KMD WORKZONE _process

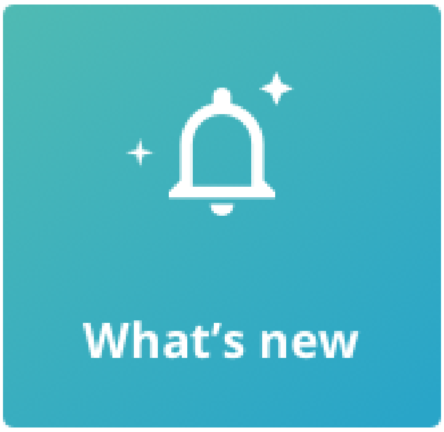
2022.0

Administrator Guide

Contents

Administrator Guide for WorkZone Process 2022.0

This guide describes how to configure WorkZone Process.



Related product documentation

- WorkZone Process User Guide
- WorkZone Process Developer Guide
- Release notes

WorkZone links

- WorkZone support
- WorkZone website
- WorkZone portal

What's new

New features and functionality in WorkZone Process 2022.0

Next generation Digital Post (NgDP)

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 30, 2021.

The WorkZone NgDP integration now also supports the PULL model.

The NgDP documentation has been updated accordingly. See Configure SmartPost to use NgDP in this guide and Install and configure WorkZone e-Boks Push Service in the WorkZone Installation Guide.

If you need help with the implementation of the NgDP integration, KMDWorkZone Consulting offers NgDP relevant services. Please contact your Service Delivery Manager for more information.

Case activities

Graphs are now called processes in the DCR Design Portal. The case activities topics in this guide have been revised according to the name change.

See About case activities .

Service workflow check when started

When a service workflow is started and an identical service workflow is already running or scheduled to start on any WorkZone agent server, the newly started workflow will be canceled in favor of the already running or already scheduled workflow.

Previously, it was possible to start the same service workflow multiple times, for example starting multiple e-Boks Handler service workflows would result in the same e-Boks message being received and saved multiple times.

e-Boks dispatcher ignores incoming messages that already exist

If an already received e-Boks messages is received again, the incoming e-Boks message will be ignored in order to avoid duplicates of identical e-Boks messages in WorkZone.

Previously, duplicates of identical e-Boks messages could occur due to inconsistent checking of incoming messages.

WorkZone Process 2021.3

Next generation Digital Post (NgDP) - Experimental

The WorkZone integration has been adjusted and improved to align with the latest changes to NgDP. A new parameter **NgDpAuthorizationHeader** has been added to the e-Boks dispatcher configuration in WorkZone Configurator and the NgDP documentation has been updated.

See Configure SmartPost to use NgDP.

The integration makes it possible to test NgDP with WorkZone. KMDWorkZone Consulting offers NgDP relevant services. Please contact your Service Delivery Manager for more information.

As the Agency for Digitisation is still developing NgDP, and therefore the WorkZone integration will be continuously adjusted and improved accordingly. The improvements to the integration will be part of coming WorkZone releases.

DCR Processes/Case Activity enhancements

Maximum number of activity loops

If there are more than 50 automatic activities executed in a loop or just sequentially in the DCR process, an error will be triggered at the 51st activity with the error message: *"Maximum number of loop iterations of graph execution reached. Loops or automatic execution flows with more than 50 executions are not allowed."*

This restriction helps prevent endless loops which can result in Case Activity processes remaining locked in the **Running** status.

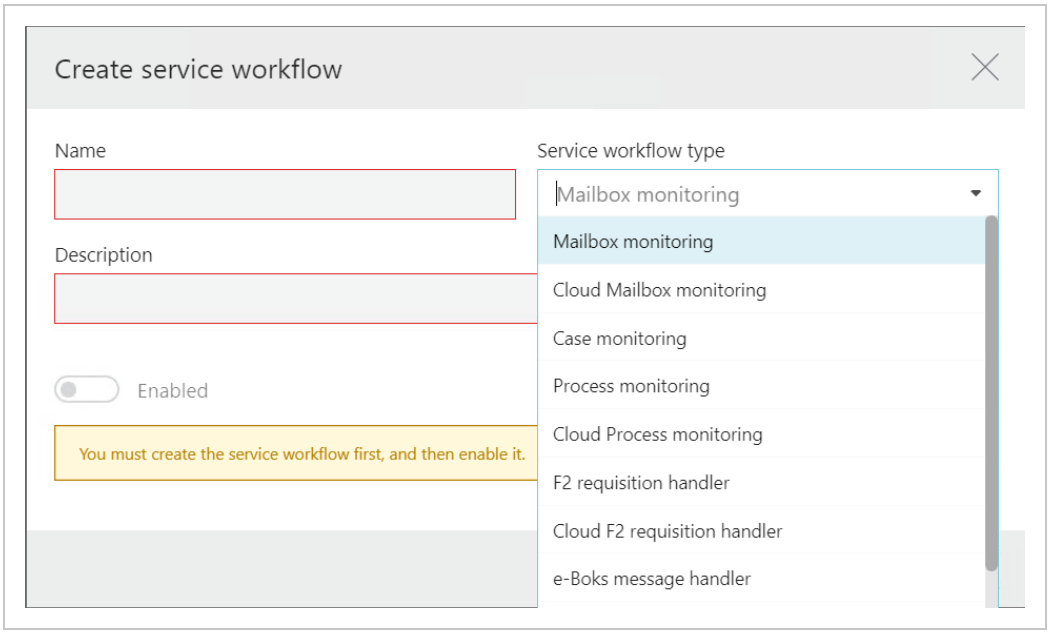
The Running status and idle processes

Whenever an activity is executed, the DCR process status will be changed to **Running**. If a DCR process remains in the **Running** status for more than 5 minutes without signs of active activities, the process will be considered to be idle, which enables users and the WorkZone system to perform operations on the process. A DCR process will be considered idle, even in the case of serious long-present network errors which could result in a Case Activity process not being able to switch back to Persisted status.
Microsoft

Microsoft Graph support for service workflows using Microsoft Exchange Online

The Mailbox monitoring, Process monitoring, and F2 requisition handler service workflows now use Microsoft Graph. With the Microsoft Graph library, the service workflows can be used with Exchange Online. Three new cloud service workflows are now available in WorkZone Configurator:

- Cloud Mailbox monitoring
- Cloud Process monitoring
- Cloud F2 requisition handler



Compared to the on-premises versions of the service workflows, these workflows contain the following new Exchange Online specific parameters:

- ExchangeOAuthClientId
- ExchangeOAuthTenantId
- ExchangePassword
- ExchangeOAuthClientSecret

See:

Configure a Mailbox Monitor service workflow

Process Monitor

Install and configure F2 integration

WorkZone Process 2021.2

Next generation Digital Post (NgDP) - Experimental

WorkZone now supports next generation Digital Post (NgDP) in an experimental version. WorkZone supports sending and receiving through NgDP as a new channel for SmartPost. As this is a regulatory change, this release will be followed by hotfixes to previous WorkZone release where relevant. The new NgDP feature makes it possible to test the new Digital Post with WorkZone. KMD WorkZone Consulting offers NgDP relevant services. Please contact your Service Delivery Manager for more information.

The Agency for Digitisation (Digitaliseringsstyrelsen) is still developing NgDP, and therefore the WorkZone integration will be continuously adjusted and improved accordingly. The improvements to the integration will be part of coming WorkZone releases.

See Configure SmartPost to use NgDP.

WorkZone Process 2021.1

No new features in this release.

WorkZone Process 2021.0

No new features in this release.

WorkZone Process 2020.3

No new features in this release.

WorkZone Process 2020.2

SmartPost

- New parameter **PdfFailIfOutOfBounds**.
- Configuration of e-Boks mailbox mappings to specific units and cases has been moved from WorkZone Configuration Management to WorkZone Configurator. See Map e-Boks mailboxes to cases.

Case monitor service workflow

New prerequisite to install WorkZone PDF Engine on the agent server where the case monitor service workflow runs if the service workflow starts a case activity list that contains SendSmartPost activities.

See Case monitor.

Case activities

Use of . dot notation in Property parameters

You can now also use the dot notation `{Case.<Property>}` introduced in the 2020.1 relase in the **Property** parameter of activities. For example, `{Case.Title}` to retrieve the title of the current case.

See the **UpdateEntities** and **ValidateEntities** activity types.

Interact connector

The **CorporateAccessUser** parameter in the Interact connecter service workflow has been renamed to **ExecutingUser**. It applies to WorkZone environments with and without corporate access. See ExecutingUser.

WorkZone Process 2020.1

SmartPost

Support for Digital Post2

The SmartPoste-Boks dispatcher now supports Digital Post 2. To use SmartPost with e-Boks using Digital Post 2, you need to install WorkZone Processe-Boks Push Service. Two new parameters have been added to the e-Boks dispatcher.

See Edit dispatcher parameters and Install the e-Boks push service in the WorkZone Installation Guide.

e-Boks error code 1000–changed SmartPost action

The SmartPost action to the e-Boks error 1000 has changed from **Retry** to **Notify**.

In case of operational issues at e-Boks, e-Boks returns an error code 1000 (internal server error) to WorkZone. The SmartPost process fails, but in previous releases the error was not reported because the SmartPost action was set to **Retry** by default. With the action set to **Notify** by default:

- The process owner will be notified about the failed dispatch.
- The process will be completed, and the history document will be generated so that you can see the status of each dispatch.

See error 1000.

Mailbox monitor

The sender, recipients, and CC recipients will be added as case parties when new cases are created.

See Mailbox monitor.

Case activities

GetValue activity type

Using the new **GetValue** activity type you can retrieve a value on, for example a case, and use it in guards to make conditions based on WorkZone data.

See GetValue.

SetValue activity type

A new **SetValue** allows you to set a value in a WorkZone property based on a query.

See SetValue.

StartProcess activity type

It is now possible to start processes without parameters automatically using the AUTO or L-AUTO roles.

See StartProcess.

L-AUTO role

A new **L-AUTO** role execute activities as soon as they are included and pending. You can also use the **L-AUTO** role to align the behavior of your WorkZone case activities with the simulation in DCR Portal using the lazy user role.

See Execute activities automatically.

Quick execution of activities

Activities can now be executed without opening dialog boxes. On all activity types, you can select an **EnableQuickExecution** option, which will display a check box next to the activity in WorkZone Client. When a user selects the check box, the activity is executed immediately without opening a dialog box.

See Enable quick execution of activities.

Changed notations

The notation for current case that you can use in queries has changed from `{CurrentFileKey}` to `{Case.ID}`. You can still use the `{CurrentFileKey}` notation.

Similarly, you can now use the notation `{Case.<Property>}` to retrieve values of specific properties on the current case in queries. For example, `{Case.Officer_Value}` to retrieve the case handler or `{Case.State_Value}` to retrieve the state of the current case.

The examples in this guide have been revised to use the new notation. See Activity types.

Interact

Document mappings are applied to system generated documents

If you have mapped meta data on documents, this mapping will also apply to the system generated PDF and XML documents. If you have not mapped any meta data to documents, the default values will be used.

See WorkZone actions.

WorkZone Process 2020.0

Interact connector

Improved error handling

If retrieval of data from an Interact form fails, a case that contains the error message and information about the form is created automatically. To get an overview of errors, you can create a search that extracts the error cases, save the search, and show search results in a list in the navigation pane in WorkZone Client.

See View Interact connector errors.

Case activities

Deadlines and delays

WorkZone now supports setting deadlines and delays on activities in a DCR process, which means that you can create processes that can execute activities automatically after a specific amount of time has passed or a deadline is reached.

See Apply deadlines and delays to activities.

Validation interval

You can configure the **ValidateEntities** activity type to be executed automatically at a specific interval using a new **ValidationInterval** parameter. Use this parameter if you await specific information to be available on a case before the next activity can be executed. For example, a receipt for payment must be saved on the case before the case handling can continue.

See ValidateEntities.

Send SmartPost activity type - new parameter

A new **ProcessOwner** parameter has been added. It specifies the process owner of the SmartPost process.

See SendSmartPost.

AUTO role

Activities with the **AUTO** role assigned are now executed by a system user.

See Execute activities automatically.

Mailbox Monitor service workflow

The Mailbox Monitor service workflow has been optimized to monitor multiple mailboxes in a service workflow.

See Mailbox monitor.

Miscellaneous enhancements

Extended submission–new **NotificationsDefaultActions** parameter

New **NotificationsDefaultActions** parameter for configuring default actions that will be selected on the **Notifications** tab in the **Start Submission (Extended) dialog box**.

See Configure extended submission.

Processes Overview settings have been removed

The **Processes overview** parameters under **Process settings** in WorkZone Configurator have been removed. The new **Processes Overview** introduced with this release does not require these parameters.

See What's new in the WorkZone Process User Guide.

New SmartPost parameter

A new **AllowOfficeRemerge** parameter has been added. If content controls have already been merged in Word, the content controls will be merged again when sending the message through SmartPost.

See Configure SmartPost.

WorkZone Process 2019.3

Notifications

You can now configure which notifications users should receive by specifying settings in WorkZone Configurator. In previous releases, you had to configure the notification settings in the database. This is no longer needed.

Users can also turn notifications on/off in WorkZone Client. In this case, the settings in WorkZone Configurator are overridden.

See Configure notifications.

SmartPost

Suggested process title

A new **SuggestedTitle** parameter allows you to specify a process title that will be prefilled in the **Start process** dialog box when users start standard processes. You can apply suggested titles to the Hearing (Basis), Submission (Basis), Submission (Extended), and Distribution (Extended) processes.

See Configure a process title.

Doc2Mail is renamed to OneTooX

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

Case activities

Extended SendSmartPost activity type

New parameters have been added to **SendSmartPost** activity type. You can now specify copy recipients and attachments to the SmartPost process using the new **CopyRecipients** and **Attachments** parameters.

A new **ProcessGuid** allows you to specify which SmartPost to start if your company uses several SmartPost processes.

See the Send SmartPost activity type parameters in the Activity types topic.

New CompleteGraph activity type

Using the new **CompleteGraph** activity type you can design when to allow users to complete an activity list even if some activities have not been executed.

See CompleteGraph.

Interact connector

- In the Interact connector service workflow, the **FormIds** parameter has been extended so that you can specify multiple form IDs. If no form ID is specified, data from all forms will be fetched.

  See Create and configure an Interact connector service workflow.

- The XML document which contains content and additional meta data about submitted data from Interact is now added as a supplementary document to the PDF document. Previously, it was added as a document on the case.

  See WorkZone actions.

