contacts or Computers** dialog box in the **Enter the object names to select** field.

9. In the **<group name> Properties** dialog box, the added members are listed. Click **OK** to verify.

Register group Organizational unit in SJ Active Directory Connector

To perform the transfer and alignment of Organizational unit data, SJ Active Directory Connector needs to know the security group that identifies the department, that is the group Organizational unit that is not member of any other group Organizational unit.

A prerequisite for this is that the distribution group `ScanJourCaptia<database>OUs` is a child of the OU `ScanJourCaptiaAdministration`. If that is not the case, see Create the ScanJourCaptia<database>Organizational units distribution group .

1. Open **Active directory Users and computers** and the Active Directory tree is displayed. Click the Organizational unit `ScanJourCaptiaAdministration` to open it. Right-click the `ScanJourCaptia<database name>OUs` distribution group and select **Properties**.
2. Click the **Members** tab.
3. Click **Add** to add root group Organizational unit's only. Type the name or part of the name and click **Check Names**.

    - If there is only one match, the name appears directly in the Enter the object names to select text box area.
    - If there are multiple matches, the **Multiple Names** dialog box is shown. In the **Multiple Names** dialog box you can select the name you were looking for and press the **Ctrl** key while you select more than one name.

> **Tip:** If you know from the start you are looking for several group OUs, you can separate entries with semicolon - `AFD1;AFD2;AFD3`.

4. Click **OK**.

Create the ScanJourCaptia<database>Organizational units distribution group

The `ScanJourCaptia<database>OUs` distribution group must be child to the Organizational unit `ScanJourCaptiaAdministration`.

The presence of this distribution group indicates to the WorkZone Active Directorythat WorkZone Organizational units are represented by groups in the Active Directory, and that the root group Organizational units can be found as member to this group.

1. Open **Active directory Users and computers** and the Active Directory tree is displayed.
2. Right-click on the Organizational unit `ScanJourCaptiaAdministration` and select **New** > **Group**. The **New Object - Group** dialog box is displayed.
3. In the **Group name** field, enter `ScanJourCaptia<database>OUs`.
4. Leave **Description** and **E-mail** empty.
5. In **Group scope**, select **Universal**.
6. In **Group type**, select **Distribition**.

Field to field transfer between Active Directory and WorkZone Content Server

This topic describes the default configuration with regard to transfers from Active Directory fields to fields in WorkZone Content Server.

You can make the changes to the default configuration only in collaboration with – or the knowledge of – your software provider, for example, KMD.

You can also do the specific changes, additions or removals of data, to fit your organization or Active Directory-setup in the `SJADConfiguration<database name>.xml` configuration file.

In the tables below you can see where you can make the changes: in the rows without a check mark (✓) in the **Mandatory dependency** column.

Furthermore, the table shows you how the transfer of information is mapped (or aligned) field by field. However, note the following exclusions:

- The fields automatically transferred via SOM, for example, the **Registered by** field in the **Addressee** register.

- The tables created for the internal audit of the transfer itself.
- Any relations to access codes.

Field to field mapping

The field to field information mapping in the default configuration between Active Directory and WorkZone Content Server database is marked in the columns **Mandatory value** and **Mandatory dependency**.

- If the **Mandatory value** column is checked (✓) in the row, for example, user log-on name, this means that the value is mandatory in Active Directory and will be transferred. If the value is missing, the data cannot be aligned.
- If the **Mandatory Dependency** column is checked (✓) in the row, for example, user log-on name, this means that the data will always be filled in according to the equivalent Active Directory-field or in case of a note according to the convention specified in the note, for example, (7).
- The transferred from Active Directory to WorkZone Content Server field information that becomes a name code will always be transferred capitalized, for example, `ELP`.

Field data concerning users

User table - Field information regarding users

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Serverfield	Mandatory dependency	Mandatory value
User logon name (pre-Windows 2000)	sAMAccountName	employe	name_code	✓	(7)
User logon name (pre-	sAMAccountName	employe	name:name_code	✓	(7)

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Serverfield	Mandatory dependency	Mandatory value
Windows 2000)					
First name	givenName	employee	name:name1		
Last name	Sn	employee	name:name2		
Telephone number	telephoneNumber	employee	address:phone_no(address_type=HA)		
Street	streetAddress	employee	address:address1 (address_type=HA)		
Zip/postal code	postalCode	employee	address:postcode (address_type=HA)		
Country/region	c	employee	address:country_code (address_type=HA)		
E-mail	Mail	employee	address:email (address_type=HA)		
Description	Description	employee	text		

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Serverfield	Mandatory dependency	Mandatory value
		employe-location_code			(1)
		employe-resigned			✓ (2)
		employe-name:end_date			✓ (2)
User logon name (pre-Windows 2000)	sAMAccountName	users	user_name	✓	(7)
	objectSid	users	Sid	✓	(8)
		users	Ntauthentication	✓	(3)
		users	Ntname	✓	(4)
		users	Authority	✓	(5)
		users	bem	✓	(6)

Notes

(1) Is filled in as the `name_code` of the Organizational unit containing the user. May be overridden by a customer Active Directory field.

(2) Is only filled in if the employee is no longer transferred from Active Directory. Left blank if the employee is transferred again at a later date.

(3) Is filled in as default value `J`.

(4) Is filled in as `<domain name>\<sAMAccountName>`.

(5) Is filled in as the name code of the Organizational unit containing the superior level

Organizational unit in the Organizational unit register if it has the value `MYNDIGHE;`, otherwise is left blank.

(6) Is filled in as `user_name - name:name1 name:name2`.

All these fields will be filled in with the same value. The value either comes from `sAMAccountName` or an alternative specified field.

If an alternative field is specified, the `<SJName>` tag must mention the field name `user_name`. For example, if using the description field in AD for the `name_code`, the following piece of XML should be added:

(7)

```
<userField>
<ADName>description</ADName>
<SJName>user_name</SJName>
<mandatory>true</mandatory>
</userField>
```

(8) This field is selected in the default configuration, and KMD recommends you not to change it. If, however, it is for some reason necessary to read the users' SIDs from a different field, it may be configured in the configuration XML-file under the tag `<userSIDADFieldname>` in the `<configuration>` section. In such situations KMD recommends to use the `securityIdentifier` field, as it has the appropriate format and is not used by Microsoft.

Field data concerning Organizational units

Field information regarding Organizational units (OU) is listed below:

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Server field	Mandatory value	Mandatory dependency
`Description`	`Description (1)`	`OU`	`name_code`	✓	
`Description`	`Description (1)`	`OU`	`name:name_code`	✓	
OU name	`OU`	`OU`	`name:name1`	✓	

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Server field	Mandatory value	Mandatory dependency
		OU	parent_ou	✓	✓ (2)
		OU	end_date	✓	✓ (3)

Notes

(1) This field is selected in the default configuration. However it is possible to change it in the Active Directory **Configuration** window in the **Organizational unit AD** field to use as identifier text box. You can specify each Organizational unit's name code explicitly.

(2) Filled in as the name code of the parent Organizational unit in Active Directory, if this is being transferred. Otherwise, it remains blank.

(3) Filled in if the Organizational unit is no longer transferred from Active Directory. Left blank if the Organizational unit is transferred again at a later date.

Field data concerning the distribution group: Groups

Global security groups that are the members of the groups distribution group are only transferred into group access codes if at least one user is a member of the unit access code in question.

Field data concerning the distribution group: Committees

Field information regarding committees is listed below:

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Server field	Mandatory value	Mandatory dependency
Group name (pre-Windows	sAMAccountName	contact	name_code	x	x

Name in AD GUI	ADSI name	WorkZone Content Server register	WorkZone Content Server field	Mandatory value	Mandatory dependency
2000)					
Group name (pre-Windows 2000)	sAMAccountName	contact	name1	x	
		contact	end_date	x	x (1)

Note

(1) Filled in as the name_code of the Organizational unit containing the user. May be over-ridden by a customer Active Directory-field.

ADSI field names

This section describes the Active Directory Service Interfaces (ADSI) fields which can be used when customizing the configuration file `SJADConfiguration<database name>.xml`.

ADSI field names for users

ADSI field names for the description group: Groups

ADSI field names for Organizational units

ADSI field names for Organizational units

The table below displays the Active Directory Service Interfaces (ADSI) equivalent of the Active Directory field names for Organizational units:

AD Field name	ADSI Field name
Name	ou

AD Field name	ADSI Field name
Description	description
Street	street
City	l (lowercase L)
State/province	st
Zip/postal Code	PostalCode
Country/region	c

ADSI field names for the description group: Groups

The table below displays the Active Directory Service Interfaces (ADSI) equivalent of the Active Directory field names for groups:

AD Field name	ADSI Field name
Name	ou
Description	description
E-mail	mail
Notes	Info

ADSI field names for users

The table below shows the Active Directory Service Interfaces (ADSI) equivalent of the Active Directory field names for Users:

	AD Field name	ADSI Field name
General		
	First name	givenName
	Initials	initials
	Last name	sn

	AD Field name	ADSI Field name
	Description	description
	Office	physicalDeliveryOfficeName
	Telephone number	telephoneNumber
	E-mail	mail
	Web page	WWWHomePage
Address		
	Street	streetAddress
	P.O. Box	postOfficeBox
	City	l (lowercase L)
	State/province	st
	Zip/Postal Code	postalCode
	Country/region	C
Telephones		
	Home	homePhone
	Pager	pager
	Mobile	mobile
	Fax	facsimileTelephoneNumber
	IP Phone	Phone ip
Organization		
	Title	title
	Department	department
	Company	company

Character restrictions

There are character restrictions to Organizational unit, user names, unit access codes, and global distribution groups.

For a description of the restrictions relevant for each element, see:

- Organizational unit name restrictions
- User name restrictions
- Group name restrictions
- Committee name restrictions

> Important: In general, do not use other characters, symbols, or digits than the ones mentioned in this section.

Organizational unit name restrictions

The following restrictions apply to the **name_code** (with standard configuration this is the value in the **Description** field):

- Maximum length is 30 characters. However, it must not exceed the length of **Address Type A' s Address Code** as configured in WorkZone Configuration Management, see Configuration of contact types.
- The only allowed characters are:
    a. Letters (including Æ, Ø and Å)
    b. Digits
    c. The following special characters:
        - Period (.)
        - Underscore (_)
        - Dash (-)

User name restrictions

The following restrictions apply to user log-on name for WorkZone Content Server:

- The user name in the **User logon name (pre-Windows 2000)** field in Active Directory has a maximum length of 20 characters. This is a restriction in the Active Directory. WorkZone Content Server allows up to 30 characters. You can utilize this by opting for an alternative field for the transfer of name code/user code.
- The user name in the **User logon name (pre-Windows 2000)** field must not exceed the length of **Address Type M' s Address Code** as configured in WorkZone Configuration Management, see Configuration of security codes.
- The only allowed characters are:
    a. Letters (including Æ, Ø and Å)
    b. Digits
    c. The following special characters:
        - Period (.)
        - Underscore (_)
        - Dash (-)

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 (-).

Committee name restrictions

The following restrictions apply to the **Group name (pre-Windows 2000)** Active Directoryfield.

- Maximum length is 30 characters. However, it must not exceed the length of **Address Type Organizational unit's** Address Code as configured in WorkZone Content Mobility (or any alternative Address Types generated), see Configuration of contact types.
- The only allowed characters are:
    a. Letters (including Æ, Ø and Å)
    b. Digits
    c. The following special characters:
        - Period (.)
        - Underscore (_)
        - Dash (-)

Manipulating name code

Default handling of name code

If your user name (name code) exceeds 20 characters or there are Active Directory prefixes that you do not want to transfer, you can strip the name before transferring from Active Directory.

Normally, the name code in WorkZone Content Server database is transferred as follows:

- Users: *<pre-Windows 2000 logon>* name.
- Units: *<pre-Windows 2000 logon>* name or other Active Directory-field. (default=description) or alternatively custom integration explicitly modified in the configuration file.
- Groups: *<pre-Windows 2000 logon>* name.
- Committees: *<pre-Windows 2000 logon>* name.

The name code instances mentioned above can be manipulated in 3 ways.

Stripping

Regular expression

Replacement

Stripping

Stripping of xml-elements

The name code instances mentioned above can be manipulated as described below before they are stored in the WorkZone Content Server database.

You can strip a defined leading and/or trailing part of a string of the data from AD. To do this, use one of the following XML elements in the `SJADConfiguration<database name>.xml` configuration file:

- leading: `<stripPrefix>`
- trailing: `<stripPostfix>`

The XML element must be entered as a sub-element of the `<domain>` element to facilitate the possibility of different name code stripping for alternate domains.

Only name codes with the defined part of the string are stripped; all others are left unchanged. You can only strip one prefix and one postfix for each kind.

The attribute kind

Both elements have an optional attribute called `kind`. The legal values of the attribute are:

- `user` - User codes will be stripped.
- `unit` - The unit codes (OUs in AD) will be stripped.
- `group` - Group access codes will be stripped.
- `committee` - Committee codes will be stripped.

> **Note:** Exclusion of the attribute will be interpreted as `kind="user"`.

The part of the string you wish to strip should always be written in CAPITAL LETTERS since they are name codes.

Example 1

```
<stripPrefix>T-</stripPrefix>
```

This stripping string will result in all user codes from the relevant domain beginning with `T-` will be stripped of these; all others will be left as they are:

AD code	WZCS code
T-VIGGO	VIGGO
HUGO	HUGO

Example 2

```
<stripPrefix kind="user">T-</stripPrefix>
```

```
<stripPostfix>O</stripPostfix>
```

This stripping string will result in all user codes from the relevant domain beginning with `T-` and ending in `O` will be stripped of these if they meet the criteria.

AD code	WZCS code
T-VIGGO	VIGG
HUGO	HUG

Example 3

```
    <stripPrefix kind=”unit”>OU-</stripPrefix>
    <stripPostfix kind=”unit”>Z-</stripPostfix>
```

This stripping string will result in all OU codes from the relevant domain beginning with `OU-` and ending in `-Z` will be stripped of these if they meet the criteria.

AD code	WZCS code
OU-DEP1	DEP1
OUDEP2-Z	OUDEPD2

Regular expression

It is possible to specify a regular expression, as if it is fulfilled by name code, results in a series of groups, that can be composed to a new name code by a composing text you specify. In the configuration file `SJADConfiguration<database>.xml`, you add the following XML-elements.

```
    <inRegularExp kind="unit">the regular expression </inRegularExp>
    <outExp kind=”unit”>the composing text</outExp>
```

`unit` can be replaced with either `user`, `group` or `committee`.

The XML elements must be entered as sub elements of the `<domain>` element in order to make it possible to have different name code regular expression for alternate domains.

Example:

```
    <inRegularExp kind="unit">([A-ZÆØÅ0-9]+)-([A-ZÆØÅ0-9\-]+)-
    ([A-ZÆØÅ0-9_]+)-M </inRegularExp>
    <outExp kind="unit"> #1-#2</outExp>
```

`outExp` can be any text, where `#<group number>` is replaced by the text from group `<group number>`.

AD code	WZCS Code	Group 1	Group 2
SOC-ADEL-ABC-SOC-MYN-M	SOC-MYN	SOC	MYN
SAC-ADEL-ABC-SOC-AFDB-M	SAC-AFDB	SAC	AFDB
SAC-ADEL-ABC-SOC-AFDB_TA-M	SAC-AFDB_TA	SAC	AFDB_TA
SAC-ADEL-ABC-SOC-AFDB-TA-SAM_AK-M	SAC-SAM_AK	SAC	SAM_AK
SAC-ADEL-ABC-SOC-AFDB-TA-DAK_AK-M	SAC-DAK_AK	SAC	DAK_AK

For more information about regular expressions, see *Regular Expression Language - Quick Reference* on MSDN.

Replacement

It is possible to specify one or more strings replacement, by the following syntax:

Example:

```
<Instring1>;<outstring1>;<Instring2>;<outstring2>; …<InstringN>;<outstringN>;
```

Example:

```
<replaceText kind="unit">_;-</replaceText>
```

In text	Out text
AFDB_TA	AFDB-TA
SAM_AK	SAM-AK
DAK_AK	DAK-AK

Active Directory replication in an OAuth2 setting

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

WorkZone Cloud and Active Directory synchronization diagam

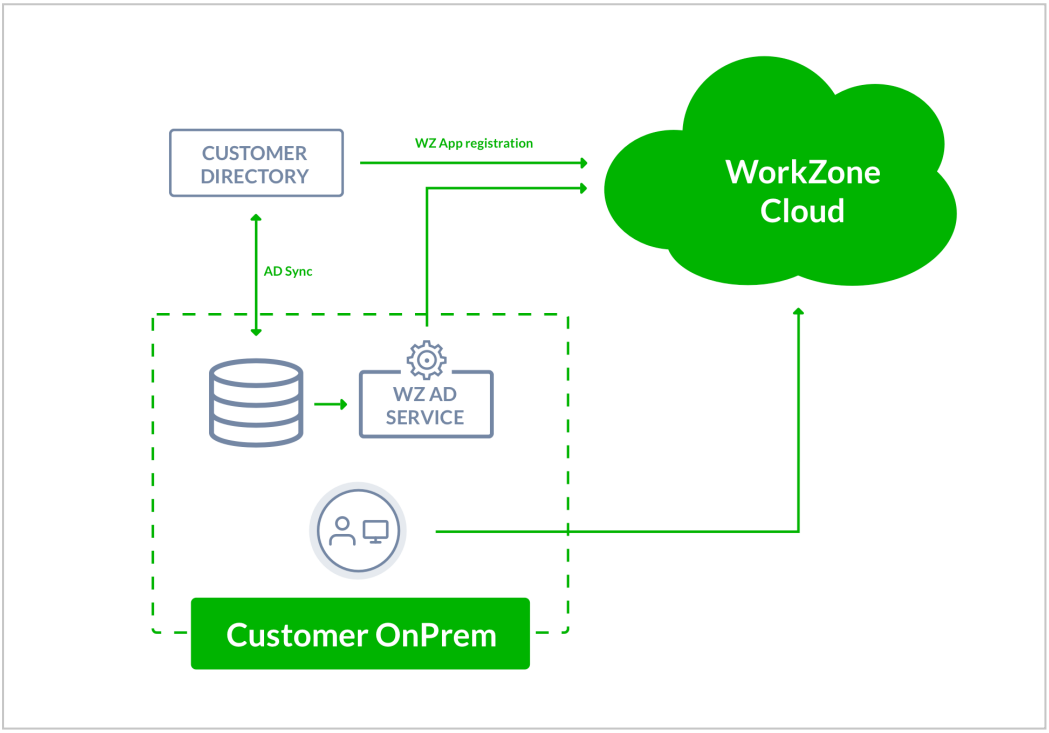


Diagram notes

The customer has an on-premise setup that contains their Active Directory servers and data as well as clients. A WorkZone Content Server is also installed on the on-premise site in order to run the WorkZone Active Directory service for synchronization purposes.

The customer setup also includes synchronization with the Azure Active Directory as well as utilization of the Microsoft Office 365 suite in the Azure cloud environment with Azure Active Directory 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 Azure Active Directory, where an app registration is used for WorkZone Cloud to authenticate the users.

The customer has an on-premise setup that contains their Active Directory servers and data as well as clients. A WorkZone Active Directory is required on the on-premise 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-site and WorkZone Cloud Active Directory replication

Running this type of replication in an OAuth2 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 Azure active directory and the two different environments.

These differences are:

- The active directory replication must be set up to export the active directory structure from the on-site 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.
  The program used to export the Active Directory structure can be set up as a recurring windows task, replicating the active directory structure at a time which fits your organizations' non-working hours, maintenance schedule and back-up timetable
- A Windows service is installed when the WorkZone Content Server is installed in OAuth2 mode in the Azure environment.
  The service is enabled and automatically started on the WorkZone Content Server and will execute the update task and update the WorkZone database with the active directory structure exported by the active directory replication on the on-site domain controller.

See also

- Setting up replication for an OAuth2 environment
- Updating the WorkZone database
- Automation of active directory replication

Setting up replication for an OAuth2 environment

Before you can replicate your active directory structure to your WorkZone Content Server installation in an Azure environment, you must:

1. Install the **wzActiveDirectoryReader.exe** program on a server that has access to the domain controller. The **wzActiveDirectoryReader.exe** program opens the **WorkZone Active Directory Connector** form which is used in the replication process.
2. Configure the replication settings of the **WorkZone Active Directory Connector** form to ensure the replication process can be repeated faithfully and different replication processes can be initiated.
3. Enable active directory replication for an OAuth2 environment in WorkZone Configurator.
4. Transfer the active directory structure from the on-site domain controller to the WorkZone Content Server database in the Azure environment.

See also

Install the wzActiveDirectoryReader.exe program

Configure the replication settings

Enable active directory replication for Oauth2

Transfer the active directory structure

Install the wzActiveDirectoryReader.exe program

The **wzActiveDirectoryReader.exe** program must be installed on the on-site domain controller machine as the program opens the **Active Directory Connector** form which is used to find, export and transfer the active directory structure to the WorkZone Content Server machine in the Azure environment.

Install the wzActiveDirectoryReader.exe program on the domain controller

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

See also

Configure the replication settings

Enable active directory replication for Oauth2

Transfer the active directory structure

Configure the replication settings

Defining the replication settings in the **WorkZone Active Directory Connector** form for an OAuth2 setting is identical to defining the replication settings for an on-site client-server environment, but you must also define the OAuth2 Client Secret for the OAuth2 environment.

How to set up the active directory replication configuration for an Azure environment

You can either create a new active directory connector configuration using the wizard 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. **WorkZone Active Directory Connector Configuration** form> **Client Secret** field, enter the OAuth2 client secret.
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 OAuth2 Client Secret for active directory replication

In order to connect to the WorkZone Content Server database in the Azure environment, you must specify the OAuth2 client secret in the **WorkZone Active Directory Connector Configuration** form. If the OAuth2 client secret is incorrect or omitted, the Active Directory replication will fail.

Defining the OAuth2 Client Secret active directory replication for initial replication

If you are setting up the active directory replication for the first time, you cannot use WorkZone Configurator to generate an OAuth2 Client secret for active directory replication as you will not be able to access the OAuth2 settings page. This is because the access codes that enable your access have not been replicated to the WorkZone database yet.

Instead, you must manually define the OAuth2 Client secret for active directory replication instead of generating it from the OAuth2 settings page in WorkZone Configurator.

The OAuth2 Client secret for active directory replication you specify manually is temporary and when the WorkZone Active Directory Connector is run the first time, a new OAuth2 client secret for active directory replication will be generated and stored internally in the system.

Defining the OAuth2 Client Secret active directory replication for subsequent replication

If the active directory replication has been set up and run successfully at least once and if your user profile exists in the WorkZone database and you are assigned the OAUTH2ADM access

code, you can generate the OAuth2 client secret on the **OAuth2 settings** page in WorkZone Configurator.