WorkZone Process 2019.2

Installation

You can now find information about installing WorkZone Process in a common WorkZone Installation Guide that covers installation of all WorkZone products.

See WorkZone Installation Guide.

SmartPost

Send attachments as separate documents

Users can now send attachments as separate PDF documents in messages sent to e-Boks. For this purpose, three new parameters have been added to the SmartPost process parameters:

- **AllowSendingSeparateDocuments** allows users to send attachments as separate PDF documents in messages to e-Boks.
- **DefaultSendSeparateDocuments** turns on **AllowSendingSeparateDocuments** by default.

- **MergeAllDocument** allows you to configure if you want to merge the letter and its attachments into one PDF document or if you only want the PDF document to contain the letter. Attachments will still be sent as separate PDF documents.

See the AllowSendingSeparateDocuments, DefaultSendSeparateDocuments and the MergeAllDocuments parameters.

Save received messages sent to subunits on specific cases

It is now possible to receive unsolicited messages from e-Boks that are sent to subunits of an organization. The received messages are then automatically saved on the specific cases that are mapped to the subunits.

See Handle e-Boks messages sent to subunits.

Validation of the contact hierarchy

Two new parameters ValidationHour and ValidateAtStartup have been added. They allow you to schedule when to validate if the contact hierarchy e-Boks Administrationsportal matches the mapping of e-Boks mailboxes and cases in WorkZone.

See Configure validation of a contact hierarchy.

Case activities

New SendSmartPost activity type

The **SendSmartPost** activity type starts a SmartPost process automatically. Currently, the **SendSmartPost** activity type only includes basic functionality such as sending a letter to recipients.

See Activity types.

WorkZone Process 2019.1

SmartPost

SecurityProtocol parameter

The SmartPost process now complies with Microsoft best practice for security protocols. This means that you no longer need to configure a security protocol for e-Boks and Strålfors dispatchers. As a result, the **SecurityProtocol** parameter has been removed from the e-Boks and Strålfors dispatcher configuration in WorkZone Configurator. See Configure digital mail, Configure remote print, and Configure dispatchers.

If you upgrade from a previous release, the new version of the e-Boks and Strålfors dispatchers will not contain the **SecurityProtocol** parameter.

For more information about Microsoft best practices, see the article Transport Layer Security (TLS) best practices with the .NET Framework.

Support for GDPR

It is now possible to define allowed classification levels of documents that SmartPost can send. You can define a maximum document classification rank that the SmartPost process will allow. It means that users will only be able to select documents with document classification ranks lower or equal to the configured threshold.

See Configure SmartPost and GDPR classification.

HistoryDocRetryPeriod parameter

A new parameter named **HistoryDocRetryPeriod** has been added. It allows you to configure the period of time that WorkZone will retry to generate a history document in case of failure. You can configure this parameter for all processes that generates history documents, such as the Submission (basis), Submission (Extended), Hearing (Basis), and Distribution (Extended) processes.

See Configure the retry period for history document creation.

Push notification certificate for WorkZone Mobile for Intune

A new certificate, **Apple Push Services: dk.kmd.workzone.intune**, used for sending push notifications from WorkZone Process to WorkZone Mobile for Intune is now installed to the certificate store. To use this certificate, you need to change the Scanjour.Process.Notification.AgentHost.exe.config file. See Configure push notification certificates for WorkZone Mobile.

Interact integration

The actions that WorkZone can perform based on data retrieved from Interact forms have been extended. The Interact connector service workflow can now:

- Add data from custom fields to a case.
- Add existing contacts as parties on a case.
- Update existing cases.

See WorkZone actions.

Case activities

A new version of the WorkZone Case Activity Template is available in DCR Portal. The template has been extended with an **AUTO** role and a new **UpdateEntities** and **ValidateEntities** activity types.

AUTO role

To reduce the number of activities that a user needs to perform in a case activity list, you can configure activities to be executed automatically. In previous releases, only the **CopyDocument** activity type could be executed automatically. Now, you can apply a new role named **Auto** to all activity types, which will execute the activity automatically. See Execute activities automatically.

UpdateEntities activity type

A new activity type named **UpdateEntities** will update text fields on a case when an activity is executed. See Activity types.

ValidateEntities activity type

A new activity type named **ValidateEntities** allows you to validate WorkZone data and if the validation is successful, execute subsequent activities. **ValidateEntities** works in connection with guards.

See Activity types.

WorkZone Process 2019.0

Case monitoring service workflow

In this release, you can create and configure case monitoring service workflows using WorkZone Configurator. For more information, see Configure a case monitoring service workflow.

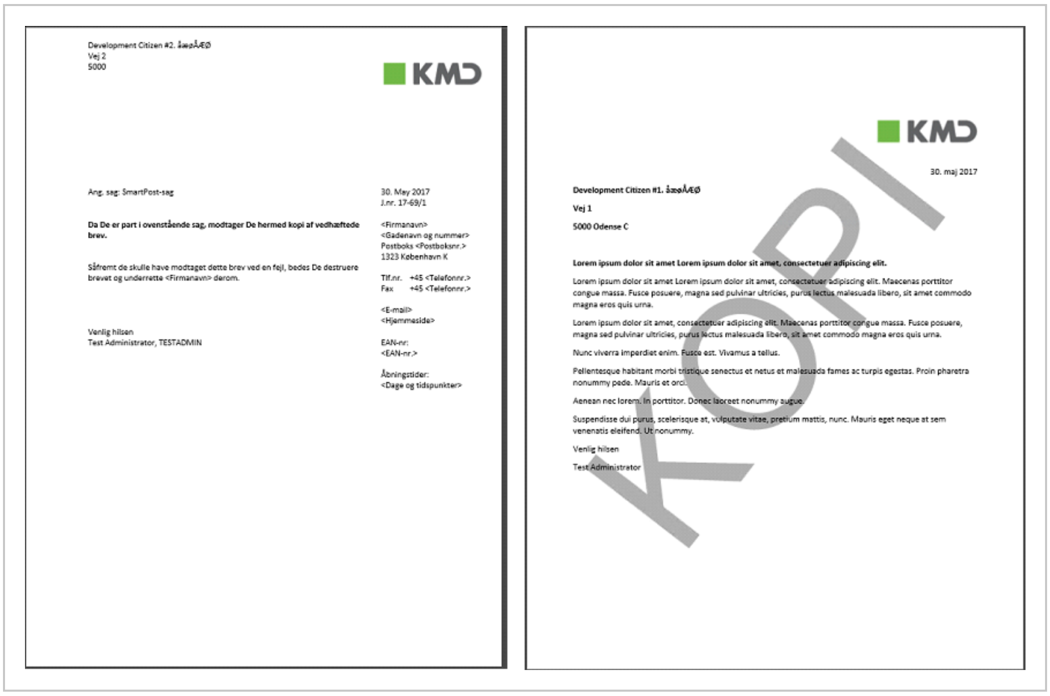
SmartPost

SecurityProtocol parameter

The **SecurityProtocol** parameter that is used when configuring Strålfors and e-Boks dispatchers is now set to **SystemDefault** by default. You no longer need to enter a specific protocol. The value of the **SystemDefault** parameter means that the operating system will negotiate the applied security protocol with the Strålfors and the e-Boks services. See the **SecurityProtocol** parameter description for Strålfors and e-Boks in Configure dispatchers.

Changing the watermark on copies

It is now possible to change the default watermark text KOPI, which is inserted on the document copies that are sent to copy recipients. In the new **CopyWatermark** parameter, you can enter the watermark text.



For more information, see the description of the **CopyWatermark** parameter in Configure SmartPost.

Allowed documents

You can now configure which documents that users are allowed to select as the letter document and attachments in the **Send SmartPost** dialog box. The list of documents shown in the **Letter** and **Attachments** fields is based on configured values from a droplist in a custom field. You configure allowed documents in WorkZone Configurator using two new parameters, **ValidationProperty** and **ValidationValues** in the SmartPost process.

For more information, see Configure allowed documents and Configure SmartPost.

WorkZone Process 2018.2 SP1

SmartPost

A new **RemergePdfEnabled** parameter allows updating the letter date of the PDF document at preview and approval of the SmartPost message before sending the message. See RemergePDFEnabled.

Interact connector service workflow

A new service workflow named **Interact connector** connects to KMD WorkZone Interact, retrieves data from Interact forms, and then creates cases and adds documents in WorkZone based on the data that users have entered in a form. See Interact connector.

Case monitoring service workflow

A new service workflow that monitors newly created cases and then automatically starts a case activity or a customized workflow without mandatory arguments. See Case monitor.

Note: In this release, you can create and configure case monitoring service workflows using WorkZone Configuration Management. As of the coming WorkZone 2019 release, you will be able to configure the service workflow using WorkZone Configurator.

Automatic start of a case activity or workflow when a case is created

A case activity or a workflow can now be started automatically when a new case is created. A case monitoring service workflow monitors when new cases are created, and if the new cases fulfill a specific set of rules, it starts a case activity or a workflow automatically.

For more information about setting up a Case monitoring service workflow, see Case monitor.

Updates and cancellations of F2 requisitions

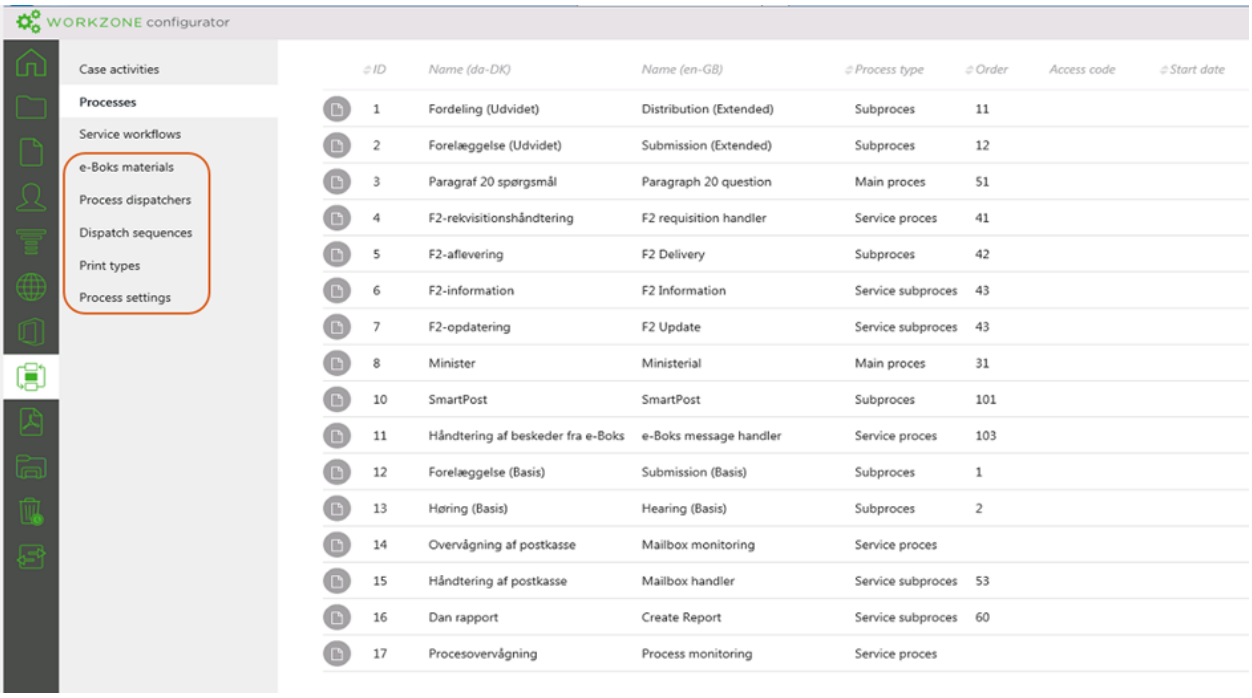
The rules for receiving updates and cancellation of F2 requisitions have changed. See Updated F2 requisitions. Cancelled F2 requisitions are now handled in WorkZone. See Cancelled F2 requisitions.

WorkZone Process 2018.2

Parameters

You can now define even more WorkZone Process parameters in WorkZone Configurator. With this release, the following configurations have been added to WorkZone Configurator:

- e-Boks materials. See Configure e-Boks materials.
- SmartPost dispatchers. See Configure dispatchers.
- Dispatch sequences. See Configure dispatch sequences.
- Print types (previously named remote print types). See Configure print types.
- General Process settings. See Other configurations.



The documentation has been revised to reflect the location of parameters in WorkZone Configurator.

Exchange Online

WorkZone Process now supports configuration of Exchange Online for sending smarttasks and e-mail notifications. You can also monitor Exchange Online mailboxes using the Mailbox monitoring and F2 requisition handler service workflows.

See Configure WorkZone Process in the WorkZone Installation Guide.

SmartPost enhancements:

A new OneTooX dispatcher has been added. Using the OneTooX dispatcher, it is possible to send SmartPost messages for remote print at KMD Printcenter. See Configure remote print - OneTooX.

WorkZone Process 2018.1

- You can now configure processes and service workflows in WorkZone Configurator. In WorkZone Configurator, click **Process**, and then select the area of configuration, for example **Processes**, or **Service workflows**. See Processes and Service workflows in the WorkZone ConfiguratorAdministrator Guide and Configuring processes and Service workflows in this guide.

> **Note:** As in previous releases, you configure general process settings and SmartPost settings in the WorkZone Configuration Management. The documentation has been revised to reflect where you find the relevant parameters.

- You can copy and rename a standard process and its labels if you want to use the process in another context. See Copy and rename a process.
- The F2 requisition handler service workflow now includes a new parameter **IncludeTemplate** and the **F2Template** parameter has been modified. See Install and configure F2 integration.
- Performance improvements have been made in the following areas:
  - User task actions.
  - Opening and loading default values in to the **Send SmartPost** dialog box.
- e-Boks and Strålfors error lists including error codes, descriptions, and SmartPost actions are now part of this guide. See Dispatcher error handling.

WorkZone Process 2018.01

- You can hide the approval check box from the SmartPost dialog box if your organization does not use the approval step in the SmartPost process. You can specify the setting named **ApprovalEnabled** in the SmartPost process settings in WorkZone Configuration Management. See Configure SmartPost.

- You can configure the SmartPost dialog box to include an option for selecting a standard letter provided by your organization. See Configure standard letters.
- You can configure the SmartPost process comply with customized of locations of CVR and CPR numbers in the database and identification of the sender when receiving SmartPost messages has been improved. See Configure CPR and CVR.