The generated OAuth2 Client secret for active directory replication is temporary and when the WorkZone Active Directory Connector is run the first time, a new OAuth2 client secret for active directory replication will be generated and stored internally in the system.

If you make a mistake, you can generate a new client secret again, overwriting the old secret.

> **Prerequisite:** You must be assigned the OAUTH2ADM access code to access the **OAuth2 settings** page in WorkZone Configurator.

To generate an OAuth2 client secret

1. In WorkZone Configurator > **Global** > **OAuth2 settings** > **WZCS.ADReplicator** setting, click **Edit** to open the **1 - OAuth2 settings** form.
2. In the **1 - OAuth2 settings** form
    1. (If you have not enable active directory replication) Select the **Enabled** radio button to enable the active directory replicator for OAuth2.
    2. In the **Client secret** field, click **Generate** to create a new OAuth2 Client secret. Make a note of the client secret, either copying the value to the clipboard or writing it down. The client secret will be encrypted once you click **Save**.
3. Click **Save** to save your changes and close the form.

See also:

- Install the wzActiveDirectoryReader.exe program
- Enable active directory replication for Oauth2
- Transfer the active directory structure
- Test the replication configuration settings

Test the replication configuration settings

You can review the displayed results to make sure the active directory structure is valid and consistent with the settings defined in the active directory replication configuration.

1. On the on-site server, run the **wzActiveDirectoryReader.exe** with administrator privileges to open the **WorkZone Active Directory Connector** form.
2. In the **WorkZone Active Directory Connector** form, click **Display only** to display the results of the active directory structure based on the current configuration displayed in the field above the **total update** check box.

Enable active directory replication for Oauth2

Before you can replicate your active directory users, you must enable active directory replication on the **OAuth2 settings** page in WorkZone Configurator.

> **Prerequisite:** You must be assigned the OAUTH2ADM access code to access the **OAuth2 settings** page in WorkZone Configurator.

To enable OAuth2 active directory replication retrieve and generate an OAuth2 client secret

1. In WorkZone Configurator > **Global** > **OAuth2 settings** > **WZCS.ADReplicator** setting, click **Edit** to open the **1 - OAuth2 settings** form.
2. In the **1 - OAuth2 settings** form
3. Select the **Enabled** radio button to enable the active directory replicator for OAuth2.
4. Click **Save** to save your changes and close the form.

See also

Install the wzActiveDirectoryReader.exe program

Configure the replication settings

Transfer the active directory structure

Transfer the active directory structure

After you have tested the WorkZone Active Directory Connector configuration, you can transfer the active directory structure to the WorkZone Content Server in the Azure environment and an update task to update the database.

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 **Transfer** display the results of the active directory structure and transfer the results to the WorkZone Content Server in the Azure environment.

Copies of the exported active directory structure as well as a log file of the transfer are located in the **C > ProgramData > ScanJour > logs > wzActiveDirectoryReader > *<Database name>* >** folder on the on-site domain controller. The *<Database name>* is the name of the WorkZone database the active directory structure is exported to.

See also

Install the wzActiveDirectoryReader.exe program

Configure the replication settings

Enable active directory replication for Oauth2

Updating the WorkZone database

Updating the WorkZone database

When the active directory structure is transferred to the WorkZone Content Server machine in the Azure environment, a new record in the AD_REPLICATION table of the AD_ REPLICATION register containing the transferred active directory structure data will be created. Additionally, a new record in the SERVICE_QUEUE table will also be created.

The new SERVICE_QUEUE record points to the new AD_REPLICATION record and the database update will be initiated by the **Scanjour Service COM ADW *<database name>*** service, where <database name> is the name of the WorkZone database the active directory structure is exported to and the service is to run on.

The **Scanjour Service COM ADW <database name>** service executes the tasks in the SERVICE_QUEUE table which updates the database with the active directory structure values in the AD_REPLICATION table.

Update the WorkZone database

To update the WorkZone database, start the **Scanjour Service COM ADW <database name>** service from the Windows **Services** form on the WorkZone Content Server machine in the Azure environment.

The **Scanjour Service COM ADW <database name>** service is by default defined to be started automatically when it is installed initially but if this setting has been changed, you must start the service manually.

See also

Active Directory replication in an OAuth2 setting

Setting up replication for an OAuth2 environment

Automation of active directory replication

Automation of active directory replication

Instead of manually executing the active directory transfer and manually starting the **Scanjour Service COM ADW <database name>** service to update WorkZone database, you can automate both procedures, making sure to schedule the tasks at times where the system is not being used or when system and database backups are not running.

Automate the active directory transfer

You can create a shortcut to the **wzActiveDirectoryReader.exe** program, define any parameters and arguments necessary, for example specifying which active directory replication configuration to use and then define a scheduled task on the on-site domain controller to run the task and execute the **wzActiveDirectoryReader.exe** program at predetermined time intervals, for example every night at 01:00, or right after back-up routines are expected to be completed.

Automate the update service

The **Scanjour Service COM ADW <database name>** service is by default defined to be started automatically when it is installed initially but if this setting has been changed, you must set up the service to start automatically.

See also

- Active Directory replication in an OAuth2 setting
- Setting up replication for an OAuth2 environment
- Updating the WorkZone database

Best practices and recommendations

Below you will find recommendations, best practices, and general advice concerning SJ 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 Content Server with SJ 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 **SJ 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 SJ 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 SJ 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 SJ Active Directory Connector, you need to re-enter the password 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 **SJ 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 Content Server.

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 SJ 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 Content Server Fields

The configuration file contains the information regarding which AD field is transferred to which WorkZone Content Server 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 Content Server and ADSI field names.

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
`/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 Content Server. Normal replication is not performed - only this single user is handled.

Parameter	Default value	Comment
`/useGroupAsOU`	No default value.	When used, the wizard uses the template `SJADConfiguration-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.

Monitor the transfer

You can check the quality of your transfer from Active Directory to WorkZone Content Server at any time. Each time you have made essential changes to your AD or the SJ Active Directory Connector, you can check the quality of the transfer.

Check the quality of transfer

1. Start SJ Active Directory Connector to open **SJ Active Directory Connector** form.
2. Click **Display only** (a trial transfer from Active Directory to the display only).
   If there are any errors, these will be listed in the window with `error` where `info` is usually shown.
3. Make the necessary changes. Repeat steps 1-2.
4. If your trail transfer comes up without any errors in your status window, click **Transfer**.
5. Even if the transfer has been completed successfully, check your **Event Viewer**:
   Click **Start** > **Control panel** > **Administration tools** > **Event Viewer**.

   Check the event log to find out if any issues occurred while the transfer, as they may not be listed in the status window.

   The event log may catch transfer problems that do not show up in your status window, see Best practices and recommendations for more details.

Corporate access code

If your organization has chosen a corporate codes installation, there are some minor deviations from the topics in this guide. However, in general the methods previously described in Active Directory also apply here.

Prerequisite:

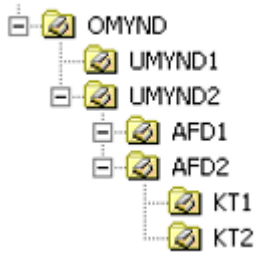
- The database installed to support corporate access codes. See About the database for further information.
- The scheduled task for **Lost and Found** has been set up. See About installing WorkZone Content Server for further information. It is a standard installation with corporate access code.
- Knowledge of how your organization requirements use the installation with corporate access code.

Configuring the Transfer from Active directory

The configuration of corporate access codes includes creating Organizational units for the company. The Organizational units are transferred from Active Directory as Organizational units.

Prerequisite: This means that the Organizational units must exist in Active Directory, before you can transfer between Active Directory and the database. You can create the Organizational units in Active Directory as described in Creating organizational units in Active Directory.

This is an example of a typical Organizational unit configuration in Active Directory:



Four levels of a standard installation with corporate access code:

- <OMYND> = Executive authority
- <UMYND>= Authority/department
- <AFD>= Section
- <KT> = Office

The following rules apply:

1. Top level Organizational unit must be known to Active Directory Connector, see Register Organizational units in SJ Active Directory Connector.
2. Users are always placed at the office level, for example, KT1, seeCreate users in Active Directory.

The effect of the above configuration will result in the following: The end-user AA, for instance, who is a member of the OU KT1 (office 1), will organizationally be placed in the framework: UMYND2, in AFD2, in KT1 - all under OMYND and segregated from any other authorities sharing the same database of OMYND.

This means that when AA creates, for example, a case in WorkZone Content Server, the case is automatically supplied with the access code string UMYND2 & ALLEEMNER:

- UMYND2 is the access code of the authority to which AA belongs.
- ALLEEMNER is a dummy access code assigned to items if none is inherited from either class or case. All users are members of this access code. See ALLEEMNER - Default group access code below.

Note: You can have more than the four levels mentioned in the example above and you can name them according to your organization.

Configure the transfer from AD

1. Do the following:

    - Open the configuration file `SJADConfiguration<database name>.xml` on the server, where the replication is to be made.
    - Search for the text `<unitField>` and add the following `<unitField>` statement after the existing:

```
<unitField>
    <ADName>st</ADName>
    <SJName>OU_GRP</SJName>
    <mandatory>false</mandatory>
</unitField>
```

    This addition will have the effect that the field `OU_GRP` is replicated from the **State/-province** field in AD.

    Note: If you want to use the **City** field or the **Zip/Postal Code** field instead of the **State/-province** field, you must replace the text `<ADName>st</ADName>` with one of the following:

    - `<ADName>l</ADName>` (representing the **City** field).
    - `<ADName>postalCode</ADName>` (representing the **Zip/Postal Code** field).

2. Save and close the configuration file.
3. Open Active Directory as described in Create an organizational unit.

    The **Active Directory Users and Computers** window appears.

4. Do the following for each OU:

    - In the tree structure in the left part of the window, right-click the name of the organizational unit to be transferred.

- Right-click the organizational unit and select **Properties**. The *<organizational unit>***Properties** window appears.

5. On the **General** tab select one of the following values in the **State/province** field according to the way your organization wants to utilize the installation with corporate access code:

   - `OVERMYN`, if the Organizational unit belongs to the *overmyndighed* level (executive authority).
   - `MYNDIGHE`, if the Organizational unit belongs to the *myndighed* level (authority/department).
   - `AFDELING`, if the Organizational unit belongs to the *afdeling* level (section).
   - `KONTOR`, if the Organizational unit belongs to the *kontor* level (office).

   - This implies that you selected the **State/province** field in step 1, and that you are using the standard solution of the corporate access code system. If you are using a customized solution, the naming of the Organizational units might be different.
   - You can change the names of these values and have more than four levels to reflect the structure of your organization.

6. Click **OK**.
7. Repeat step 3 to 5 for every Organizational unit that needs to be transferred.
8. Proceed with the transfer as described in Transfer data.

Special access codes in AD for corporate access code installations

You must create a special group in AD for installations with Corporate Access Code System (CACS) to work properly.

ALLEEMNER - Default group access code

All cases and documents in an installation with corporate access code are created with an access code string of a minimum of two access codes: One organizational access code and one group access code.

These strings are the foundation of the complete separation between each individual authority (DA: "Myndighed") in the database of an installation with corporate access code. However, when a class or document has no inherited group access code, that is, either from the class or the case a document is attached to, a default group access code is necessary to comply with the rule of minimum one organizational access code and one group access code. This default group access code is `ALLEEMNER`.

Register WorkZone in Azure

WorkZone Azure AD 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.

The WorkZone Process module requires additional application registrations.