WorkZone Process 2018

- The WorkZone Process **Configuration Wizard** has been changed.
  - WorkZone Process now runs under a dedicated WorkZone Process user named SJPROCESSUSER. As in previous releases, you must create a service user in the AD, and enter information about it in the **KMD WorkZone Process Configuration Wizard**. The wizard will then handle the SID association with the SJPROCESSUSER automatically.

    Note: You no longer need to associate the SID.

  - You can now choose to run the configuration on either a web server role or an agent server role, or both from the **KMD WorkZone Process Configuration Wizard**. In previous releases, this selection was part of the **WorkZone ProcessSetup Wizard**. If you select the **Web** role, process packages and service workflows will be installed in the database, database changes will be downloaded, WorkZone Process will be configured in IIS, and process settings will be available in WorkZone Configuration Management. If you select the **Agent** role, all agents will be installed on the server and process services will be enabled.
  - A new **Validate** button allows you to validate that prerequisites are fulfilled and features connected with a specific role are in place before starting the actual configuration. You can also perform the validation using command line configuration by using a new `-val` parameter.

  - The WorkZone ProcessWorkZone Process **Configuration Wizard** now automatically adds logon as service to the service user.

- A new workflow log profile, which limits the amount of log information that is written to the **WZP_WORKFLOW_LOG** table, is introduced. You enable the profile for each process type in WorkZone Configuration Management.
- Error handling in the Mailbox Monitor service workflow has been improved. You can now separate faulty emails that have not been saved on cases from the emails in the monitored mailbox for better overview. You can set up the Mailbox Monitor service workflow to move the faulty emails to a specific Outlook folder and notify a specific user about by email. Two new settings **FaultedFolderName** and **FaultNotificationMailbox** settings are added in WorkZone Configuration Management. See Unsaved emails.
- F2 integration service workflow improvements:
  - The default process owner for F2 service workflows can be an organizational unit with an email.
  - Only one F2 mailbox monitor is allowed in a standard access code setup. One F2 mailbox monitor is allowed per authority in a corporate access code setup.

    See Create and configure an F2 requisition handler service workflow.

- Ministerial process improvements:
  - The Approval phase (Danish: Godkendelse) is now named Submission (Danish: Forelæggelse").
  - The Delivery phase (Danish: Aflevering) is now named Approval (Danish: Godkendelse).
  - When the extended submission process is started, you can set up the Ministerial process to move forward to the Submission phase. The Processing phase will be closed. See Configure a ministerial process.
  - When the extended submission process reaches a contributor, such as a unit or an employee with a specific role, the ministerial process is auto-

matically moved forward to the Approval phase. See Configure a ministerial process.

- If running with the F2 integration, you will see that information about sender and copy recipients is now merged from F2 to the description in the Ministerial process, so that you can see who sent the requisition and who are copy recipients on the requisition.

- SmartPost improvements:
  - The SmartPost dispatcher settings are now moved from the general **Process Settings** to the SmartPost process under **Processes** in WorkZone Configuration Management. See Configure dispatchers.
  - The **DefaultShipmentTypeKey** setting has been renamed to **DefaultDispatcherSequenceId**. See Configure dispatch sequences.
  - The preliminary history document is no longer needed and has been removed. **DummyPDFDocumentId** setting is no longer used and has been removed. The history document now shows the watermark "Preliminary" while in process.
- A new ProcessMonitor service workflow that can monitor for failed processes. See Process Monitor.
- You can now configure a history document for each process using four new settings, **ReportId**, **RecordType**, **RecordState**, and **TitleTemplate**. customize the process history document. See Configure the process history document.
- You can now create customized lists to display in the **Processes** overview and share these lists across an organization. See Create and share lists.

WorkZone Process 2017 SP1

- A new section on how to set up the SmartPost add-on package has been added. See Configuring SmartPost.
- The WorkZone Case Activities package is now in production. In the 2017 release, this package was released as a Beta version. For instructions on configuring case activity lists, see Case activities in the WorkZone Configurator online Help.

- A new section about how you can set up the Exchange server to handle concurrent Exchange connections on the same user in connection with the Mailbox Monitor and F2 integration service workflows.
- If you upgrade from 2016 R2 to 2017 SP1 and use the Mailbox Monitor process service, see Upgrading from previous versions.
- New settings have been added to the Extended Submission process. With these settings, you can manage what will happen when a submission is started, approved, completed, or rejected. In WorkZone Configuration Management, click **Operation** > **Processes**, select the **Submission (Extended)** process to view settings. See Configure extended submission.
- You can now remove a failed process from the **Errors and Warnings** list in the **Processes Overview** list using WorkZone Configuration Management. In WorkZone Configuration Management, click **Diagnostic** > **Process State** and change the state of the process in question to **Resolved** in the **State** field.
- Process history documents are now created using a WorkZone PDF template. The template can be customized to an organization's needs.

WorkZone Process 2017

- Support for multiple databases. See Configuration for multiple databases.
- An additional service workflow, the Mailbox Monitor, has been added. The mail box monitor can monitor an inbox and save incoming mails to a case. See Mailbox Monitor..
- IFor this version, a Beta release of the Case activities functionality will be available. Case activities is a task management feature that enable you to create workflows with activities that are connected by a set of rules. With case activities you can map the possible events in a workflow and associate each event with a rule that calls for a certain action.
- A new setting has been added in the WZP_SETTINGS table to enabled when you use AD Replication to recycle names in WorkZone Process. See Configure the use of new name instances.
- Two new parameters have been added to the WZP_SERVICE_PARAMETERS table.

  - `F2PartyMap`
  - `F2Template`

  See Install and configure F2 integration and F2 integration.

- The following has been added to the Troubleshooting section.
  - When you get to the point in the configuration of WorkZone Process where you start the WorkZone Process web service, you might receive an error with the message "403 Forbidden". The error indicates that OData information cannot be accessed and you cannot complete the configuration.
  - Creating a process in WorkZone Process fails and you get an error message stating that there is no access to the server.

Configuring processes

You can configure how processes should run in your organization by specifying parameters for each process in WorkZone Configurator.

You set up general WorkZone Process settings in **Process settings** in WorkZone Configurator.

Configure extended submission

When an extended submission process is part of a phase process, you can manage, promote (move forward), and demote (move back) actions when the extended submission process is started, approved, completed, or rejected.

1. In WorkZone Configurator, click **Process**.
2. Click **Processes**.
3. Point to the **Submission (Extended)** process, and click **Edit parameters**.
4. Specify the parameters depending on how you want the process to execute.

PromoteOnEnter	Moves to the next phase in the phase process when a submission starts. The default value is **False**.
PromoteBeforeClose	Moves to the next phase in the phase process when the last approver has approved. The default value is **False**.
PromoteOnExit	Moves to the next phase in the phase process when the submission ends. The default value is **True**.
DemoteOnReject	Moves to the previous phase in the phase process if the submission is rejected. The default value is **False**.
NotificationsDefaultActions	The default actions that will be selected on the **Notifications**

	tab in the **Start Submission (Extended)** dialog box. When the selected actions are performed in the submission process, notifications emails will be sent to the employees that the process owner has selected. See Start an extended submission process in the WorkZone Process User Guide.

The parameters **ReportID**, **RecordType**, **RecordState**, and **TitleTemplate** relate to the history document. See Configure the process history document.

See also Processes in the WorkZone Configurator Administrator Guide.

Configure a ministerial process

You can configure the ministerial process to move forward automatically between the phases.

Move from the Processing phase to the Submission phase automatically

To move from the Processing phase to the Submission phase automatically, you must configure the extended submission process to move to the next phase when the extended submission is started.

You need to set the **PromoteOnEnter** setting for the extended submission to **True**. See Configure extended submission.

Move to the next phase automatically based on a role

You can configure the ministerial process to move forward to the next phase based on a role. You can, for example, have the Submission phase move to the Approval phase automatically when the extended submission process reaches a specific actor, such as a unit or an employee with a specific role, for example `MANSEC` (Management secretariat).

Add roles

You add roles in WorkZone Configuration Management.

- Click **Basic Data** > **Custom domain**, and select the **WZP-ROLE** domain.

By default, WorkZone Process includes the roles listed below.

Role	Description
CASEHNDL	Case handler
DIRECTOR	Director
MANAGER	Manager
MANSEC	Management secretariat
MINISTER	Minister

Configure "move to next phase" according to role

The next step is to set up roles for each phase in WorkZone Configurator.

1. In WorkZone Configurator, click **Processes**.
2. Click **Processes**.
3. Point to the **Ministerial** process. A menu bar appears.
4. Click **Edit**.
5. In the **Edit process parameters** dialog box, select roles for the phases depending on how you want the process to execute. In this example, select the `MANSEC` role as default value for **Role4** in order for the Submission phase to move to the Approval phase automatically when the extended submission process reaches an actor with the role `MANSEC`

Assign roles to an organizational unit or an employee

You set up the default process role on either an organizational unit or an employee on the WorkZone contact by using ScanSQL.

> **Example**: You want the ministerial process to move from the Submission phase to the Approval phase when it reaches the employee named Elisabeth. Execute the following in ScanSQL:

```
update name set default_process_role = 'MANSEC' where name_
code = 'ELISABETH'
```

Important: If you have added roles in WorkZone Configuration Management, you must recycle the WzpSvc AppPool for the role-based configuration to take effect. Recycling of the AppPool is not necessary if you use the default roles.

Service workflows

A service workflow is a workflow that runs continuously in the environment where it is started. The service workflow can start any kind of workflow, based on the defined service parameters. One example of a service workflow is a workflow that monitors a mailbox, and starts workflows based on incoming mails.

F2 integration

With the F2 add-on package installed, the phase process capabilities of WorkZone Process become available in the communication between work groups that use F2 and WorkZone, respectively.

Overview

- When a requisition from an F2 work group is received in WorkZone, a case is automatically created, and a Ministerial phase process is started.
- A case handler is automatically appointed according to the requisition and the case handler receives the requisition as a smarttask.
- The case handler can work with the process and add contributors. When the contributors have completed their tasks, the case handler can submit the input from WorkZone Process to F2.

Monitor mailboxes for requisitions

Emails with requisitions that will be processed in WorkZone Process are identified by a mail monitor. The mailboxes that receive F2 requisitions must be set up with a mail monitor that polls for emails with an XML attachment. The XML attachment serves the following purposes:

- It identifies emails with requisitions that should start a service workflow.
- It contains information about responsibilities and deadlines and this information is used in the service workflow.

Emails that do not have an XML attachment are disregarded by the mail monitor.

For more information about setting up mail monitors, see Install and configure F2 integration.

Requisition instructions

A document may be available for additional descriptions or instructions. The document is saved on the case that is created based on the requisition.

You specify a template for the instruction document using the **F2Template** parameter in WorkZone Configurator. For more information about the **F2Template** parameter, see the parameter overview in Install and configure F2 integration

Requisitions that you receive in a mailbox

Requisitions that are received in a mailbox are either issued with the mailbox on the TO line or with the mailbox on the CC line.

Mail recipients on the TO line

- When an F2 requisition is identified in a mailbox where this mailbox is on the TO line, a case is created and a Ministerial phase process is started.
- Any documents from the requisition are attached to the case, and case details such as case handler and case unit are derived from the XML document attached to the F2 requisition. Note that all parties are looked up in existing contacts.
- A phase process of the type Ministerial is created. Service workflow details such as the title of the workflow and F2 specific deadlines are derived from the XML document. The phase approval deadline is calculated as the deadline specified in the XML minus two days.

Mail recipients on the CC line

- When an F2 requisition is identified in a mailbox where the mailbox is on the CC line, the mail is saved on a shared case, and a predefined mailbox receive a notification about the requisition. The notification contains a link to the default case and to the requisition.
- The shared case that is used for this information is created automatically when a mail with a mailbox recipient on the CC line is registered. For more information about

automatic creation of a case, see F2 integration in the WorkZone Installation Guide.

- The mailbox that receives information about the requisition is set up in the **F2InformationMailBox** parameter in WorkZone Configurator.

Why do I receive requisition emails that I have received once before?

If you experience that the same requisition email is sent to you more than once, it might be due to one of the following changes:

- A service handle name has been changed for a service that monitors the mailbox that handles your requisitions.
- A new service with a new service handle name has been created for the mailbox that handles your requisitions.

Both of the changes mentioned above have the effect that all requisition emails are handled once again. For more information about the **ServicHandleName** parameter, see Install and configure F2 integration.

Parties associated with cases and documents

When an F2 requisition is identified in a mailbox, cases are created and documents are saved. Parties associated with the cases and documents can be controlled by the **F2PartyMap** parameter in WorkZone Configurator. See the **F2PartyMap** parameter, see Install and configure F2 integration.

The F2PartyMap parameter is NOT specified

When the **F2PartyMap** parameter is not specified, the contacts become parties on documents and cases:

- Cases: The mail recipient, the return-to user, and any CC recipients.
- Documents on cases: The sender, the recipient, and any CC recipient.

The F2PartyMap parameter is specified

When the **F2PartyMap** parameter, individual email addresses are mapped to a contact name codes as specified in WorkZone Client:

- When an F2 case is created based on a requisition, the parties on the case include contacts that are specified by the **F2PartyMap** parameter. For example, say that a case is created based on an email sent by Elisabeth@Fvst.dk to Ann@lmdom.local, and the **F2PartyMap** parameter specifies that the fvst and the lmdom domains should map to the contacts FOODAUTHORITY and FSA, respectively. This would mean that apart from Elisabeth and Ann, the FOODAUTHORITY and the FSA contacts are included as parties on the F2 case and documents that are created by the F2 service workflow.

Updated F2 requisitions

If F2 requisitions are updated by F2, emails are sent to the monitored inbox. WorkZone identifies the F2 update emails based on the email subject. If an existing case with a corresponding requisition ID is found, it is updated with new information. The case handler and the mailbox that receives information about requisitions (as specified in the **F2InformationMailbox** parameter) are notified about the update in an email. See Updated requisitions in the WorkZone Process User Guide.

If the requisition case does not exist, the update email is ignored.

> **Note:** The update emails do not contain an XML attachment as the original email from F2.

Cancelled F2 requisitions

If F2 requisitions are cancelled from F2, emails are sent to the monitored inbox. WorkZone identifies the cancelled F2 requisition emails based on the email subject.

The Ministerial phase process will be cancelled but any sub processes must be handled manually. The case handler and the mailbox that receives information about requisitions (as specified in the **F2InformationMailbox** parameter) are notified about the cancellation of the F2 requisition in an email. See Cancelled requisitions in the WorkZone Process User Guide.