> **Prerequisite:**
>
> When creating an application registration for WorkZone, the full hostname of the WorkZone instance must be used as the identifier URI. For example, if WorkZone should be accessible at `https://wzExample.test.workzone.cloud`, then the identifier URI must be "https://wzExample.test.workzone.cloud".
>
> Because of the requirements for the identifier URIs, only verified custom domains can be used in the URIs. For more information about adding a custom domain, see the Microsoft article Add your custom domain name using the Azure Active Directory portal.
>
> If you have issues with the verification of the domain, WorkZone DevOps can assist you.

Register the application

> **Note:** The download location for the scripts mentioned in this topic will be supplied when you request a WorkZone environment.

To register WorkZone in your Azure AD, run the `New-KmdWorkZoneIdentityAp.ps1` script.

Use the following parameters:

- `DisplayName`: Display name of the Azure AD app.
- `IdentifierUri`: Identifier URI of the Azure AD app that is also used for updates (script reruns). See the prerequisite for the domain above.
- `ReplyUrlPrefix`: Prefix for the reply URLs. This should match the IdentifierUri. For example, `https://wzExample.test.workzone.cloud`.
- `TenantId`: Azure AD Tenant ID.

> **Example**:
>
> ```
> .\New-KmdWorkZoneIdentityApp.ps1 `
>       -DisplayName 'KMD WorkZone - Production' `
>       -IdentifierUri 'https://wzExample.test.workzone.cloud' `
>       -ReplyUrlPrefix 'https://wzExample.test.workzone.cloud' `
>       -TenantId XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX `
> ```

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

Register the application for WorkZone Process

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 Azure AD app.
- `TenantId`: Azure AD 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.