Replies to F2

When a requisition has been processed, it can be delivered to F2 using the **F2 Delivery** sub process. The following recipients get the delivery:

- The case handler in the F2 work group. The case handler is identified by a return field in the requisition XML. For more information, see How XML information maps to an F2 requisition workflow.
- A mailbox that is set up for the F2 work group. Via this mailbox information can be routed to people in the work group that should be notified about the delivery. The mailbox is defined in the **F2InformationMailbox** parameter in WorkZone Configurator. For more information, see Configure recipients of F2 answers.
- Additional recipients in the WorkZone environment. These recipients are people that should be notified about the delivery. You can add these recipients manually when you return the delivery to F2. For more information, see Return input to F2 in the online Help for WorkZone Process.

How XML information maps to an F2 requisition workflow

The following table describes the attributes of the case that is created when an F2 requisition is sent from F2 to a WorkZone mailbox. The attributes are mapped from an XML document attached to the F2 requisition.

Note: F2 requisition contacts must be matched with contact information that exists in the system. For more information, see Searching the WorkZone contacts for F2 parties.

Case attributes	XML fields	How information maps from XML to WorkZone Process fields
ID	<ID>	The **F2 requisition ID** field is populated with the requistion ID from the <ID> field in the XML.
Receiver name and unit	<ReceiverUserName>, <Receiv-	The **Case hander** and the **Case unit** fields are automatically populated with the information from the <ReceiverUserName> and the <ReceiverUnitName>

Case attributes	XML fields	How information maps from XML to WorkZone Process fields
	erUnitName>	fields. When an email with an XML attached is sent to <ReceiverUserName>, a user task is sent to this person and a process is started for this person.
Return information	<ReturnToEmail> <ReturnToUserName> <ReturnToUnitName>	The return-to fields are populated with recipients of the requisition after it has been processed. The recipient information is retrieved from the <ReturnToEmail>,<ReturnToUserName>, and the <ReturnToUnitName> fields. The fields are searched in this order to identify a valid receipt address. Delivery to the F2 work group can be completed using the **F2 Delivery** process task. Note, that the return-to recipients are recipients within the F2 environment, that should be informed about the delivery. A mailbox for F2 return deliveries must also be stated in the F2AnswerMailBox parameter in the WZP_SERVICE_PARAMETER table. For more information about the parameter setup, see Monitor mail activity.
Sender information	<SentByUserName> <SentbyUnitName>	External sender fields can be shown on the case and populated with the external sender information from the <SentByUserName> and the <SentbyUnitName> fields.
Description	<Description>	The description fields are automatically populated with the information from the <Description> field.

Case title	<RequsitionChoices>
	<Title>
		The title of the case is combined from the <RequsitionChoices> strings and the <Title> field.
		For example:
		`<RequisitionChoices><string>§ 20-question</string>`
		`<string>Ur-`

Case attributes	XML fields	How information maps from XML to WorkZone Process fields
		`gent</string></RequisitionChoices>` and `<Title>Transport Regulations</Title>` merge into the case title, " [Urgent] [§ 20-question] Transport Regulations"
Case number	<CaseNumber>	The **External case number** field can be shown on the case and populated with the case number from the <CaseNumber> field.
Case type		By default, the case type is set to SJ-TEMP.

Searching the WorkZone contacts for F2 parties

When an F2 service workflow is started, the F2 requisition identifies the parties of the requisition. The requisition parties are persons that must be matched with contacts in WorkZone.

The F2 requisition party information is available in the XML file, which is part of the F2 requisition and the information in the XML file may vary in terms of detail levels.

In some cases both a name and an email address is available and in other cases only a name (Name1 + Name2) is stated.

The search for a match of contacts is processed in the following sequence:

1. Email address.
2. Name1 + Name2
3. NameCode.

F2 integration

With the F2 add-on package installed, the phase process capabilities of WorkZone Process become available in the communication between work groups that use F2 and WorkZone, respectively.

Overview

- When a requisition from an F2 work group is received in WorkZone, a case is automatically created, and a Ministerial phase process is started.
- A case handler is automatically appointed according to the requisition and the case handler receives the requisition as a smarttask.
- The case handler can work with the process and add contributors. When the contributors have completed their tasks, the case handler can submit the input from WorkZone Process to F2.

Monitor mailboxes for requisitions

Emails with requisitions that will be processed in WorkZone Process are identified by a mail monitor. The mailboxes that receive F2 requisitions must be set up with a mail monitor that polls for emails with an XML attachment. The XML attachment serves the following purposes:

- It identifies emails with requisitions that should start a service workflow.
- It contains information about responsibilities and deadlines and this information is used in the service workflow.

Emails that do not have an XML attachment are disregarded by the mail monitor.

For more information about setting up mail monitors, see Install and configure F2 integration.

Requisition instructions

A document may be available for additional descriptions or instructions. The document is saved on the case that is created based on the requisition.

You specify a template for the instruction document using the **F2Template** parameter in WorkZone Configurator. For more information about the **F2Template** parameter, see the parameter overview in Install and configure F2 integration

Requisitions that you receive in a mailbox

Requisitions that are received in a mailbox are either issued with the mailbox on the TO line or with the mailbox on the CC line.

Mail recipients on the TO line

- When an F2 requisition is identified in a mailbox where this mailbox is on the TO line, a case is created and a Ministerial phase process is started.
- Any documents from the requisition are attached to the case, and case details such as case handler and case unit are derived from the XML document attached to the F2 requisition. Note that all parties are looked up in existing contacts.
- A phase process of the type Ministerial is created. Service workflow details such as the title of the workflow and F2 specific deadlines are derived from the XML document. The phase approval deadline is calculated as the deadline specified in the XML minus two days.

Mail recipients on the CC line

- When an F2 requisition is identified in a mailbox where the mailbox is on the CC line, the mail is saved on a shared case, and a predefined mailbox receive a notification about the requisition. The notification contains a link to the default case and to the requisition.
- The shared case that is used for this information is created automatically when a mail with a mailbox recipient on the CC line is registered. For more information about automatic creation of a case, see F2 integration in the WorkZone Installation Guide.
- The mailbox that receives information about the requisition is set up in the **F2InformationMailBox** parameter in WorkZone Configurator.

Why do I receive requisition emails that I have received once before?

If you experience that the same requisition email is sent to you more than once, it might be due to one of the following changes:

- A service handle name has been changed for a service that monitors the mailbox that handles your requisitions.

- A new service with a new service handle name has been created for the mailbox that handles your requisitions.

Both of the changes mentioned above have the effect that all requisition emails are handled once again. For more information about the **ServicHandleName** parameter, see Install and configure F2 integration.

Parties associated with cases and documents

When an F2 requisition is identified in a mailbox, cases are created and documents are saved. Parties associated with the cases and documents can be controlled by the **F2PartyMap** parameter in WorkZone Configurator. See the **F2PartyMap** parameter, see Install and configure F2 integration.

The F2PartyMap parameter is NOT specified

When the **F2PartyMap** parameter is not specified, the contacts become parties on documents and cases:

- Cases: The mail recipient, the return-to user, and any CC recipients.
- Documents on cases: The sender, the recipient, and any CC recipient.

The F2PartyMap parameter is specified

When the **F2PartyMap** parameter, individual email addresses are mapped to a contact name codes as specified in WorkZone Client:

- When an F2 case is created based on a requisition, the parties on the case include contacts that are specified by the **F2PartyMap** parameter. For example, say that a case is created based on an email sent by Elisabeth@Fvst.dk to Ann@lmdom.local, and the **F2PartyMap** parameter specifies that the fvst and the lmdom domains should map to the contacts FOODAUTHORITY and FSA, respectively. This would mean that apart from Elisabeth and Ann, the FOODAUTHORITY and the FSA contacts are included as parties on the F2 case and documents that are created by the F2 service workflow.

Updated F2 requisitions

If F2 requisitions are updated by F2, emails are sent to the monitored inbox. WorkZone identifies the F2 update emails based on the email subject. If an existing case with a corresponding requisition ID is found, it is updated with new information. The case handler and the mailbox that receives information about requisitions (as specified in the **F2InformationMailbox** parameter) are notified about the update in an email. See Updated requisitions in the WorkZone Process User Guide.

If the requisition case does not exist, the update email is ignored.

Note: The update emails do not contain an XML attachment as the original email from F2.

Cancelled F2 requisitions

If F2 requisitions are cancelled from F2, emails are sent to the monitored inbox. WorkZone identifies the cancelled F2 requisition emails based on the email subject.

The Ministerial phase process will be cancelled but any sub processes must be handled manually. The case handler and the mailbox that receives information about requisitions (as specified in the **F2InformationMailbox** parameter) are notified about the cancellation of the F2 requisition in an email. See Cancelled requisitions in the WorkZone Process User Guide.

Replies to F2

When a requisition has been processed, it can be delivered to F2 using the **F2 Delivery** sub process. The following recipients get the delivery:

- The case handler in the F2 work group. The case handler is identified by a return field in the requisition XML. For more information, see How XML information maps to an F2 requisition workflow.
- A mailbox that is set up for the F2 work group. Via this mailbox information can be routed to people in the work group that should be notified about the delivery. The

mailbox is defined in the **F2InformationMailbox** parameter in WorkZone Configurator. For more information, see Configure recipients of F2 answers.

- Additional recipients in the WorkZone environment. These recipients are people that should be notified about the delivery. You can add these recipients manually when you return the delivery to F2. For more information, see Return input to F2 in the online Help for WorkZone Process.

How XML information maps to an F2 requisition workflow

The following table describes the attributes of the case that is created when an F2 requisition is sent from F2 to a WorkZone mailbox. The attributes are mapped from an XML document attached to the F2 requisition.

Note: F2 requisition contacts must be matched with contact information that exists in the system. For more information, see Searching the WorkZone contacts for F2 parties.

Case attributes	XML fields	How information maps from XML to WorkZone Process fields
ID	<ID>	The **F2 requisition ID** field is populated with the requistion ID from the <ID> field in the XML.
Receiver name and unit	<ReceiverUserName>, <ReceiverUnitName>	The **Case hander** and the **Case unit** fields are automatically populated with the information from the <ReceiverUserName> and the <ReceiverUnitName> fields. When an email with an XML attached is sent to <ReceiverUserName>, a user task is sent to this person and a process is started for this person.
Return information	<ReturnToEmail> <ReturnToUserName> <ReturnToUnitName>	The return-to fields are populated with recipients of the requisition after it has been processed. The recipient information is retrieved from the <ReturnToEmail>,<ReturnToUserName>, and the <ReturnToUnitName> fields. The fields are searched in this order to identify a valid receipt address.

Case attributes	XML fields	How information maps from XML to WorkZone Process fields
		Delivery to the F2 work group can be completed using the **F2 Delivery** process task. Note, that the return-to recipients are recipients within the F2 environment, that should be informed about the delivery. A mailbox for F2 return deliveries must also be stated in the F2AnswerMailBox parameter in the WZP_SERVICE_PARAMETER table. For more information about the parameter setup, see Monitor mail activity.
Sender information	<SentByUserName> <SentbyUnitName>	External sender fields can be shown on the case and populated with the external sender information from the <SentByUserName> and the <SentbyUnitName> fields.
Description	<Description>	The description fields are automatically populated with the information from the <Description> field.
Case title	<RequsitionChoices> <Title>	The title of the case is combined from the <RequsitionChoices> strings and the <Title> field. For example: <RequisitionChoices><string>§ 20-question</string> <string>Urgent</string></RequisitionChoices> and <Title>Transport Regulations</Title> merge into the case title, " [Urgent] [§ 20-question] Transport Regulations"
Case number	<CaseNumber>	The **External case number** field can be shown on the case and populated with the case number from the <CaseNumber> field.
Case type		By default, the case type is set to SJ-TEMP.

Searching the WorkZone contacts for F2 parties

When an F2 service workflow is started, the F2 requisition identifies the parties of the requisition. The requisition parties are persons that must be matched with contacts in WorkZone.

The F2 requisition party information is available in the XML file, which is part of the F2 requisition and the information in the XML file may vary in terms of detail levels.

In some cases both a name and an email address is available and in other cases only a name (Name1 + Name2) is stated.

The search for a match of contacts is processed in the following sequence:

1. Email address.
2. Name1 + Name2
3. NameCode.

Install and configure F2 integration

F2 integration is a service workflow that you can select as a package when you configure WorkZone Process.

Follow the instructions below to activate the F2 integration. These guidelines assume that WorkZone Process is already installed on your system. If WorkZone Process is not installed, refer to Install WorkZone Process in the WorkZone Installation Guide and follow the guidelines for the installation.

Activate the F2 Integration package

1. Open WorkZone Configurator.
2. Go to **Global** > **Feature settings** > **WorkZone Process**.
3. Select the check box next to **F2**.

Monitor email activity

The F2 integration requires monitoring of email activity in a mailbox. You specify which mailbox to monitor, and how often the mailbox will be checked for emails.

In general, the email activity in an F2 mailbox is monitored by the Exchange user that owns the mailbox. If you need to set up the mailbox to be monitored by a user different from the owner of the mailbox, see Provide access to monitor an F2 mail account.

You configure the F2 mailbox monitor by specifying parameters for the **F2 requisition handler** service workflow in WorkZone Configurator.

You need to create an F2 requisition handler service workflow for each mailbox that you want to monitor.

Create and configure an F2 requisition handler service workflow

The F2 integration service uses mail monitors that require a set of F2 service parameters.

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. Add a new service workflow of the type **F2 requisition handler** or **Cloud F2 requisition handler** depending on whether your organization uses Exchange On-Premises or Exchange Online.
4. Enter a name and description, and then click **Create**.
5. Point to the **F2 requisition handler** service workflow that you just created, and click **Edit parameters**, and fill in the value for the parameters. The values that you enter, must correspond to the values that are set up for your environment. For an example, refer to the list of parameters in the following table.

> **Note:** You can only set up one F2 mailbox monitor in a standard access code setup. In a corporate access code setup, you can set up one F2 mailbox monitor per authority.

Refer to the following table for an overview of the parameter values required for the F2 requisition handler workflow. Note that the values listed in the tables are just examples.

The Exchange configurations depend on whether your organization uses Exchange On-Premises or Exchange Online.

On-premises

Name	Description	Sample values
ExchangeUrl	The URL of the Exchange web service.	https://<host>/EWS/Exchange.asmx.
ExchangeDomain	The domain for the Exchange user.	
ExchangeUser	Login for the Exchange user. This user must have access to the Exchange mailbox. The user must be a WorkZone user and the name must be in uppercase.	The user that you have set up as the smarttask sender during configuration of WorkZone Process.
ExchangePassword	The password for the Exchange user.	

Online

Name	Description	Sample values
ExchangeOAuthClientId	The OAuth2 Client ID that is used to access the mailbox in Exchange Online.	
ExchangeOAuthTenantId	ExchangeOAuthTenantId: The OAuth2 Tenant ID used to access the mailbox in Exchange Online.	
ExchangePassword	The password of the Exchange user that is used in the public client flow also named Resource Owner Password Credentials (ROPC) flow. It is recommended to choose between setting this parameter and the **ExchangeOAuthClientSecret** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	
ExchangeOAuthClientSecret	The OAuth2 Client secret used to access the mailbox in Exchange Online. If set, the client credentials flow is used.	

Name	Description	Sample values
	It is recommended to choose between setting this parameter and the **ExchangePassword** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	

Note:

The public client flow (ROPC) with the **ExchangePassword** parameter is less complex to set up, but it allows logging in without multi-factor authentication to the application in the AAD, so it may decrease the security level for organizations that use multi-factor authentication to AAD.

The client credential flow with **ExchangeOAuthClientSecret** parameter is better suited for service accounts such as the service accounts that the Mailbox monitoring workflow monitors, but is complex to set up correctly because it requires a second application registration in the AAD (Azure Active Directory) with the access scoped only to a group of service users.

Other parameters

The parameters below are common to both the **F2 requisition handler** and **Cloud F2 requisition handler** workflows.

Name	Description	Sample values
ExchangeMailBox	The email address of the mailbox to be monitored.	ann@lmdom.local
WatchInterval	Interval in seconds between checks of the Exchange mailbox for new requisition emails. With an entry of 60, the mailbox is checked every minute.	60
RetryInterval	The interval in seconds	5

Name	Description	Sample values
	between resending of mails that failed. If this parameter is shorter than WatchInterval, it has no effect.	
RetryCount	The number of retries before mails are abandoned.	2
ServiceHandleName	The name used by a service to mark a mail as handled. This parameter is used if a mailbox is monitored by more than one service. The ServiceHandleName must be unique for each service. Note, that if you change a service handle name for a service that monitors a specific mailbox or if you create a new service for the same mailbox with a new service handle name, all requisition mails will be handled again.	F2Handle
F2InformationCaseNo	The case number of a case that stores requisitions received as CC. This case exists in the WorkZone database.	16-80/1
F2InformationMailBox	Address of a mailbox that receives information about requisition emails that are received as CC by the owner of the Exchange mailbox.	testadmin@lmdom.local
F2AnswerMailBox	Address of the mailbox that	susan@lmdom.local

Name	Description	Sample values
	should receive a copy of the answer mails that are sent as F2 deliveries.	
DefaultOwner	The user who becomes the owner of the process. The user must be a WorkZone user and the name must be capitalized. The default process owner may also be a unit with an email address.	
DefaultReceiver	If specified, the user who should receive the requisition.	
F2PartyMap	Enables mapping of parties that should be associated with cases and documents. A company-specific email domain is mapped with a name contact code and a name contact type. For a series of mappings, each mapping must be separated by a semicolon. Invalid name codes and name types and missing email domains will be skipped.	Fvst.dk,F-FOODAUTHORITY;Im-dom.local,A-FSA;
IncludeTemplate	Turn on **IncludeTemplate** if you want to include a document with instructions on how, for example, to handle F2 requisitions. You can	

Name	Description	Sample values
	select a document to use in the **F2Template** field. The parameter is enabled by default. The document template must have the type SKAB.	
F2Template	Select a Word document that will be used for building a document with instructions. If you do not select a document, a default Word document containing the F2 description will be used. If a document is created, it is saved on the case and added to smarttask.	

Provide access to monitor an F2 mail account

Mails sent to an F2 mailbox can be monitored by the exchange user that owns the mailbox. As an alternative, the F2 mailbox can be monitored by a user different from the owner of the mailbox.

If you want the F2 mailbox to be monitored by a user different from the owner of the mailbox, ExchangeUser can be given access rights to the mailbox.

Delegate access to a mailbox

Follow the steps to give ExchangeUser access rights to an F2 mailbox.

The F2 mailbox is the mailbox defined for the ExchangeMailBox parameter in the WZP_SERVICE_PARAMETERS table.

From Outlook:

1. As the owner of the mailbox (ExchangeMailBox), open Outlook.
2. Click the **File** tab, and select **Account settings** > **Delegate access**, then click **Add**.
3. Select the user that is defined for the ExchangeUser parameter.
4. Click **Add** > **OK**, and in the **Tasks** field, select **Editor**.
5. Click the **Home** tab, and select the Inbox.
6. Right-click the Inbox, and click **Properties**.
7. Click the **Permissions** tab, select the user to be given permissions, and, in the **Permission level** field, select the **Editor** role. Optionally, you can clear the **Create Item** check box.

   You can select a role that has more permissions, such as **Publishing editor** or **Owner**, but you cannot select a role with fewer permissions.

On Exchange

1. As an Exchange administrator, open a Windows PowerShell prompt.
2. Enter one of the following commands to load the Exchange snap-in that corresponds to the Exchange version you are using:

```
Add-PSSnapin Microsoft.Ex-
change.Management.PowerShell.E2010
```

```
Add-PSSnapin Microsoft.Ex-
change.Management.PowerShell.E2016
```

3. Enter the following command:

```
Add-MailboxFolderPermission <Mailbox> -AccessRight
ReadItems, FolderVisible, EditOwnedItems,
EditAllItems, DeleteOwnedItems, DeleteAllItems -User
<monitor user>
```

Where `mailbox` is the mailbox you want to monitor and `monitor user` is the user who will monitor the mailbox. In this example, the permission to create items is disabled.

4. Repeat step 3 for each mailbox you want to monitor.

Mailbox monitor

Mailbox monitor is a service workflow that can monitor one or more Outlook mailboxes and save incoming emails as documents on cases.

Cases for incoming mails

The case on which the Mailbox monitor service workflow saves incoming emails is identified as follows:

- If an email title contains a case number in brackets such as "[00001234-2016]" and the case exists, the mail is saved on this case.
- If an email title does not contain a case number in brackets and a default case is specified in the service parameters, all incoming emails are saved on the default case.
- If there is no case number in an email title or if a default case is not identified, a new case is created for individual emails. The new case gets the title of the email subject and the sender, recipients, and CC recipients are added as case parties.

The Mailbox Monitor service workflow does not handle emails that have the monitored mailbox as BCC recipient. These emails are not saved.

Unsaved emails

In some cases, incoming emails are not saved on cases due to issues in the emails or their attachments. To get an overview of unsaved emails that must be saved manually, you can set up the Mailbox Monitor service workflow to move the faulty emails to a specific Outlook folder, and in this way separate the faulty emails from the emails in the monitored mailbox. The folder with the faulty emails is a subfolder of the monitored mailbox. A user must then save the faulty emails on cases manually.

You can specify the email address of a user who will then receive a notification email when an email is not saved automatically due to errors.

To handle unsaved emails, specify the FaultedFolderName and FaultNotificationMailbox parameters in WorkZone Configurator.

Supported email messages

Mailbox monitor only handles standard email messages of the type IPM.Note. If, for example, a monitored mailbox is also used to send messages, and an automatic out of office reply is received in the monitored mailbox, the Mailbox monitor service workflow will not handle this message because an automatic reply is of the type IPM.Note.Rules.OofTemplate.

See the Microsoft article Item Types and Message Classes for a list of supported messages in Outlook.

Configure a Mailbox Monitor service workflow

The Mailbox Monitor service workflow monitors email activity in one or more mailboxes. The service workflow defines which mailboxes are monitored, and how often the mailboxes are checked for emails. You can create service workflows in WorkZone Configurator.

Create a Mailbox monitor service workflow

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. In the bottom right corner of the page, click **Create**.
4. Select the **Mailbox monitoring** or the **Cloud Mailbox monitoring** service workflow depending on whether your organization uses Exchange On-Premises or Exchange Online.
5. Enter a name and description, and then click **Create**.

See Service workflows in the WorkZone Configurator Administrator Guide.

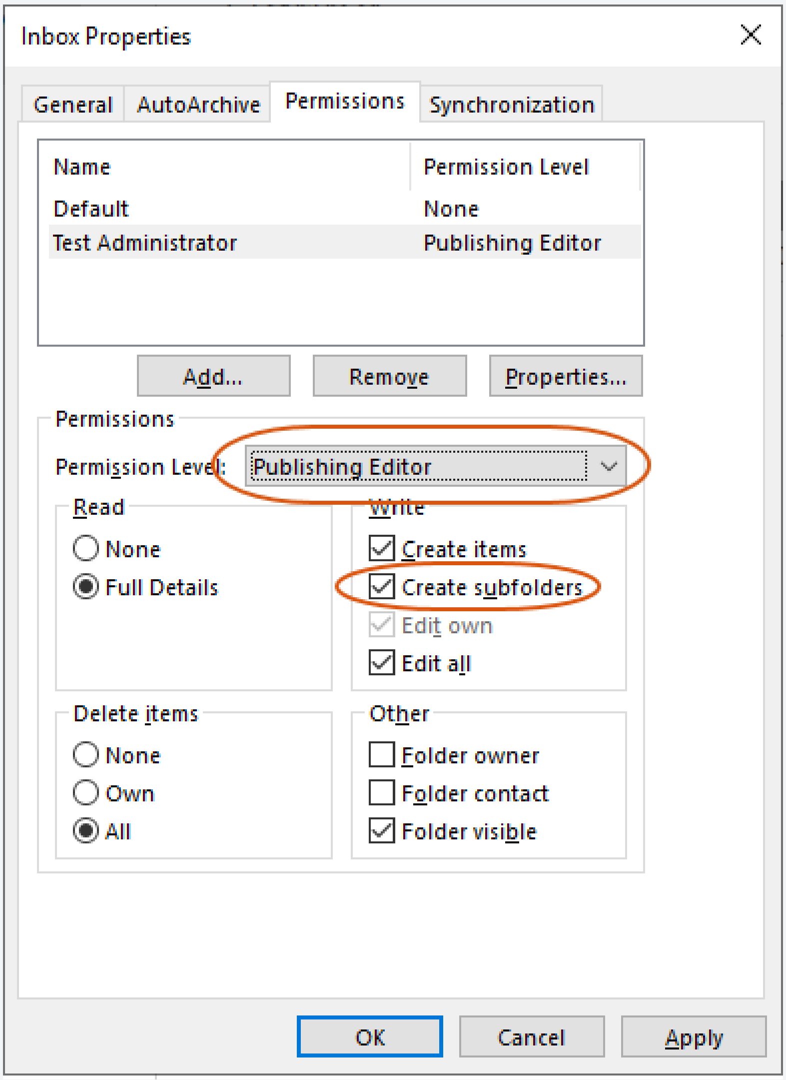
Important: The number of mailboxes that the Mailbox Monitor service workflow can monitor depends on the capacity of the environment. The number of monitored mailboxes and the number of emails that the mailboxes receive will impact the system memory, disk space, and load. Please contact WorkZone support for technical advice if you plan to monitor many mailboxes with a high volume of emails. For example, more than 10 mailboxes and 100 emails per day per mailbox.

Configure a Mailbox Monitor service workflow

Prerequisite:

- The Exchange user must have the **Delegate** access with **Editor** permission on the inboxes that you want to monitor. See the Configure a Mailbox Monitor service workflow parameter. In Outlook, log on to each of the Exchange mailboxes that you want to monitor, and go to **File** > **Account Settings** > **Delegate access** and add the Exchange user as a delegate.
- The Exchange user must have publishing editor rights. To verify that the permissions are correct, right-click the inbox and click **Properties** > **Permission** tab. Verify that the Exchange user has the permission level **Publishing Editor**

and that the **Create subfolders** check box is selected.



1. Open WorkZone Configurator.
2. Click **Process** > **Service workflows**.
3. Point to the **Mailbox monitoring** service workflow that you just created, and click  **Edit parameters** to configure the service workflow.
4. Enter values for the parameters.

   If you want the service workflow to monitor multiple mailboxes, pay attention to the configuration of the following parameters:

- ExchangeMailBox
- DefaultCase
- FaultedFolderName
- FaultNotificationMailbox
- RecipientAddressProperty

The Exchange configurations depend on whether your organization uses Exchange On-Premises or Exchange Online.

On-premises

Name	Description	Sample values
ExchangeUrl	The URL of the Exchange web service.	https://<host>/EWS/Exchange.asmx.
ExchangeDomain	The domain for the Exchange user.	
ExchangeUser	Login for the Exchange user. This user must have access to the Exchange mailbox. The user must be a WorkZone user and the name must be in uppercase.	The user that you have set up as the smarttask sender during configuration of WorkZone Process.
ExchangePassword	The password for the Exchange user.	

Online

Name	Description	Sample values
ExchangeOAuthClientId	The OAuth2 Client ID that is used to access the mailbox in Exchange Online.	
ExchangeOAuthTenantId	ExchangeOAuthTenantId: The OAuth2 Tenant ID used to access the mailbox in Exchange Online.	
ExchangePassword	The password of the Exchange user that is used in the public client flow also named Resource Owner	

Name	Description	Sample values
	Password Credentials (ROPC) flow. It is recommended to choose between setting this parameter and the **ExchangeOAuthClientSecret** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	
ExchangeOAuthClientSecret	The OAuth2 Client secret used to access the mailbox in Exchange Online. If set, the client credentials flow is used. It is recommended to choose between setting this parameter and the **ExchangePassword** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	

Note:

The public client flow (ROPC) with the **ExchangePassword** parameter is less complex to set up, but it allows logging in without multi-factor authentication to the application in the AAD, so it may decrease the security level for organizations that use multi-factor authentication to AAD.

The client credential flow with **ExchangeOAuthClientSecret** parameter is better suited for service accounts such as the service accounts that the Mailbox monitoring workflow monitors, but is complex to set up correctly because it requires a second application registration in the AAD (Azure Active Directory) with the access scoped only to a group of service users.