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 Azure AD 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"
```

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.

The WorkZone Content Server 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.	• Work with delegates
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 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.	• Corporate access codes
CONFIGADM	**WorkZone Client:** • Configure and distribute WorkZone Client configurations. • Edit templates for reports. **WorkZone Configurator:** Configure settings of: • WorkZone PDF Crawler • WorkZone PDF Engine	• Working with WorkZone Client configurations • Reports • Work with delegates • WorkZone PDF settings • WorkZone for

Access code	Usage	More information
	• 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	Office settings • WorkZone Explorer configuration • Custom types • Custom type fields • Chat settings
DATAADM	**WorkZone Configurator:** 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	• Cases, documents, and contacts • Custom types • Custom type fields • Security group rights

Access code	Usage	More information
	• 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	
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
DIAGADM	**WorkZone Configuration Management**: • Use of trace log	• The Diagnostic module
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 and not part of the Content Management module.	

Access code	Usage	More information
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 • Documents • Contacts **Prerequisite:** Users must have the * access code to display, open and edit the displayed hidden items.	• Hidden entities
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

Access code	Usage	More information
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.	
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. **WorkZone Configuration Management:** • State (CM)	• Process settings • Process logs • Export and deploy case activity graphs • Unlocking a locked task • Work with delegates
RETENTIONADM	**WorkZone Client:** • Change the retention policy on a case. **WorkZone Configurator:** • Set up and maintain retention policies.	• Meta data fields • Retention policies

Access code	Usage	More information
SOFTDELETE	**WorkZone Client:** • Send cases and archived documents to the recycle bin. • Restore cases and archived documents from the recycle bin. • Delete cases and documents permanently if you have access code associated with the case's or document's retention policy.	• Delete a case • Restore a deleted case • Delete a document • Restore a deleted document
STEPSUBMISSION	**WorkZone Process:** • Displays the **Advanced submission (Extended)** process in the **Process** menu in WorkZone Client and WorkZone for Office, and allows users to start advanced submissions. • Create, delete and edit templates for advanced submissions.	• Start an advanced submission • About templates for advanced submissions
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.	• Global and departmental access

Access code	Usage	More information
	• 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 information. Assign these rights only when needed.	
TEMPLATEADM	**WorkZone Process:** • Create templates for standard letters used by SmartPost.	• Configure standard letters
TERMSADM	Set up and maintain the Terms module.	• The Terms module
USERADM	Gives rights and access to these modules in WorkZone Configuration Management: • **Owner** Access and configure in WorkZone Con-	• Users • Use logs • Deletion logs

Access code	Usage	More information
	figurator: • **Users** • **Use Logs** • **Deletion Logs**	
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 menuitem
CONTENT_SERVICES	Enable and disable Content Services.
FILINGPERIOD	Used in the now discontinued Captia Web Client. A system access code for enabling Filing Period menuitems.
LISTCONF	Used in the now discontinued Captia Web Client. A system access code for list configuration.

Access Code	Notes
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 with-drawn Phrases module.
PHRASEEDIT_ORGANIZATION	Used to manage access to the obsolete and with-drawn Phrases module.
PHRASEEDIT_USER	Used to manage access to the obsolete and with-drawn Phrases module.
POST	Used to manage access to mail lists.
PROFILADM	Used in WorkZone Configuration Management Used to manage access to Sysadm profile admin-istration module.
RAPDEF	A system access code which provides access to old reports created with Crystal Reports (3rd party product).
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.

After installation

After installation, use the post-installation checklists and test the installation to ensure that all steps were completed properly.

Check Content Security Policies

To enhance effective security controls available to the web browser and help prevent client-side attacks, such as Cross-Site Scripting, Content Security Policies have been configured by default for WorkZone Client and WorkZone Configurator.

A correctly configured Content Security Policy response header enables WorkZone Clientor WorkZone Configurator to define which content sources the browser may load. A strict policy can help mitigate the risk of various content injection vulnerabilities, including XSS and click-jacking attacks and help prevent an attacker from inserting crafted content, such as malicious JavaScript or CSS, which could result in XSS or CSS injection attacks.

While a correctly configured Content Security Policy can help mitigate the risk associated with injection attacks, it should be considered a defense-in-depth measure for injection attacks, as it is dependent on browser support.

Default WorkZone Client policy

The default WorkZone Client Content Security Policy is:

default-src data: *; frame-src blob: ms-access: ms-infopath: ms-project: ms-publisher: ms-visio: ms-word: ms-powerpoint: ms-excel: *; script-src 'self' 'unsafe-eval' 'unsafe-inline' blob:; connect-src *; img-src 'self' data:; style-src 'self' 'unsafe-inline'; frame-ancestors 'self';

Default WorkZone Configurator policy

The default WorkZone Configurator Content Security Policy is:

default-src 'self'; font-src 'self' data:; script-src 'self' 'unsafe-eval'; connect-src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; frame-ancestors 'self';

Troubleshooting issues

If your organization experiences connectivity issues or issues with the execution of scripts or other code snippets in browsers accessing WorkZone Client and WorkZone Configurator, these issues might be attributed the default Content Security Policy values.

You can check the default Content Security Policies on the Microsoft IIS 7 server in the IIS Manager form to see if the policy performs as expected and adjust the policy values if necessary.

You can also check the Content Security Policy settings by using the developer tools in the relevant browser or by using 3rd party development tools – for example Postman (a platform for API development).

Configure a Content Security Policy

Content Security Policies can be inspected and configured on a Microsoft IIS 7 server in the IIS Manager form:

1. On the Microsoft IIS 7 server, open the **IIS Manager** form.
2. In the **IIS Manager** form > **Features** View, select **HTTP Response Headers** to open the **HTTP Response Headers** page.
3. On the **HTTP Response Headers** page > **Actions** pane, click **Add** to open the **Add Custom HTTP Response Header** form.
4. In the **Add Custom HTTP Response Header** form > **Name** field, enter a name for your Content Security Policy, for example Content-Security-Policy.
5. In the **Add Custom HTTP Response Header** form > **Value** field, configure the policy you want to apply.
6. Click **OK** to save your policy

Important notes regarding the Content Security Policy

A Content Security Policy header allows you to define approved sources for content that the browser can load. By specifying only those sources that you wish the browser to load content

from, you can help prevent loading malevolent or harmful content that may have been placed on the site or page.

A Content Security Policy header is only enforced per page. The browser will not cache a Content Security Policy header and continue to enforce the policy. You must send the Content Security Policy header with every response you want the policy to be enforced on.

Browser support

The Content-Security-Policy header is supported in all latest versions of Chrome, Edge, FireFox, Safari (OSX and iOS), Opera (but not Mini), Android Browser and Chrome for Android.

The Internet Explorer browser requires the X-Content-Security-Policy header instead so you must issue the header twice if you want to have the most widespread support for the Content Security Policy header.

Test the Policy

After you have configured the Content Security Policy, you can test the policy by sending the header **Content-Security-Policy-Report-Only:** instead of the **Content-Security-Policy:** header.

Your browser will still receive and act upon the configured policy, but the browser will display a list of the expected effects of the defined policy.

Post-installation checklists

Use the post-installation checklists to ensure that all steps were completed.

WorkZone for Office post-installation checklist

When you have installed WorkZone for Office, perform the following steps to verify that the installation is complete.

☑	To be verified	Comments
☐	Enure that versions of WorkZone for Office server and WorkZone for Office clients are absolutely equal.	Check build numbers in the **Add/Remove Pro-**

☑	To be verified	Comments
		grams page.
☐	Ensure that release versions of WorkZone for Office and WorkZone Content Server are equal.	Check release versions.
☐	Check availability of the **Office Services** feature in WorkZone Content Server installation.	See Testing web services.
☐	Ensure that WorkZone Content Server has installed the WorkZone for Office default values correctly.	See Required data and default values.
☐	Test the installation.	See Testing WorkZone for Office.
☐	Check the Event Viewer for any issues listed for administrative events.	

WorkZone PDF post-installation checklist

When you have installed WorkZone PDF, perform the following steps to verify that the installation is complete.

☑	To be verified	Comments
☐	Ensure that release versions of WorkZone PDF and WorkZone Content Server are equal.	Check release versions in the **Add/Remove Programs** page.
☐	Ensure that WorkZone PDF Engine web service exists.	Open `https://{server}/render` in your browser.
☐	Ensure WorkZone PDF Crawler service is present and is running.	Go to the services list and find `KMD WorkZone PDF Crawler - Instance{Id} -`

☑	To be verified	Comments
		`{DB_name}`.
☐	Test the installation.	See Testing WorkZone PDF.
☐	If your license includes policy usage, ensure that the policy is enabled in WorkZone Configurator.	See Conversion policies.
☐	Check the Event Viewer for any issues regarding WorkZone PDF listed for administrative events.	

WorkZone Process post-installation checklist

When you have installed WorkZone Process, perform the following steps to verify that the installation is complete.

☑	To be verified	Comments
☐	Verify the installation by this overview: Test the installation. • To verify the installation of WorkZone Process, refer to the section "Testing WorkZone Process". • To verify that WorkZone PDF is installed together with each web server, refer to the section "Testing WorkZone PDF".	The tests mentioned in the description in the Test the installation section cover the whole product suite. Perform the tests that are relevant for your installation. In WorkZone 2014 R2 and WorkZone 2016 R2, WorkZone PDF is required for the use of print tasks.
☐	In WorkZone Client, verify that the WorkZone Process add-in is enabled.	
☐	Check the **Event Viewer** for any issues listed for administrative events.	

☑	To be verified	Comments
☐	In WorkZone 2014 R2 and WorkZone 2016 R2, for the use of notifications, verify that the notification services are running.	To verify that the notification services are running, open **Services** on the server environment and verify that the following services are listed with the status **Running** and the status type **Automatic**: • ScanJour Process Mail Notification Agent • ScanJour Process Push Notification Agent • ScanJour Service Process Agent • ScanJour WorkZone Process Asset Update Service
☐	Check the version of the installed application.	Open **ScanJour SQL**, type `select * from version`, and click **Execute**.
☐	Check that the service queue does not contain a status code "2" in order to verify that the mail agent can access the process web service on the web server.	Open **ScanJour SQL**, type `select * from service_queue where agent_type`

☑	To be verified	Comments
		= 'WZP', and click **Execute**.
☐	Check the packages installed	Open **ScanJour SQL**, type `select * from wzp_package`, and click **Execute**.
☐	If you use OAuth authorization, check that **Anonymous Authentication** is enabled for the Process site in IIS Manager.	

Test the installation

When you upgrade or install WorkZone, it is recommended that you perform a minimal installation test to verify the installation.

The tests below cover the full WorkZone product suite. Perform the tests that are relevant for your installation.

Prerequisite:

- Perform this test on a client or reference PC.
- Use a test user who is a member of an organizational unit in WorkZone, and who is a member of a security group which has access rights to creating documents.

Testing web services

To test web services, follow this procedure:

1. Call the OData service with the url `http(s)://[hostname]/OData`.
2. Call the Office service with the url `http(s)://[host-name]/Office/CaseService.svc`.
3. Call the Process service with the url `http(s)://[host-name]/Process/Process.svc`.

Testing WorkZone Client

To test WorkZone Client, follow this procedure:

1. Open WorkZone Client with the url `http(s):[hostname]/app/client/`.
2. Open the user's desktop case.
3. Add a new party to the case.
4. Remove the party.
5. In the Ribbon, open **Settings** and select WorkZone Client as the standard client.

Testing WorkZone for Office

To test WorkZone for Office, follow this procedure:

1. Create a Word document.
2. Save the document in state UÅ (Draft) on the user's desktop case: Click **Select Case** > **Without Case**.
3. On the Registration Pane, click the case link and verify that the document opens in WorkZone Client.
4. Close Word.
5. Open Microsoft Outlook and view the document in Outlook Overview.
6. In WorkZone Client, delete the document.
7. Open Microsoft Outlook, select an email, and click **Save element**.
8. On the list of most recently used items, select the desktop case.

9. Verify that the **Save Outlook item** dialog box opens.
10. Click **Cancel**.

Testing WorkZone Explorer

- WorkZone PDF must be installed.
- To verify the existence of a PDF version, the PDF policy (DVS_policy) must be running.

To test WorkZone Explorer, follow this procedure:

1. From Internet Explorer, open WorkZone Explorer with the url `http://[hostname]/Explorer`.
2. Click **Browse using File Explorer**.
3. Open Windows Explorer, navigate to the folder **Open cases**, and find the user called "Desktop case".
4. Copy a document to the desktop case.
5. Verify that a PDF version of the document is created in the **PDF** folder.
6. Click the shortcut icon of the case to open the case in WorkZone Client.
7. In WorkZone Client, delete the document.

Testing WorkZone PDF

1. In WorkZone Client, open the detail page of a document.
2. Click  **Preview**. The PDF version must be displayed in the preview pane.
3. Open the detail page of a document that does not have a generated PDF version yet.
4. Click  **Create PDF**. The PDF version of the document must be created.

Testing WorkZone Mobile

1. Open WorkZone Mobile application.
2. Log in.

Testing WorkZone Process

To test WorkZone Process, follow this procedure:

1. In Outlook, save an e-mail on the user's desktop case.
2. From the e-mail, create a hearing process.
3. Select the test user as an actor, and start the process.
4. Verify that the test user receives a smartmail.
5. Open the smartmail and click **Respond**.
6. Verify that the test user receives another smartmail.
7. Open the smartmail and click **Complete**.
8. Open the **Processes** overview and verify that the process is there.
9. Open the case and verify that it contains a process history document.

Testing URL rewrite

To test url rewrite, follow this procedure:

1. Open the url that was used for WorkZone Client BEFORE the upgrade.
2. Open the NEW url `http(s)://[hostname]/app/client` and verify that WorkZone Client opens correctly.
3. Open the url that was used for WorkZone Explorer BEFORE the upgrade (`http(s)://[old webdav host]`).
4. Verify that you are redirected to `http(s)://[hostname]/Explorer/`.

5. Open the url that was used for OData BEFORE the upgrade (`http(s)://[old host]/[dsn]/web-services/Scanjour.Services.OData.web/OData.svc`).
6. Verify that you are redirected to `http(s)://[hostname]/OData/`.

Testing WorkZone Configurator

When you upgrade or install WorkZone Configurator, it is recommended that you perform a minimal installation test to verify the installation.

To test WorkZone Configurator, follow this procedure:

> **Tip:** If WorkZone Client is not installed yet, skip steps 4-5.

1. Open WorkZone Configurator with the URL

   ```
   https:<hostname>/app/configurator
   ```

   .
2. Go to **Case** > **Custom fields**.
3. On the **Primary** tab, add a new custom field.
4. Open WorkZone Client with the URL

   ```
   https:<hostname>/app/client.
   ```
5. In the distribution mode, add the new custom field to the web interface.
6. Go back to the WorkZone Configurator and remove the new custom field.

Upgrade

In this section you can read how to upgrade WorkZone products from older to newer versions. General rule is to uninstall the old version and to install the new version. However, some of the products might have additional requirements depending on a version.

Upgrade WorkZone Content Server

If you want to install WorkZone Content Server on a server where an earlier release of WorkZone Content Server is already installed, you need to uninstall the earlier version before starting the installation of the new release.

The reason for this is that the earlier releases may contain customer specific adaptations, which have overwritten standard files.

When you have uninstalled the earlier release, check the following:

- The web server
- WorkZone Content Server components
- The database configuration and ODBC
- Windows registry containing WorkZone Content Server components, Oracle and ODBC.

Upgrade WorkZone Content Server

The procedure of upgrading a version of WorkZone Content Server is identical to the installation procedure described in About installing WorkZone Content Server and Configure WorkZone Content Server

> Important: If you upgrade your WorkZone Content Server 2021.0 or WorkZone Content Server 2021.1 installation to WorkZone Content Server 2022.0, the meta data for the **File**, **Record**, **Contact**, and **Address** tables must reindexed. Reindexing the meta data for the **Document** table is not necessary.

Upgrade a WorkZone database

This procedure describes how you manually upgrade a WorkZone database.

> **Important:** Before you upgrade, you must stop all ScanJour services, including the Internet Information Service (IIS) for the WorkZone Client.

> **Prerequisite:**
>
> - You must log on as sjsysadm, to upgrade an existing database.

If you are upgrading a WorkZone 2021.3 or newer database, the upgrade process is completed in one step, using the **WZsql.exe** database tool.

If you are upgrading a WorkZone 2021.2 or older database, the upgrade process is split into two sequential steps:

1. Upgrade the database to WorkZone 2021.3 using the **Scansql.exe** database tool.
2. Upgrade the 2021.3 database to your current version using the **WZsql.exe** database tool.

> **Note:** If the sjsysadm user in the WorkZone database you are upgrading from does not contain sufficient privileges, you must log on to the database as the Sys user and re-create the sjsysadm user and password. The re-creation process will automatically assign the necessary privileges to the sjsysadm user.
>
> See steps 4 and 5 in the **Upgrade a WorkZone 2021.3 or newer database** below.

Upgrade a WorkZone 2021.2 or older database

If you are upgrading a database from WorkZone 2021.2 or older, you must first use the **Scansql.exe** database tool to upgrade the database to WorkZone 2021.3 and then use the

WZSql database tool to upgrade the new 2021.3 database to your current WorkZone version.

This procedure describes the first upgrade step which upgrades the database to 2021.3. See below for the next step upgrading a 2021.3 database to your current WorkZone version.

1. Locate and start the **scansql.exe** program in Program Files (x86) > KMD > WorkZone > Program to open the **ScanJour SQL** application and display the **Connections** form.
2. In the **Connections** form, select the relevant combination of DSN and UID, and click **OK** to display the **Oracle ODBC Driver Connect** dialog with the selected DSN displayed in the **Service Name** field.
3. In the **Oracle ODBC Driver Connect** form:
    1. In the **User Name** field, enter sjsysadm
    2. In the **Password** field, enter the password for the sjsysadm user.
4. Click **OK** to close the **Oracle ODBC Driver Connect** dialog and access the **ScanJour SQL** application. The database name and user name is displayed in the title bar of the **ScanJour SQL** application.
5. In the **ScanJour SQL** application, select **Sjbase** > **Installation/Upgrading**.
6. The **Scansql** dialog opens with the text "*User SJSYSADM allready exist, do you wish to grant access to sys objects?*"
7. Click **Yes** to open the Password SJSYSADM dialog, enter the password for the SJSYSADM user and click **Save** to open **the Database upgrading** form.
   See The database upgrading form for further information.
8. Select the relevant options in **Database upgrading** form.
9. Under **Execution level**, select the **sjbasecall.bat** script to use for the installation. By default the script is located in `<SCAN_HOME>\program\dbsetup\script`. The default path to the script is displayed in the field. If you have placed the script somewhere else, use the **Browse** button to locate and select the script.
10. The database upgrade process will open a command prompt and start executing the program. The **ScanJour Database window** dialog is displayed, requesting confirmation before the database upgrade can start.
11. In the **ScanJour Database window** dialog, click **Yes** to start the database upgrade.
    Note the upgrade process may take some time.

12. If the program cannot automatically map all logical tablespaces to physical tablespaces, the **ScanJour table spaces** form will be displayed.
    1. In the **ScanJour table spaces** form:
        1. Ensure all logical tablespaces are mapped to the relevant physical tablespaces and map those that are not mapped correctly.
        2. Click **Save** to continue the upgrading process.
13. When the upgrade has finished, upgrade information is displayed in the **obs.txt – Notepad** window.
    If necessary, take appropriate action to the information in the **obs.txt – Notepad** window.
14. Close the **obs.txt – Notepad**window to display The **Scansql** application.
15. The **Scansql** application indicates that the database upgrade has finished.
    The database upgrade process generates log files containing information on the upgrade process. The log files can be accessed in the folder with the same name as the database, located in <SCAN_HOME>\program\dbsetup\log\.
16. Click **OK** to close the **Scansql** application.
17. Perform the procedure described in Install the WorkZone Content Server database

When you have completed the first part of the database upgrade, you must upgrade the database from your new 2021.3 database to your current .WorkZone version.

Upgrade a WorkZone 2021.3 or newer database

If you are upgrading a database from WorkZone 2021.3 or newer, you must use the **WZsql.exe** database tool to upgrade the database to your current WorkZone version.

1. Start the `wzsql.exe` program on the server where WorkZone Content Server is installed. **WZsql** form is displayed with the **Odbc connect** form on top.

2. In the **Odbc connect** form:
    1. **Data Source name** field: Select the relevant database in the **Data Source Name** (DSN) column.
    2. **User name** field: The name of a database system administrator with sufficient rights to upgrade the database
    3. **Password** field: The password of the system administrator defined in the **User name** field above.
3. Click **OK** to log on access and display the **WZsql** form. The title of the **WZsql** form now displays your user name and database name.
4. In the **WZsql** form, click **Sjbase** > **Install/Upgrade db** to open the **Create a privilege to Sjsysadm** form.
5. In the **Create a privilege to Sjsysadm** form:
    1. Click **Select version.txt** to navigate to and select the **version.txt** field for the database to be upgraded.
    2. In both **Password sjsysadm** fields, enter the password of the system administrator defined in the step previously
6. Click **Save** to save the defined credentials and close the **Create a privilege to Sjsysadm** form.
7. In the **WZsql** form, click **Sjbase** > **Install/Upgrade db** to open the **Database update from version...** form.
8. In the **Database update from version...** form, click **Select version.txt** to navigate to and select the **version.txt** file for the database to be upgraded.
9. Click the **Install/Upgrade** button to start the database upgrade.
10. When the database upgrade is complete, remember to restart Internet Information Services (IIS), see below

See Also

Tablespaces in WorkZone Content Server

The database upgrading form

Using Oracle proxy users

Upgrade WorkZone for Office server

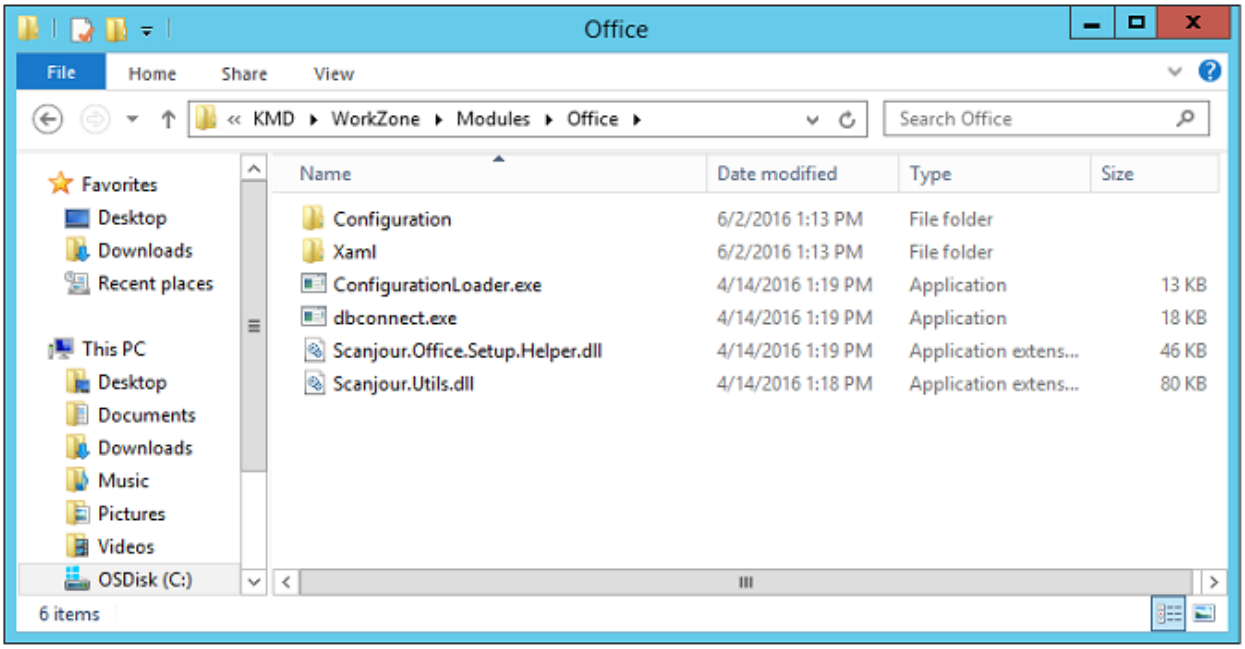
Upgrade

> **Prerequisite:** Before you upgrade the WorkZone for Office server, it is recommended you remove from the database the data installed as a part of the current installation.

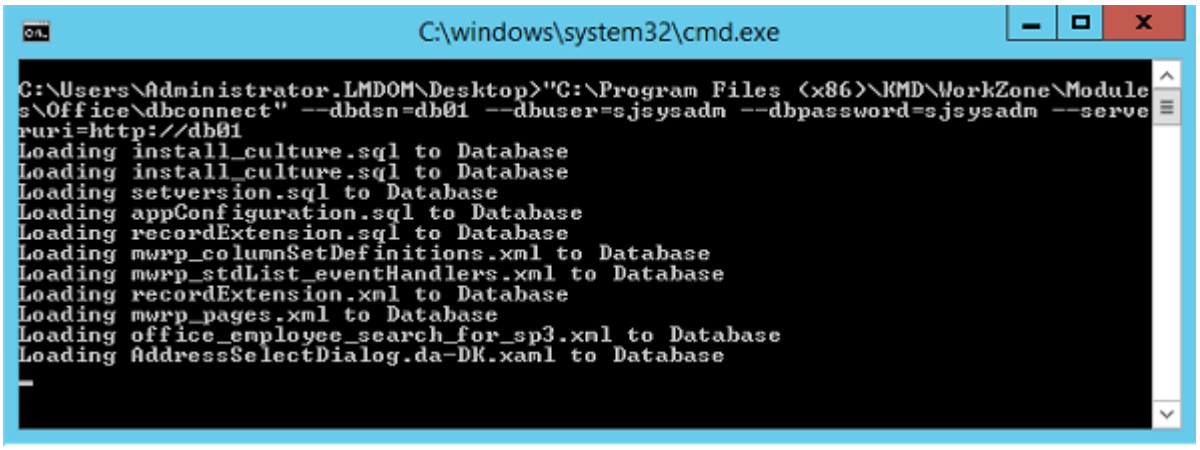
1. Run `dbconnect.exe` with the `/u` option to remove previously installed data from the database.
2. Uninstall the old WorkZone for Office server package from **Programs and Features**.
3. Install the new WorkZone for Office server package.
4. Run `dbconnect.exe` without the `/u` option to update the database.

Update the database

The Office Server installer installs all configuration files and tools into the file system under `C:\Program Files (x86)\KMD\WorkZone\Modules\Office`.



When you have completed the installation, you can load the configuration into the database via the `dbconnect.exe` command line tool. It is located in the Office folder.



`dbconnect.exe` is a command line tool which enables you to load and unload database configuration files, SQL scripts, and XAMLs (dialog boxes).

This tool has the following options:

- `/dbdsn=<dsn>` - The name of the database to be updated (required).
- `/dbuser=<user>` - The name of the database user (required).
- `/dbpassword=<password>` - The password of the database user.
- `/serveruri=<protocol>://<hostname>` - Protocol and hostname for the oData service.
- `/u` - Unloads installed data from the database (optional).
- `/log=<path>` - Writes log to the file at the specified address (optional).

Example:

```
c:\Program Files (x86)\KMD\WorkZone\Modules\Office\dbconnect.exe /dbdsn=demo /dbuser=sjsysadm /dbpassword=xyzz /serveruri=https://demo.captialive.com /u
```

Note: `dbconnect.exe` updates only one database at a time. If you want to update multiple databases, run it several times with a different `/dbdsn` option.

> **Important:** Restart IIS (Internet Information Services) for the configuration changes to take effect on the server.

Upgrade

> **Prerequisite:** Before you upgrade the WorkZone for Office Server, it is recommended you remove from the database the data installed as a part of the current installation.

1. Run `dbconnect.exe` with the `/u` option to remove previously installed data from the database.
2. Uninstall the old WorkZone for Office Server package from **Programs and Features**.
3. Install the new WorkZone for Office Server package.
4. Run `dbconnect.exe` without the `/u` option to update the database.

Repair

You can restore damaged installation files by repairing the installation. If the database is damaged, you need to rerun `dbconnect.exe` as described in Update the database.

To repair a damaged WorkZone for Office Server installation, do one of the following:

- Right-click the.msi file and then select **Repair**.

  -Or-

- Go to **Programs and Features** and select **Repair.**

Upgrade WorkZone for Office client

Upgrade

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

Repair the installation

You can repair a damaged installation at any given time during the installation. Right-click the.msi file, and then select **Repair**, or go to **Programs and Features**, and select **Repair**.

Change the installation

You can change the installed modules of WorkZone for Office.

1. Right-click the `KMD WorkZone for Office.msi` file, and then select **Change**, or go to **Programs and Features**, and select **Change**.
2. The **KMD WorkZone for Office Setup** wizard is displayed. Click **Next**.
3. From the list of operations, select **Change**.
4. The **Ready to change** page is displayed. Click **Change**.
5. The **Completed Setup Wizard** window is displayed. Click **Finish**.

Upgrade WorkZone Client

To upgrade WorkZone Client from a previous version, follow these steps:

1. Uninstall the previous version of WorkZone Client.
2. Install WorkZone Client 2022.0.

> Important: If you upgrade from a version earlier than WorkZone Client 2016 R2 (3.3), you must:

1. Migrate the user configuration from the previous version to the new version of WorkZone Client. The user configuration is migrated with the url `https://<hostname>/app/client/migrate` after you have completed installation.
2. Clear the browser cache when you access WorkZone Client from a client after upgrading.

Upgrade WorkZone Configurator

To upgrade WorkZone Configurator to a newer version, follow these steps:

1. Uninstall the previous version of WorkZone Configurator.
2. Install a new version.
3. To ensure correct work of WorkZone Configurator, clean cash in your browser.

Upgrade WorkZone Process

To upgrade WorkZone Process you run the WorkZone Process installation procedure for the new version. As part of the installation, the previous version of WorkZone Process will be uninstalled.

See Install WorkZone Process.

When you upgrade WorkZone Process:

- Active feature settings in WorkZone Configurator are kept. See Activate process packages.
- The WorkZone Process configuration and the WorkZone Process version marking in the **Version** table are left unchanged in the WorkZone database. To uninstall the WorkZone Process version entry from the database, see Command line configuration.

Upgrade WorkZone PDF

Upgrade WorkZone PDF

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

Note: We recommend that you stop the PDF Crawler agent manually before the WorkZone PDF upgrade. While the upgrade process stops the agent automatically, the WorkZone upgrade may suddenly interrupt the document conversion and affect it negatively.

Important:

- If you want to upgrade from version 2017 SP2 or earlier, please follow this procedure.
- If you want to upgrade from version 2020.2 or earlier, you must uninstall the old version before installing the new one.

Upgrade WorkZone PDF Engine

Upgrade manually

1. Double-click the `KMD WorkZone PDF.exe` file. On the **Welcome to the KMD WorkZone PDF Installation Wizard** page, click **Next**.
2. On the WorkZone PDF **Products** page, click **WorkZone PDF Engine**.
3. On the **WorkZone PDF Engine** page, click **Update**.
4. On the **End-User License Agreement (EULA)** page, read the license agreement, select the **I accept the terms of this license agreement** check box and then click **Next**.

5. On the **Prerequisites** page, click **Verify** to verify that all prerequisites are present, and then click **Next**.
6. On the **Existing WorkZone PDF Engine Instances** page, select all instances of WorkZone PDF Engine you want to update, and then click **Next**.
7. On the **Ready to update WorkZone PDF Engine** page, click **Update** to upgrade the selected PDF Engine instance.

Upgrade silently

1. Open the **Command prompt** window as administrator.
2. Type the path to the `KMD WorkZone PDF.exe` file.
3. Specify the product name `-engine`.
4. Specify the parameters:

Parameter	Meaning
-u	Upgrade mode.
-apps	Application(s) to be upgraded.

Example:

```
"KMD WorkZone PDF.exe"-engine -u -apps:"Test1\Pdf,
Test2\Pdf"
```

Upgrade WorkZone PDF Crawler

Upgrade manually

1. Double-click the **KMD WorkZone PDF.exe** file. On the **Welcome to the KMD WorkZone PDF Installation Wizard** page, click **Next**.
2. On the WorkZone **Products** page, click **WorkZone PDF Crawler**.
3. On the **WorkZone PDF Crawler** page, click **Update**.

4. On the **License Agreement** page, you must accept the license agreement terms before you can continue the installation. Select the **I accept the terms of this license agreement** check box and then click **Next**.
5. On the **Existing WorkZone PDF Crawler Instances** page, select all instances of WorkZone PDF Crawler you want to upgrade, and then click **Next**.
6. On the **Ready to update WorkZone PDF Crawler** page, click **Update** to upgrade the selected PDF Crawler instances.

Upgrade silently

1. Open the **Command prompt** window as an administrator.
2. Type the path to the KMD WorkZone PDF.exe file.
3. Specify the product name `-crawler`.
4. Specify the parameters:

Parameter	Meaning
-u	Upgrade mode.

-instances	Number(s) of instances separated by comma in "00" format
	
	Example: One instance
	`"-instances:01"`
	
	Example: Multiple instances
	`"-instances:01,02,03"`

Example:

```
"KMD WorkZone PDF.exe" -crawler -u -instances:01
```

Upgrade Database Configuration

There is no upgrade installation option for **Database Configuration**. When upgrading your WorkZone PDF Engine andWorkZone PDF Crawler applications, you must also perform a **Database Configuration**.

> **Note:** When upgrading your database configuration through the KMDWorkZone Wizard, any existing custom parameter settings that have been added or customized for your organizational needs will be maintained. You can define new custom parameter settings during the upgrade and these will overwrite the existing ones.

> **Tip:** Create a backup of your existing custom parameter settings for both WorkZone PDF Engine and WorkZone PDF Crawler applications prior to performing an upgrade so you have a backup of your parameters in case you make an error during the upgrade.

Upgrade WorkZone PDF from version 2017 SP2 or earlier

> **Important:** If you upgrade WorkZone PDF from version 2018 or later, ignore this section and follow a regular update procedure.

WorkZone PDF Engine 2018 and later versions contain an installation process that is different from the previous versions of WorkZone PDF Engine. WorkZone PDF Engine 2018 and later versions also contain an improved method of specifying and maintaining the configuration settings of the WorkZone PDF Engine and WorkZone PDF Crawler.

For these reasons, previous versions of WorkZone PDF cannot be directly upgraded upon installation.

WorkZone PDF Engine 2018 or a later version can still be installed on a server that does not contain previously installed versions of WorkZone PDF.

The four general steps are displayed below.

1. Back up configuration files

This step is optional and is not necessary if you do not want to keep your WorkZone PDF Engine and/or WorkZone PDF Crawler configuration.

If you want to apply your configuration settings to the new installation of WorkZone PDF, you must create a backup copy of the configuration files and then reapply the WorkZone PDF Engine configuration file and/or manually reinstate the WorkZone PDF Crawler parameters after the installation.

> **Note:** WorkZone PDF Crawler policies will not be uninstalled as they are stored in the database and not in the configuration files.

You can create backup copies of the WorkZone PDF Engine and/or WorkZone PDF Crawler.

See Back up the WorkZone PDF Engine configuration file

See Back up the WorkZone PDF Crawler configuration file

2. Uninstall old version

Once you have created a backup of the configuration files, you can uninstall the old version of WorkZone.

You can uninstall WorkZone PDF Crawler first and then WorkZone PDF Engine in any order you want.

> **Note:** You must uninstall the WorkZone PDF from the **Programs and Features** form found in the **Windows Control Panel** because the **Uninstall** option in the WorkZone PDF installation program is converted inaccessible when trying to install a WorkZone PDF 2018 on a machine that already contains a previous version of WorkZone PDF.

3. Install new version

When you have uninstalled the old version, you can install the new version of WorkZone.

See Install WorkZone PDF Engine.

See Install WorkZone PDF Crawler.

4. Restore configuration files

This step is optional if you do not want to restore your old WorkZone PDF Engine and/or reinstate your WorkZone PDF Crawler parameter settings.

After the installation of a new WorkZone PDF version, you can restore the configuration settings from the backup files.

See Restore the WorkZone PDF Engine configuration file.

See Reinstate the WorkZone PDF Crawler parameters.

Back up the WorkZone PDF Engine configuration file

You can create a backup of your WorkZone PDF Engine configuration file in order to be able to restore the configuration settings after the WorkZone PDF Engine has been uninstalled or to restore the configuration settings if the original settings are damaged or are converted inaccessible or unreadable.

When you uninstall the WorkZone PDF Engine, the WorkZone PDF Engine file will be deleted. If you want to use your configuration settings after you have reinstalled WorkZone PDF Engine, you must create a backup of the configuration file before uninstalling WorkZone PDF Engine and then replace the installed configuration file with the backup configuration file after the new installation.

The WorkZone PDF Engine configuration file is called Web.config and is located at C:\Program Files (x86)\ KMD\ WorkZone\ IIS\ WorkZone\ Render

Create a backup of your WorkZone PDF Engine Web.config file

1. Stop the WorkZone PDF Engine service in the **Services** form.
2. Copy the Web.config file to another folder on the server.
   Make sure the new folder containing the copy of the Web.config file will not be affected when you uninstall the WorkZone PDF Engine.

Restore the WorkZone PDF Engine configuration file

If you have created a backup copy of your WorkZone PDF Engine configuration file (the PDF Engine Web.Config file), you can restore your configuration settings for example after hav-

ing installed a new WorkZone PDF Engine or if your current configuration file is damaged, unreadable or needs replacing.

To restore some or all of the parameters in the backup copy of your PDF Engine configuration file, manually enter the parameter values from the backup copy in the WorkZone Configurator or manually through the WorkZone PDF Engine installation wizard.

> Important: Do not replace the existing PDF Engine Web.config file with the backup copy of your old PDF Engine web.config file as compatibility issues may arise.

Back up the WorkZone PDF Crawler configuration file

You can create a backup of your WorkZone PDF Crawler configuration file in order to be able to restore the configuration settings after the WorkZone PDF Crawler has been uninstalled or to restore the configuration settings if the original settings are damaged or are converted inaccessible or unreadable.

When you uninstall the WorkZone PDF Crawler, the WorkZone PDF Crawler configuration file will be deleted.

The WorkZone PDF Crawler configuration file is called **WZPDFagentCOM.exe.config** and is located at C:\Program Files (x86)\KMD\workzone\Program\WorkZone PDF Crawler - <instance id> - <dbname>\

Create a backup of the WZPDFagentCOM.exe.config file

To create a backup copy of the WorkZone PDF Crawler configuration, copy the **WZPDFagentCOM.exe.config** file to another folder on the server.
Make sure that the new folder containing the copy of the WZPDFagentCOM.exe.config file will not be affected when you uninstall the WorkZone PDF Crawler.

Reinstate the WorkZone PDF Crawler parameters

If you have created a backup copy of your WorkZone PDF Crawler configuration file, you can reinstate your configuration settings after you have installed the WorkZone PDF Crawler from WorkZone 2018.1.

WorkZone 2018.1 does not contain a configuration file for WorkZone PDF Crawler and you must manually enter the parameter values from the backup copy of the WorkZone PDF Crawler configuration file in the WorkZone Configurator.

Upgrade WorkZone Mass Dispatch

WorkZone products, WorkZone Mass Dispatch must be upgraded as a Windows service manually. To do this, we recommend using **SC tool**.

To upgrade WorkZone Mass Dispatch, see How to create a Windows service by using Sc.exe and Sc config.

Install and set up URL Rewrite

If you are operating on a WorkZone installation that contains HTTP references after having converted the installation to run in an HTTPS environment, you can install and configure the URL Rewrite extension to the Microsoft Internet Information Server (IIS).

The URL Rewrite extension enables you to replace the HTTP protocol part of a URL with its HTTPS equivalents – for example changing SmartTask references in WorkZone Client still containing HTTP to their HTTPS equivalents without having to locate and update all links and references.

The URL Rewrite detects the URL request containing the HTTP request and rewrites the URL, replacing the HTTP protocol part of the URL with HTTPS before it is processed by the WorkZone server.

This is a bit different than a URL redirect operation as a URL redirect operation sends information back to the client requesting an incorrect URL (or at least the URL which is to be redirected). The information enables the client to then request the correct URL and display the results. A redirect is a client-side request that redirects the web browser to access another predefined URL.

A URL rewrite is processed on the server and “rewrites” or updates the requested URL to another predefined URL. The requesting client does not receive any information regarding the new URL from the server. The only indication that the new URL is used is the new URL displayed in the address bar. A URL rewrite is a server-side edit of a URL before it is processed by the IIS.

Note:

- Disable URL rewriting of requests generated through the WZ Client, Internet Proxy, the firewall and the Net Load Balancer.
- Clear the cache of the client machine's web browser to remove any URL Rewrite rules from the cache.

Download and install the URL Rewrite extension

The URL Rewrite extension is not installed by default on IIS servers and must be downloaded and installed separately.

Download and run the **rewrite_amd64_en-US.msi** installer from the Microsoft homepage to install the URL Rewrite extension.

To check if the URL Rewrite extension has been correctly installed, open the **Internet Information Services (IIS) Manager** form for the WorkZone site. The **URL Rewrite** extension is displayed in the **IIS** section on the information (right) pane for the WorkZone site.

If the **Internet Information Services (IIS) Manager** form was open during the installation, the URL Rewrite extension may not be displayed as the form needs to be updated.

Close and reload the form to display the **URL Rewrite** extension for the WorkZone site. In some cases, you may have to reboot the IIS server for the changes to take effect.

Set up URL Rewrite

After the **URL Rewrite** extension is installed, you must clear the **Require SSL** check box to accept HTTP calls for the WorkZone site.

In the **Internet Information Services (IIS) Manager** form, WorkZone site, click **SSL Settings** in the **IIS** section on the information (right) pane for the WorkZone site and clear the **Require SSL** check box.

If the **Require SSL** check box is selected, any URL requests containing HTTP will be rejected before the **URL Rewrite** extension can access the HTTP request to rewrite the request.

Create, edit, enable and disable URL Rewrite rules

Once you have correctly set up the URL Rewrite settings, you can create new URL rewrite rules.

> **Tip:** Remember to create a backup copy of the web.config file before creating new URL rewrite rules through the IIS Manager.

In the **Internet Information Services (IIS) Manager** form, WorkZone site, double-click **URL Rewrite** in the **IIS** section on the information (right) pane for the WorkZone site to open the **URL Rewrite** panel.

In the **URL Rewrite** pane, you can add new URL rewrite rules, edit existing rules, enable and disable rules as well as test the URL rewrite rules.

Each rule must be created manually. You cannot import or export rules in the **URL Rewrite** pane.

The IIS settings are stored in the web.config file for the selected site. If you need to mass-create or mass-update URL rewrite rules, you can edit the web.config file instead, copy-pasting the relevant lines to and from web.config files.

All URL rewrite rules in the web-config file are displayed in the **URL Rewrite** panel.

Use the Web.config file to create URL rewrite rules

You can use the web.config file on the IIS server to manually create and edit URL rewrite rules. The web.config file is an XML-based configuration file used by IIS to manage various settings used to configure a website hosted on IIS. The web.config file can be edited in any text-editor and in this way you can control a website's configuration without editing the server's configuration.

The default path to the web.config file is C:\Program Files (x86)\KMD\WorkZone\IIS\WorkZone.

> **Tip:** Remember to create a backup copy of the web.config file before manually editing the file.

To create URL rewrite rules in a web-config file, you must add the following rules:

```
<rule name="httpsRedirect" enabled="true" stopProcessing="true">
    <match url="(.*)" />
    <conditions>
        <add input="{HTTPS}" pattern="^OFF$" />
    </conditions>
    <action type="Redirect" url="https://{HTTP_HOST}{REQUEST_URI}" appendQueryString="false" redirectType="Temporary" />
</rule>
<rule name="assetRootRedirect" enabled="true" stopProcessing="true">
    <match url="(.*)" />
    <conditions trackAllCaptures="true">
        <add input="{HTTPS}" pattern="^ON$" />
        <add input="{QUERY_STRING}" pattern="^(.*)assetRoot=http://(.*)$" />
        <add input="{QUERY_STRING}" pattern="^.*assetRoot=https://.*$" negate="true" />
    </conditions>
    <action type="Redirect" url="https://{HTTP_HOST}{URL}?{C:1}assetRoot=https://{C:2}" appendQueryString="false" redirectType="Temporary" />
</rule>
```

The `httpsRedirect` rule rewrites the first part of the URL to HTTPS while the `assetRootRedirect` rewrites the internal HTTP URL. For example for WorkZone SmartMail which employs an imbedded URL in the URL.

See also:

URL Rewrite (External link to IIS.net)

Uninstall

In this section you can read how to uninstall WorkZone products.

Uninstall WorkZone Content Server

The procedure below describes how to uninstall WorkZone Content Server. The installation program will prompt you to uninstall.

Before you uninstall WorkZone Content Server, you must uninstall the services that are installed from the WorkZone Configuration Management.

For more information, see Uninstall services in the WorkZone Content Server service framework

> Important:
>
> - If the purpose of uninstalling is to remove WorkZone Content Server permanently, you must uninstall the services in WorkZone Configuration Management first.
> - If the purpose is to upgrade WorkZone Content Server do not uninstall the services, but remember to stop them before upgrading the database.
>   For more information, see the Content Server Database

Uninstall WorkZone Content Server using **Programs and Features** in the **Control Panel**.

Remove the third party programs

The third party programs are not removed when you uninstall WorkZone Content Server. Log files and certain ini-files are retained as well, and you must delete them manually, if needed. You can remove third party programs from the **Programs and Features** in the **Control Panel**.

Uninstall WorkZone Configurator

To uninstall WorkZone Configurator, go to **Programs and Features** in the Windows Control Panel, right-click **KMD WorkZone Configurator**, and select **Uninstall**. In the **KMD WorkZone Setup** wizard, click **Remove**.

If you have WorkZone Configurator installed on several databases, you must uninstall all instances of WorkZone Configurator.

For the load balancing reason, WorkZone Configurator can be installed on several web servers that refer to a common database. If you remove a single instance, while other instances continue running, assure that the **Remove from database** check box is cleared. This preserves communication between other WorkZone Configurator instances and the database. Otherwise, WorkZone Configurator instances installed on different web servers will not be accessible.

You should only select the **Remove from database** check box if you want to remove the last WorkZone Configurator instance for the given database.

> Important: Uninstall does not affect the databases. When WorkZone Configurator is uninstalled, all data is preserved.

Uninstall WorkZone Client

> Prerequisite: To uninstall WorkZone Client, you must have administrative rights.

To uninstall WorkZone Client, go to **Programs and Features** in the Windows Control Panel, right-click **KMD WorkZone Client** and select **Uninstall**. In the **KMD WorkZone Client Setup** wizard, click **Remove**.

If you have WorkZone Client installed on several databases, you must uninstall all of instances of WorkZone Client.

For the load balancing reasons, WorkZone Client can be installed on several web servers that refer to a common database. If you remove a single instance, while other instances continue

running, you must clear the **Remove from database** check box. This preserves communication between other WorkZone Client instances and the database. Otherwise, WorkZone Client instances installed on different web servers will not be accessible.

Select the **Remove from database** check box only if you remove the last WorkZone Client instance for the given database.

> Important: Uninstalling does not affect the databases. When WorkZone Client is uninstalled, all data (cases, documents, contacts, and so on) is still preserved.

Uninstall WorkZone 365

Uninstall WorkZone 365 for Microsoft Office 365

See the detailed instruction on how to uninstall WorkZone 365 for Microsoft Office 365 in the following article by Microsoft: Remove an add-in for Outlook.

Uninstall WorkZone 365 for Microsoft Office 2016 and 2019

To uninstall WorkZone 365, proceed with the following steps:

1. Remove manifests from the shared folder.
2. Remove the trusted catalog address.

> Note: You must remove the trusted catalog address by using the same method as you have installed it:
>
> - manually
> - by using group policy, or
> - by using the registry script

See how to remove a trusted catalog address:

1. Open a new document in Word, Excel, or PowerPoint.
2. Go to the **File** tab, and then click **Options**.
3. Click **Trust Center**, and then click **Trust Center Settings**.
4. Click **Trusted App Catalogs**.
5. Select the required trusted catalog address.
6. Click **Remove**, and then click **OK**.

Uninstall WorkZone 365 for Microsoft Outlook 2016 and 2019

See the detailed instruction on how to uninstall WorkZone 365 for Microsoft Outlook 2016 or 2019 in the following article by Microsoft: Delete the add-in.

Uninstall WorkZone for Office

Uninstall WorkZone for Office client

To uninstall WorkZone for Office, right-click the `KMD WorkZone for Office.msi` file, and then select **Uninstall**, or go to **Programs and Features**, and select **Uninstall**. You will be asked to verify the action.

> **Tip:** Reinstall SjDocIntegration after uninstallation of WorkZone for Office, as WorkZone for Office add-ins are not always enabled for all users during uninstallation.

Uninstall WorkZone for Office server

> **Prerequisite:** Before uninstalling WorkZone for Office Server, you need to run `dbconnect.exe` with the `/u` option to unload installed data and customizations from the database.

1. Open **Control Panel** > **Programs and Features**.
2. Select the Office Server application and click **Change** > **Remove**. You will be asked to verify the action.
3. Click **Uninstall**.

> Important: You must always disable or uninstall WorkZone for Office customizations in the configuration (if any) before uninstalling Office Server.

Uninstall WorkZone Meeting

Uninstall WorkZone Meeting client

- Run the `WorkZone Meeting.msi` file and then select **Remove** in the **WorkZone Meeting Setup** wizard.

-Or-

- Open **Programs and Features**, right-click **WorkZone Meeting**, and then select **Remove**.

Uninstall WorkZone Meeting server

1. Open **Control Panel** > **Programs and Features**.
2. Run the WorkZone Meeting **Server** application.
3. On the WorkZone Meeting **Server Setup** page, click **Remove**. You will be asked to provide the database DSN name, user name, and password.
4. Click **Remove**.

Uninstall WorkZone Process

You can use **Remove** (**Add or Remove programs** to uninstall WorkZone Process manually or you can use silent uninstalation.

Command line uninstallation

To uninstall, type the following command:

```
msiexec.exe /uninstall KMD Process Setup.msi /qn /l*v uninstall.log
```

Note: A complete uninstallation leaves both the WorkZone Process configurations and the WorkZone Process version marking in the **Version** table unchanged in the WorkZone database. To uninstall the WorkZone Process version entry from the database, see Command line configuration.

Uninstall WorkZone PDF

There is no **Database Configuration** installation option to uninstall or delete the database configuration. If you need to remove or edit entries in the database, you must do that manually, using normal database operations (Create, Read, Update and/or Delete).

Uninstall WorkZone PDF Engine

You can uninstall one or more instances of the WorkZone PDF Engine either through the **KMDWorkZone PDF Installation Wizard** or by using Microsoft Windows Programs and Features.

Uninstall using Microsoft Windows Programs and Features

1. In Windows **Programs and Features**, right-click WorkZone PDF and click **Change**. The **KMD WorkZone PDF Installation Wizard** is displayed. Click **Next**.
2. On the **WorkZone PDF Products** page, click **WorkZone PDF Engine**.
3. On the **WorkZone PDF Engine** page, click **Uninstall**.
4. On the **Prerequisites** page, click **Verify** to verify that all prerequisites are present and then click **Next**.

5. On the **Existing WorkZone PDF Engine instances** page, select all instances of WorkZone PDF Engine you want to uninstall, for example WorkZone PDF/Render, and then click **Next**.
6. On the **Ready to uninstallWorkZone PDF Engine** page, click **Uninstall** to uninstall the selected PDF Engine instance.

Uninstall using the installation wizard

1. Double-click the `KMD WorkZone PDF.exe` file. On the **Welcome to the KMDWorkZone PDF Installation Wizard** page, click **Next**.
2. On the **WorkZone PDF Products** page, click **WorkZone PDF Engine**.
3. On the **WorkZone PDF Engine** page, click **Uninstall**.
4. On the **Prerequisites** page, click **Verify** to verify that all prerequisites are present and then click **Next**
5. On the **Existing WorkZone PDF Engine instances** page, select all instances of WorkZone PDF Engine you want to uninstall, for example WorkZone PDF/Render, and then click **Next**.
6. On the **Ready to uninstallWorkZone PDF Engine** page, click **Uninstall** to uninstall the selected PDF Engine instance.

Uninstall silently

1. Open the **Command prompt** window as administrator.
2. Type the path to the WorkZone PDF Setup.exe file.
3. Specify the product name `-engine`.
4. Specify the parameter:

Parameter	Meaning
-x	Uninstall mode
-apps	Specify application/applications to be removed

Example:

```
"KMD WorkZone PDF.exe"-engine -x -apps:Test1\Pdf
```

Uninstall WorkZone PDF Crawler

You can uninstall one or more instances of the WorkZone PDF Crawler either through the **KMD WorkZone PDF Installation Wizard** or by using Microsoft Windows Programs and Features.

Tip: When uninstalling the WorkZone PDF Crawler, close all Windows services viewer programs.

Uninstall manually

1. In Windows **Programs and Features**, right-click WorkZone PDF and click **Change**.

   - Or -

   Double-click the **KMD WorkZone PDF.exe** file.

2. On the **Welcome to the KMDWorkZone Installation Wizard** page, click **Next**.
3. On the **WorkZone PDF Products** page, click **WorkZone PDF Crawler**.
4. On the **WorkZone PDF Crawler** page, click **Uninstall**.
5. On the **Existing WorkZone PDF CrawlerInstances** page, select all instances of WorkZone PDF Crawler you want to uninstall, and then click **Next**.
6. On the **Ready to uninstallWorkZone PDF Crawler** page, click **Uninstall** to uninstall the selected PDF Crawler instances.

Uninstall silently

1. Open the **Command prompt** window as an administrator.
2. Type the path to the KMD WorkZone PDF.exe file.
3. Specify the product name `-crawler`.
4. Specify the parameters:

Parameter	Meaning
-x	Uninstall mode.
-instances	Number(s) of instances separated by comma in "00" format **Example:** `"-instances:01", "-instances:01,02,03".`

Example:

```
"KMD WorkZone PDF.exe" -crawler -x -instances:01
```

Uninstall WorkZone Mass Dispatch

In contrast to other WorkZone products, WorkZone Mass Dispatch doesn't have its own installer yet. That is why it must be uninstalled as a Windows service manually. To do this, we recommend using the `sc.exe` utility that is a software component of Microsoft Windows.

Commands to uninstall WorkZone Mass Dispatch

Execute the following commands in Command Prompt.

Stop WorkZone Mass Dispatch Windows service

```
sc.exe stop "<your service name>"
```

> **Example**: sc.exe stop "KMD WZMD service"

Delete WorkZone Mass Dispatch Windows service

```
sc.exe delete "<your service name>"
```

> **Example**: sc.exe delete "KMD WZMD service"

For more information about the `Sc.exe` utility, see the Microsoft links:

How to create a Windows service by using Sc.exe

Sc config

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.