Other parameters

The parameters below are common to both the **Mailbox monitoring** and the **Cloud Mailbox monitoring** service workflows

Name	Description	Sample value
ExchangeMailBox	The email address of the mailbox to be monitored. If you want to monitor multiple mailboxes, separate the mailbox addresses by commas.	
WatchInterval	The interval in seconds between checking the Exchange mailbox for new emails. A value of 60 - 300 seconds is suitable in most cases.	60
RetryInterval	The interval in seconds between rereading emails that failed to be read. The value must be higher than the watch interval to have effect. This value should be 2 - 5 times larger than the value for the **WatchInterval** settings.	300
RetryCount	The number of times a rereading of the emails is atttempted before the emails are abandoned A value of 2 - 5 times is appropriate.	2
ServiceHandleName	The name used by a service to mark an email as handled. The ServiceHandleName must be unique for each service and never be changed for a specific mailbox. Any unique combination of letters and numbers.	
ProcessOwner	The user that will be assigned as process owner.	

Name	Description	Sample value
	The process owner may also be an organizational unit.	
DefaultCase	The case number of the default case that is used for incoming emails. If it is not specified, each email will be saved on a new case. If you monitor multiple mailboxes, the default case will be a combined case for all incoming emails in any of the monitored mailboxes.	Optional value.
DefaultOfficer	The user that will become case handler on the cases that are created. If it is not specified, no case handler is assigned.	Optional value.
DefaultCaseGroup	The case group that will be assigned to new cases. If not specified, SJ-TEMP is used.	Optional value.
AttachmentsIsAppendices	Email attachments are stored as supplementary documents. If it is not enabled, the email attachments will be saved as main documents.	Optional value. If “AttachmentsIsAppendices” is enabled, the document state cannot be ‘AFS’.
NotificationReceivers	The users who will receive a notification when an email is received. If you do not specify recipients, no notifications are sent.	
DocumentState	The document state that the documents will be saved with. If it is not specified, the document state will be ARK.	If “DefaultCaseGroup” is not defined, the document state cannot be ‘AFS’.
Authority	The current authority to grant access to the case. Mandatory for	This value is ignored for a WorkZone standard access

Name	Description	Sample value
	corporate access codes.	codes setup, but it is mandatory for a WorkZone corporate access codes setup.
MailList	The name of the mail list that you want the email documents to be shown on.	Optional value.
MailType	The email document type.	Default value = I.
AttachmentType	The document type of the attachment. Must be a valid value from the AT domain.	Default value = DOK.
SaveSender	The field that the sender's email address is saved to. By default, the email address is saved to the **Sent from** field. If you do not specify a field, the sender email address will not be saved. You can use a custom field, and in this case,both the sender's email address and name will be saved.	Optional value.
FaultedFolderName	Name of the Outlook folder used for emails that cannot be saved automatically in WorkZone due to issues in the emails or their attachments. The folder will be created as a subfolder of the monitored mailbox. The folder will only be created if there are faulty emails. If you monitor multiple mailboxes, a folder with this name will be created as a subfolder of each of the mon-	

Name	Description	Sample value
	itored mailboxes.	
FaultNotificationMailbox	The email address of a user who will receive an email notification when an email is not saved automatically. If you monitor multiple mailboxes, the email address that you specify will receive notifications about faulty emails from all monitored mailboxes.	
RecipientAddressProperty	If you monitor several mailboxes with one service workflow, you may want to add a field on the document detail page for the email document that shows to which mailbox the document was sent. If you have set up such a field, add the code for the field here, and it will be populated with the email address. See Optional configurations in WorkZone Client.	

> **Note:** If you have configured the Mailbox Monitor service workflow to monitor multiple mailboxes, you can do additional configuration in WorkZone Client, which will make it easier for users to monitor incoming documents per mailbox and work with the documents. See Optional configurations in WorkZone Client.

Optional configurations in WorkZone Client

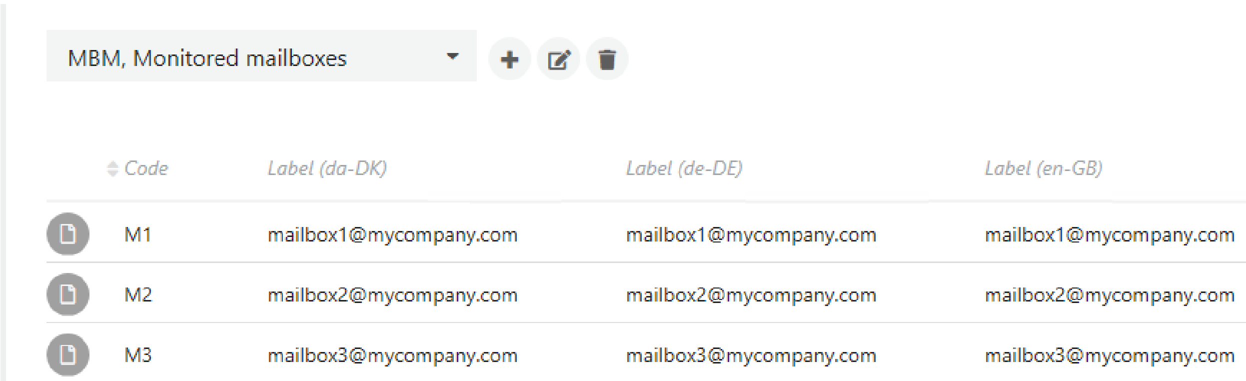
If you have configured a Mailbox Monitor service workflow to monitor multiple mailboxes, you can do additional configuration in WorkZone Client to make it easier for users to work with the incoming documents that the service workflow creates. The configurations may be relevant, if you have configured a default combined case using the DefaultCase parameter as opposed to creating new cases for all incoming emails.

Create a custom field to display the monitored mailbox on the document detail page

You can, for example, add a custom field on the document detail page that displays the name of the mailbox that the email was sent to. Such a field will also allow the user to select another mailbox if, for some reason, the email was sent to the wrong mailbox.

Create a custom field of the type droplist

1. Open WorkZone Configurator
2. Go to **Document** > **Custom fields**.
3. Create a new field of the type **Droplist**, for example Monitored mailbox.
4. Go to **Global** > **Custom droplists**.
5. Create a new droplist, for example Monitored mailboxes.
6. Add the mailbox addresses of the mailboxes you monitor as items on the droplist. Enter the mailbox address in the **Label** field and a code in the **Code** field.

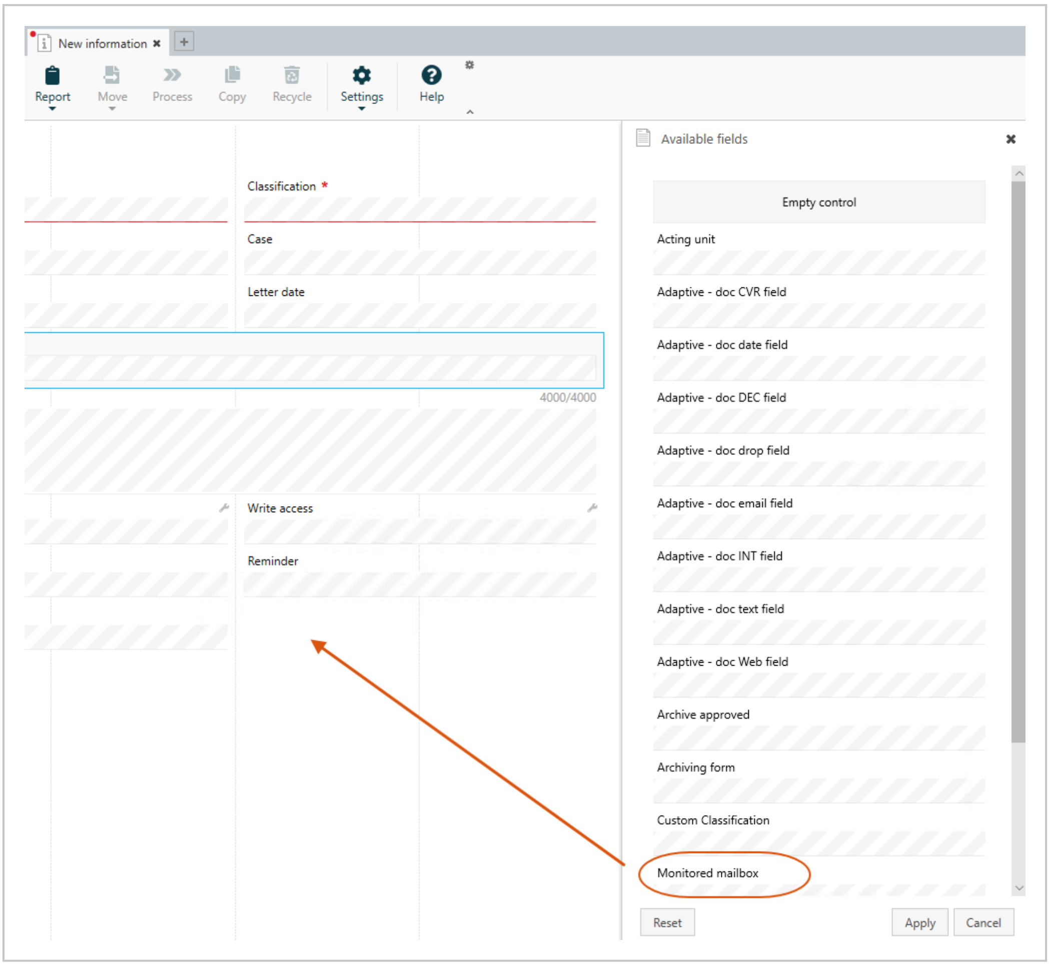


See Custom fields and Custom droplist in the WorkZone Configurator.

Display the custom field on the document detail page

1. In WorkZone Client, create a new configuration or edit an existing configuration. See Working with configurations in the WorkZone Client Administrator Guide.
2. Click **Document** > **Information** in the main ribbon.

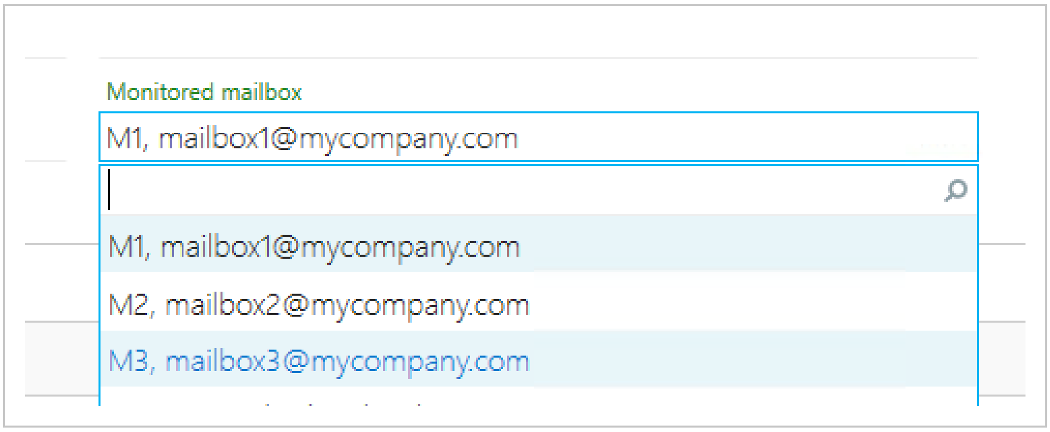
3. Click **Configure page** at the top right-hand corner to open the **Available fields** pane. Add the custom field to the document detail page.



See Configure a detail page in the WorkZone Client Administrator Guide.

4. Distribute the configuration to your organization. See Distribute a configuration in the WorkZone Client Administrator Guide.
5. Exit distribution mode.

Users can now see the mailbox and select another mailbox on the document detail page.

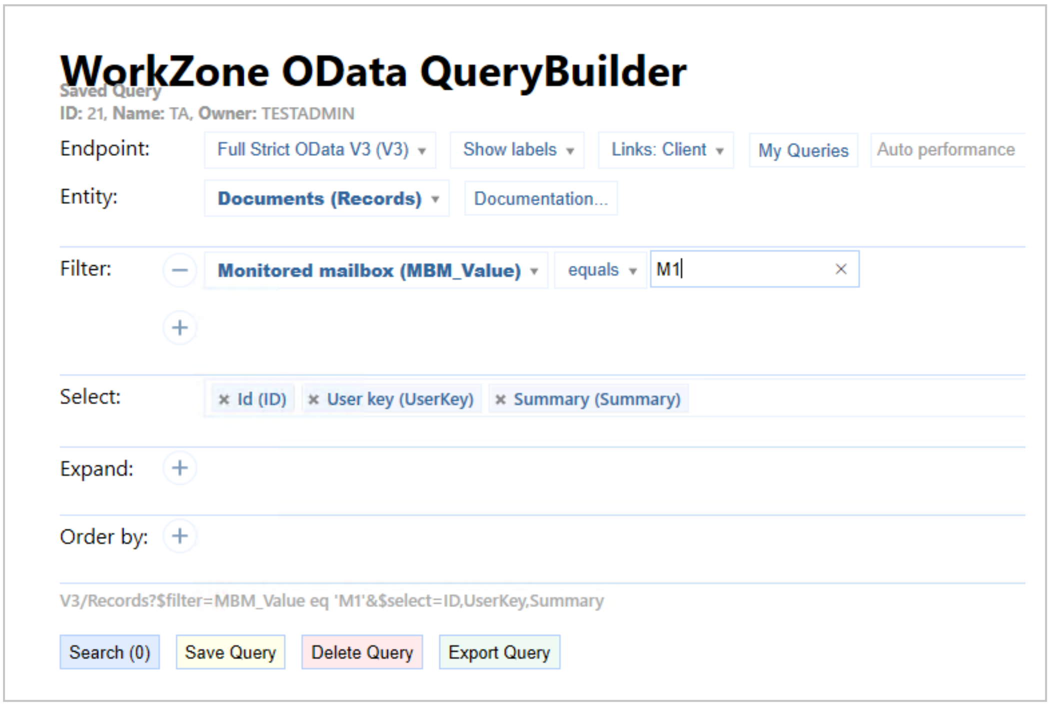


Create saved searches to show incoming documents per mailbox

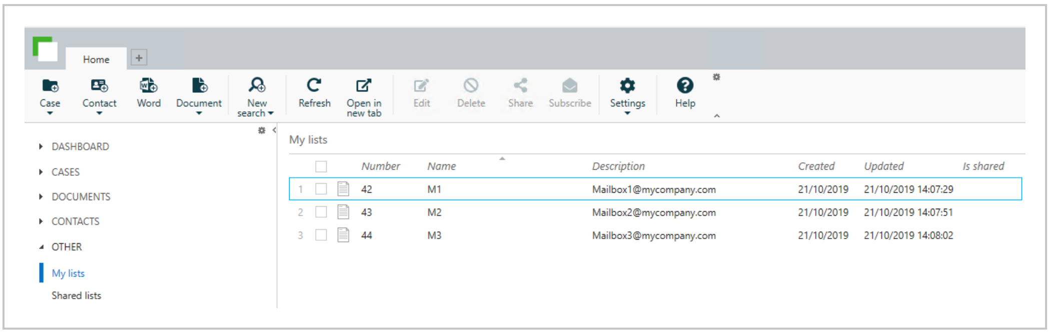
You can create saved searches that show incoming documents created by Mailbox Monitor per mailbox and, for example, you can display the saved searches on the dashboard in WorkZone Client for easy access.

Create a saved search per mailbox using WorkZone QueryBuilder

1. Open WorkZone QueryBuilder.
2. Select **Documents(Records)** in the **Entity** field.
3. Filter on the mailbox using the custom field code that you just created, in this example filter on the code **M1** using the **Monitored mailbox** field.



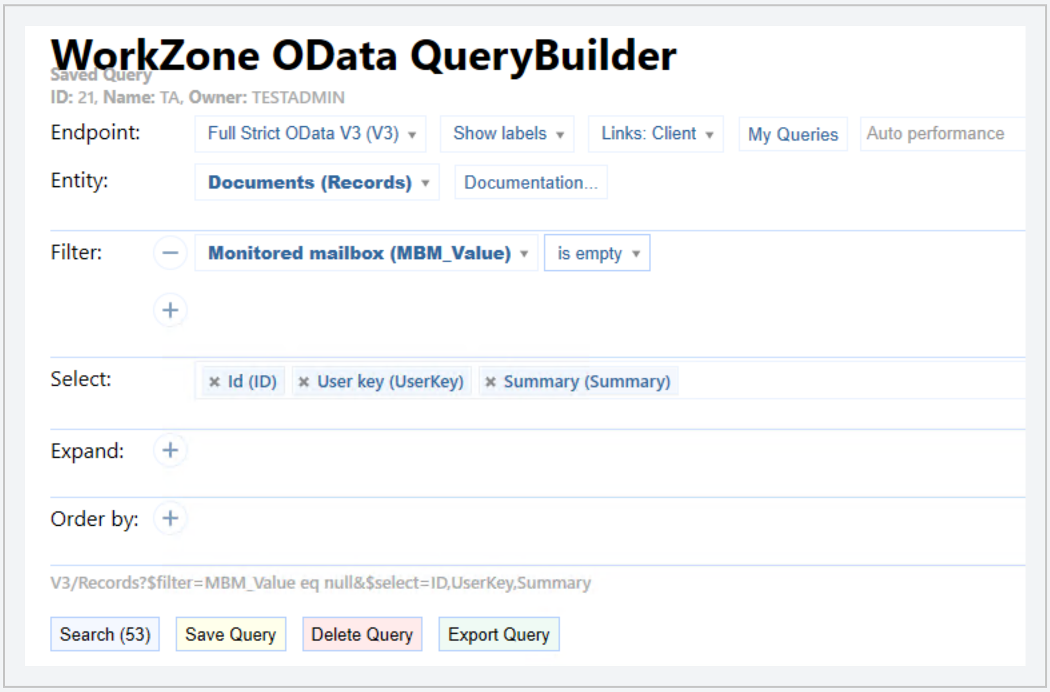
4. Click **Save Query**. The saved search now appears in the navigation pane under **OTHER** > **My lists**.



5. Repeat the steps 1-4 for each of the mailboxes that are monitored.

You can now share the saved search list with the relevant users. See Share a saved search list in the WorkZone Client User Guide.

Tip: If you want to check that all monitored mailboxes are shown in the droplist in WorkZone Client, you can create a saved search where the filter of the custom field is **is empty**. This is useful if you add mailboxes to service workflows, and want to make sure that you have not forgotten to add them as items on the droplist. For example:



Process Monitor

The process monitor is a service workflow that can monitor if processes fail. It monitors:

- Failed processes. For example, a process will fail if an actor has been deleted from the Active Directory, or an actor does not have appropriate access rights.
- Unsent smarttask in the service queue. If Microsoft Exchange is not running, smarttask as emails will not be sent.

In each case, an email is sent to the process owner to inform about the process that has failed. The email contains a link to the process in the **Processes** overview and the process ID. The process owner can send the information to the organization's WorkZone administrator for further investigation. The WorkZone administrator should then check the workflow log or the service queue for more information. See Process logging in the WorkZone Operations Guide.

Create a Process monitor service workflow

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. In the bottom right corner of the page, click **Create**.
4. Select the **Process monitoring** or the **Cloud Process monitoring** service workflow depending on whether your organization uses Exchange On-Premises or Exchange Online.
5. Enter a name and description, and then click **Create**.

See Service workflows in the WorkZone Configurator Administrator Guide.

Configure a Process monitoring service workflow

1. Open WorkZone Configurator.
2. Click **Process** > **Service workflows**.
3. Point to the **Process monitoring** service workflow that you just created, and click **Edit parameters** to configure the service workflow.
4. Enter values for the parameters.

The Exchange configurations depend on whether your organization uses Exchange On-Premises or Exchange Online.

On-premises

Name	Description	Sample values
ExchangeUrl	The URL of the Exchange web service.	https://<host>/EWS/Exchange.asmx.
ExchangeDomain	The domain for the Exchange user.	
ExchangeUser	Login for the Exchange user. This user must have access to the Exchange mailbox. The user must be a WorkZone user and the name must be in uppercase.	The user that you have set up as the smarttask sender during configuration of WorkZone Process.
ExchangePassword	The password for the Exchange user.	

Online

Name	Description	Sample values
ExchangeOAuthClientId	The OAuth2 Client ID that is used to access the mailbox in Exchange Online.	

Name	Description	Sample values
ExchangeOAuthTenantId	ExchangeOAuthTenantId: The OAuth2 Tenant ID used to access the mailbox in Exchange Online.	
ExchangePassword	The password of the Exchange user that is used in the public client flow also named Resource Owner Password Credentials (ROPC) flow. It is recommended to choose between setting this parameter and the **ExchangeOAuthClientSecret** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	
ExchangeOAuthClientSecret	The OAuth2 Client secret used to access the mailbox in Exchange Online. If set, the client credentials flow is used. It is recommended to choose between setting this parameter and the **ExchangePassword** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	

Note:

The public client flow (ROPC) with the **ExchangePassword** parameter is less complex to set up, but it allows logging in without multi-factor authentication to the application in the AAD, so it may decrease the security level for organizations that use multi-factor authentication to AAD.

The client credential flow with **ExchangeOAuthClientSecret** parameter is better suited for service accounts such as the service accounts that the Mailbox monitoring workflow monitors, but is complex to set up correctly because it requires a second application registration in the AAD (Azure Active Directory) with the access scoped only to a group of service users.

Other parameters

The parameters below are common to both the **Process monitoring** and the **Cloud Process monitoring** service workflows.

Name	Description	Sample values
ExchangeMailBox	The email address of the Exchange user mailbox.	
WatchInterval	Defines how often the workflow should check for failed processes.	300 seconds.
DefaultReceiver	The email address of a person who will receive the email in case the process owner does not have an email address.	

Process Monitor

The process monitor is a service workflow that can monitor if processes fail. It monitors:

- Failed processes. For example, a process will fail if an actor has been deleted from the Active Directory, or an actor does not have appropriate access rights.
- Unsent smarttask in the service queue. If Microsoft Exchange is not running, smarttask as emails will not be sent.

In each case, an email is sent to the process owner to inform about the process that has failed. The email contains a link to the process in the **Processes** overview and the process ID. The process owner can send the information to the organization's WorkZone administrator for further investigation. The WorkZone administrator should then check the workflow log or the service queue for more information. See Process logging in the WorkZone Operations Guide.

Create a Process monitor service workflow

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. In the bottom right corner of the page, click **Create**.
4. Select the **Process monitoring** or the **Cloud Process monitoring** service workflow depending on whether your organization uses Exchange On-Premises or Exchange Online.
5. Enter a name and description, and then click **Create**.

See Service workflows in the WorkZone Configurator Administrator Guide.

Configure a Process monitoring service workflow

1. Open WorkZone Configurator.
2. Click **Process** > **Service workflows**.
3. Point to the **Process monitoring** service workflow that you just created, and click **Edit parameters** to configure the service workflow.
4. Enter values for the parameters.

The Exchange configurations depend on whether your organization uses Exchange On-Premises or Exchange Online.

On-premises

Name	Description	Sample values
ExchangeUrl	The URL of the Exchange web service.	https://<host>/EWS/Exchange.asmx.
ExchangeDomain	The domain for the Exchange user.	
ExchangeUser	Login for the Exchange user. This user must have access to the Exchange mailbox. The user	The user that you have set up as the smarttask sender during configuration of WorkZone Process.

Name	Description	Sample values
	must be a WorkZone user and the name must be in uppercase.	
ExchangePassword	The password for the Exchange user.	

Online

Name	Description	Sample values
ExchangeOAuthClientId	The OAuth2 Client ID that is used to access the mailbox in Exchange Online.	
ExchangeOAuthTenantId	ExchangeOAuthTenantId: The OAuth2 Tenant ID used to access the mailbox in Exchange Online.	
ExchangePassword	The password of the Exchange user that is used in the public client flow also named Resource Owner Password Credentials (ROPC) flow. It is recommended to choose between setting this parameter and the **ExchangeOAuthClientSecret** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	
ExchangeOAuthClientSecret	The OAuth2 Client secret used to access the mailbox in Exchange Online. If set, the client credentials flow is used. It is recommended to choose between setting this parameter and the **ExchangePassword** parameter. If you fill in both, the **ExchangeOAuthClientSecret** parameter will be prioritized over the **ExchangePassword** parameter.	

Note:

The public client flow (ROPC) with the **ExchangePassword** parameter is less complex to set up, but it allows logging in without multi-factor authentication to the application in the AAD, so it may decrease the security level for organizations that use multi-factor authentication to AAD.

The client credential flow with **ExchangeOAuthClientSecret** parameter is better suited for service accounts such as the service accounts that the Mailbox monitoring workflow monitors, but is complex to set up correctly because it requires a second application registration in the AAD (Azure Active Directory) with the access scoped only to a group of service users.

Other parameters

The parameters below are common to both the **Process monitoring** and the **Cloud Process monitoring** service workflows.

Name	Description	Sample values
ExchangeMailBox	The email address of the Exchange user mailbox.	
WatchInterval	Defines how often the workflow should check for failed processes.	300 seconds.
DefaultReceiver	The email address of a person who will receive the email in case the process owner does not have an email address.	

Case monitor

The Case monitoring service workflow can monitor newly created cases and automatically start a case activity or a workflow without mandatory arguments. The case activity or workflow starts if a case fulfills a predefined rule set. The rule set determines which cases to start a case activity or a workflow on and optionally a duration. Rule sets are based on saved searches that you create using WorkZone Client.

> **Prerequisite:** If you want a case monitoring service workflow to start a case activity list that contain SendSmartPost activities, the WorkZone PDF Engine must be installed both on the web server and the agent server. It is not sufficient to install it on the web server only.
>
> The reason for the agent server installation is that when a case monitor service workflow starts a case activity list, the case activity list is started by the agent server that runs the service workflow. If the case activity list contains **SendSmartPost** activities, the SmartPost processes will also be started on the agent server. Because SmartPost processes require the PDF Engine to generate PDF documents, it must be installed on the same server as the case monitor service workflow.

You create and configure Case monitoring service workflows and rule sets in WorkZone Configurator.

You must complete the following steps to set up a Case monitoring service workflow:

1. Create, save, and share saved searches.
2. Create a rule set and one or more rules to add to the rule set.
3. Create a Case monitoring service workflow.

> **Note:** In this release, you can only start one case activity list or one workflow per created case.

Creating rule sets

Rule sets define on which new cases, a case activity or a workflow will start. A rule set consists of:

- Name and description of the rule set and optionally, a start and an end date.
- Rules that are based on saved searches.

Create rule sets

Prerequisite: One or more saved and shared searches. The searches must be shared with the organization. You create, save, share searches using WorkZone Client. See Save and reuse search lists in the WorkZone Client User Guide.

1. Open WorkZone Configurator.
2. Go to **Process** > **Rule sets**.
3. Click **Create rule set**.
4. Enter a name and a description in the **Create rule set** dialog box, and then click **Save**.
5. Click **Create** to create a rule that will be included in the rule set. For each rule that you add, you need to specify the following parameters:

Name	Description
Search	Select a saved search that you want to use to find cases to start a case activity or a workflow on.
Priority	Enter priority, if you have more than one rule in the rule set. The rules will be applied according to the order specified by the priority.
Process	Select which process you want to start. In this release, you can only select case activities or workflows without mandatory parameters.
Duration	Enter the duration of the case activity. The duration is used to calculate the deadline of the case activity. The deadline will be calculated as the time when a case fulfills the rule + the duration. You can use the following relative date and time stamps to specify the duration: d days/dage

Name	Description
	t timer h hours **Examples:** Duration / The process deadline will be... +5d: 5 days after a case fulfills the rule. +2h: 2 hours after a case fulfills the rule. +5d2h: 5 days and 2 hours after a case fulfills the rule. Note that you must write the number of days followed by the number of hours in this order. If you do not specify a duration, the case activity will be started without a deadline. If the duration is invalid, for example +0d, which is now, the case activity is stopped and an error is written in the Event Log.

6. Switch to **Enabled** to start using the rule.

> Important: If you make changes to a rule set, which is already used by a case monitoring service workflow, you must disable the service workflow, wait a couple of minutes, and then enable it again to apply the change. You can check the Event Log to make sure that the service workflow is actually stopped before you enable it again.

Configure a case monitoring service workflow

The Case monitoring service workflow can monitor when new cases are created and then automatically start a case activity or a customized workflow.

Create a case monitor service workflow

You can create a Case monitoring service workflow in WorkZone Configurator. See [Service workflows] in the WorkZone Configurator Administrator Guide.

Configure a Case monitoring service workflow

> **Prerequisite:** You must create one or more rule sets that define on which cases, a case activity or a workflow will start. See Creating rule sets.

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. Point to the **Case monitoring** service workflow that you just created, and click **Edit parameters** to configure the service workflow.
4. Enter values for the parameters.
5. Click **Save**.

Name	Description	Sample value
WatchInterval	The interval in seconds between checking for new cases. A value of 60 - 300 seconds is suitable in most cases.	60
ProcessOwner	The name of the contact that will be assigned as process owner of the case activity or workflow that will be started.	
RuleSet	The name of the set of rules that determines on which cases a case activity will start. If the rules are met, the case activity or workflow starts. See Creating rule sets.	

6. Click **Edit** and turn on **Enabled** to start the service workflow.

Interact connector

KMD WorkZone Interact is a tool that organizations can use to design, create, and maintain digital forms. For more information about WorkZone Interact, please see KMD WorkZone Interact.

The Interact connector is a service workflow that connects to WorkZone Interact and monitors if data is submitted from Interact forms. If this is case, the workflow retrieves the data and performs actions in WorkZone. For an overview of the actions that the Interact connector service workflow supports, see WorkZone actions.

The Interact connector service workflow retrieves data from Interact at an interval that you specify when you configure the service workflow in WorkZone Configurator.

Getting started

Before you can start using the Interact integration, you need to:

- Acquire and install the Interact certificate.
- Create and configure an Interact connector service workflow per form that you want WorkZone to retrieve data from.

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

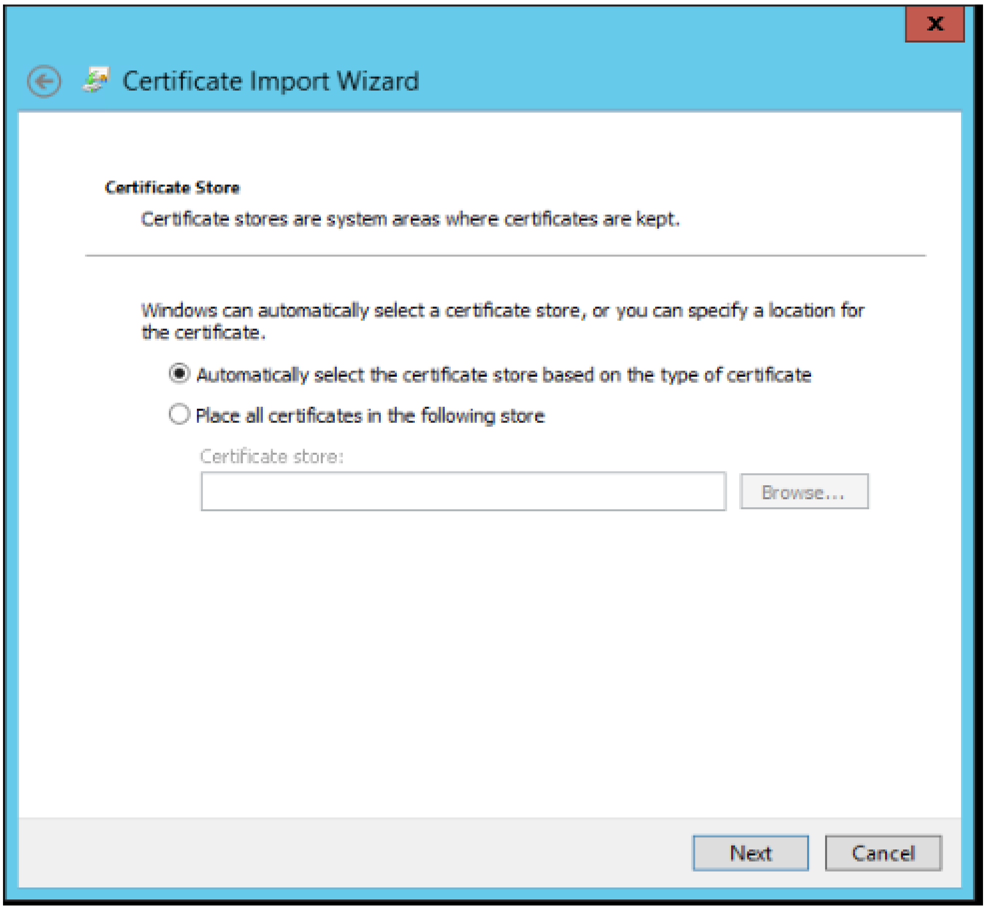
Contact the organization's certificate administrator to get the Interact certificate including the private key that can be used for Interact.

Import the certificate to the certificate store

You need to import the certificate to the certificate store on the WorkZone Process server that runs the Interact service workflow using the **Windows Certificate Import Wizard**. If you have both a web server and agent server, you must install the certificate on both.

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 workflows in the WorkZone Configurator Administrator Guide.

Create and configure an Interact connector service workflow

You can create an Interact service workflow in WorkZone Configurator. See Service work-flows in the WorkZone Configurator Administrator Guide.

You must create an Interact connector service workflow per form that you want WorkZone to fetch data from.

Configure an Interact connector service workflow in WorkZone Configurator

1. Open WorkZone Configurator.
2. Go to **Process** > **Service workflows**.
3. Point to the **Interact connector** service workflow that you have created, and click **Edit parameters** to configure the service workflow.
4. Enter values for the parameters, and click **Save**.

Name	Description	Sample value
WatchInterval	The interval in seconds between checking for new data from Interact. A value of 60 - 300 seconds is suit-able in most cases.	60
Url	Enter the URL for the Interact ser-vice. Depending on whether the con-figuration is made for test or pro-duction, enter one of the two URLs.	Test: https://-preprod-interact-api.mycompany.dk Production: https://interact-api-mycompany.dk
ClientId	The organization's Interact ID, which is defined by ACOS.	mycompany-workzone
CertificateThumbprint	Enter the thumbprint that identifies the Interact certificate.	
FormIds	The IDs of the Interact form that the Interact connector service workflow	800636

Name	Description	Sample value
	fetches data from. You can see the form ID in the Interact client. You can select multiple forms by listing the form IDs separated by a comma. If you do not specify a form ID, data from all forms will be fetched.	
ExecutingUser	Select the user that will be used to create and update cases, documents, and contacts in WorkZone. The user you select as the executing user must have sufficient permissions to perform the actions on cases, documents, and contacts that the Interact forms are designed to do. The executing user's permissions must always be aligned with the functionality of the Interact forms. If you introduce new forms or change existing forms, you should always verify that the executing user's permissions are still valid. **Security group** Interact requires Create, Read, and Update permissions. By default, security group 6 includes these permissions but your organization may have defined the groups differently. For information about security groups, see Apply security groups to users in the WorkZone Installation Guide. **Access codes**	

Name	Description	Sample value
	The selected user must also have the necessary access codes to be able to perform create and update actions on cases, documents, and contacts. The required access codes depend on how your organization has set up WorkZone. If you want Interact to be able to create and update cases, documents, and contacts that are protected with certain access codes, the executing user needs to have the same access codes. For example, if you want to update a case with the access code HR, the executing user will need to have the HR access code applied as well. **Note:** If you run on a corporate access environment, the selected user determines which organizational unit and access code will be applied to a case that is created.	

5. Point to the **Interact connector** service workflow, and click **Edit** .
6. Turn on **Enabled** to start using the service workflow.

Status

You can check the status of processed Interact forms in the Workflow log in the same way as any other service workflow, see Monitoring WorkZone Process in the WorkZone Operations

Guide. In addition, you can see the status in the Interact app. In Interact, go to **Submitted dialogues**. The table below describes what the Interact status means in WorkZone context.

Interact status	What does it mean in WorkZone?
Delivered	The form has been submitted for handling in WorkZone.
Temporary blocked	An error has occurred when creating an error case in WorkZone. See Error cases. If a submission has this status, it means that some WorkZone setup is missing or wrong, for example there is no access to OData or the default case group that are automatically assigned to error cases is no longer valid.
Imported	The submission was successful and has been processed in WorkZone or an error case has been created in WorkZone.

WorkZone actions

The table below lists the actions that the Interact connector service workflow can perform in WorkZone based on data that is retrieved from Interact forms. The Interact connector service workflow supports:

- Creating new cases
- Updating existing cases

In both scenarios, information from the Interact form is inserted into the corresponding fields on the case. If documents are attached to the Interact form, they are added to the case. In addition, two system generated documents are always added to the case:

- A PDF document–A user-friendly representation of what the user submitted through the Interact form.
- An XML document–This is the corresponding technical document, which contains the same content and additional meta data about the submitted data. This document is added as a supplementary document to the PDF document.

Note: If you have mapped meta data on documents, this mapping will also apply to the system generated PDF and XML documents. If you have not mapped any meta data to documents, the default values will be used. The default values for the two documents are the document type **DOK, Document** and the document state **ARK, Archive**. If the Interact submission contains invalid mapping and it results in creation of an error case, the PDF and XML documents will be added to the error case with default values and not the values from the mapping. See View Interact connector errors.

The table below provides an overview of the actions that the Interact connector service workflow supports.

Action	What happens?
Insert data from fields	Data from the Interact form is inserted into the corresponding fields on the case, attached documents, and to new contacts that are added. This action applies to both standard and custom fields on cases, but only standard fields are supported on documents and contacts.
Add documents	Documents that are attached to the Interact form are added to the case. The documents are created with the document title that the user has specified in the form. The title will be applied to all attached documents. If the title is not specified, the file names of the attached documents will be used as document titles.
Add a new contact	If the contact does not exist in WorkZone, a new contact is created and assigned as a party on the case. The party will be assigned the role **Case party** (Sagspart) by default. It is not possible to change the configuration of the default role. The contact is created based on the type that the user has specified in the Interact form, for example persons with CPR or companies with CVR. Note that if you see the following error message: *"Failed to construct OData Entities. Check OData property names. (Custom label Sagspart with the type equal to SP does not exist in the database.)"* It means that the **Case party** role that was assigned has an end date. You must remove the end date to solve the issue.
Add a contact as a	If a contact already exists in WorkZone, the contact is added as a party on the case. Existing contacts are identified on the basis of the **NameCode** and

Action	What happens?
party on a case	**NameType** fields. This means that these fields must be mandatory in the Interact form. **Note:** In this release, parties cannot be removed from the case.
Update an existing case	If a user submits an Interact form that contains a file key (FileKey or FileNo) that exists in WorkZone, the following happens: • If new documents are submitted with the Interact form, they are added to the case. • If new contacts are submitted with the Interact form, they are added as new parties on the case. • New XML and PDF documents are added. • A new Interact reference ID is added on the **Information** tab on the case in WorkZone Client. The reference ID refers to the a specific submitted dialogue in Interact.

Mapping fields in Interact forms to data

This section provides basic introductions on how to map fields in Interact forms to WorkZone data. For more information about creating Interact forms, refer to the Interact documentation.

To map data in Interact, you need to know the WorkZone OData entity names and field IDs. If you are not familiar with the WorkZone data model, you can use WorkZone QueryBuilder to help you find the entity names and IDs.

Supported entities:

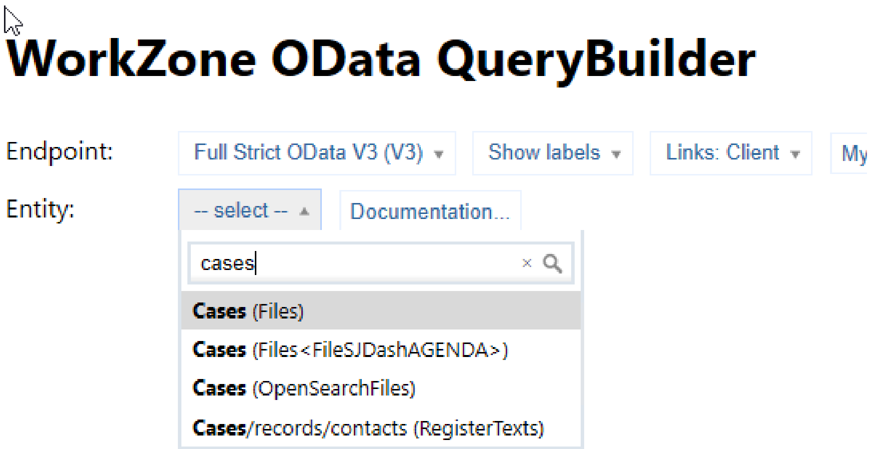
- Files (Cases/Sager)
- Records (Documents/Dokumenter)
- Contact (Contacts/Kontakter)
- AddressMains (address_main/address_main)

Identifying OData entity names and IDs using WorkZone QueryBuilder

You can use WorkZone QueryBuilder to find the IDs that you need to know to be able to map fields in Interact forms to WorkZone data. You can either click the **Documentation** button in WorkZone QueryBuilder to get an overview of fields by entity or you can look up entities and fields using WorkZone QueryBuilder.

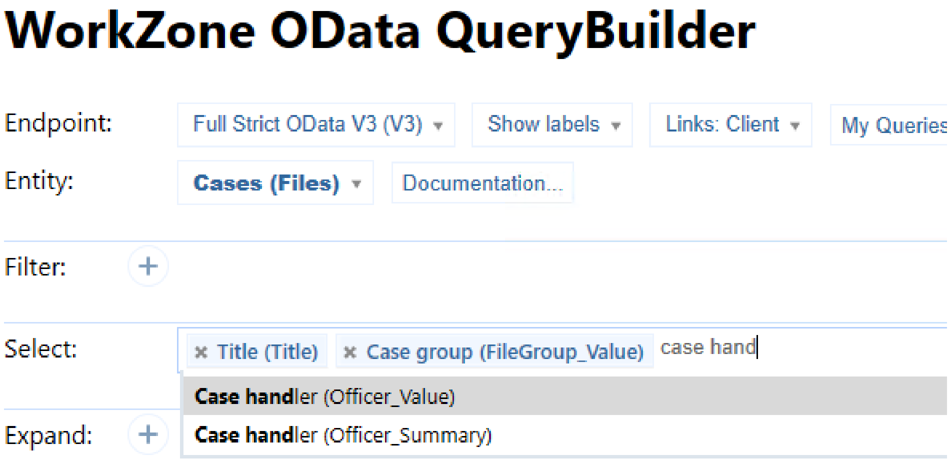
Look up entities and fields

1. Open WorkZone QueryBuilder.
2. Select an entity. You can search for the label, for example **Cases** or **Sager** depending on the language setup. If you search for the **Cases** label, you will see the OData entity name in brackets **Cases (Files)**.



3. Select fields. You can search for the labels of the fields, for example **Title** or **Titel**, **case group** or **sagsgr.**, **Case handler** or **Sagsbeh.**, and so on. You will see the OData field ID in brackets. In this example, **Title (Title)**, **Case value (FileClass_ Value)**, and **Case handler (Officer_Value)**. The name in the bracket is the ID that

you need for the mapping.



Note:

- You can only use fields of the type _Value, not _Summary.
- Labels in your organization may be named differently.

Some fields are mandatory and some fields have dependencies on each other. See Mandatory fields and dependencies.

Mapping in Interact

Set up OData access

To access OData from the Interact server, follow these steps:

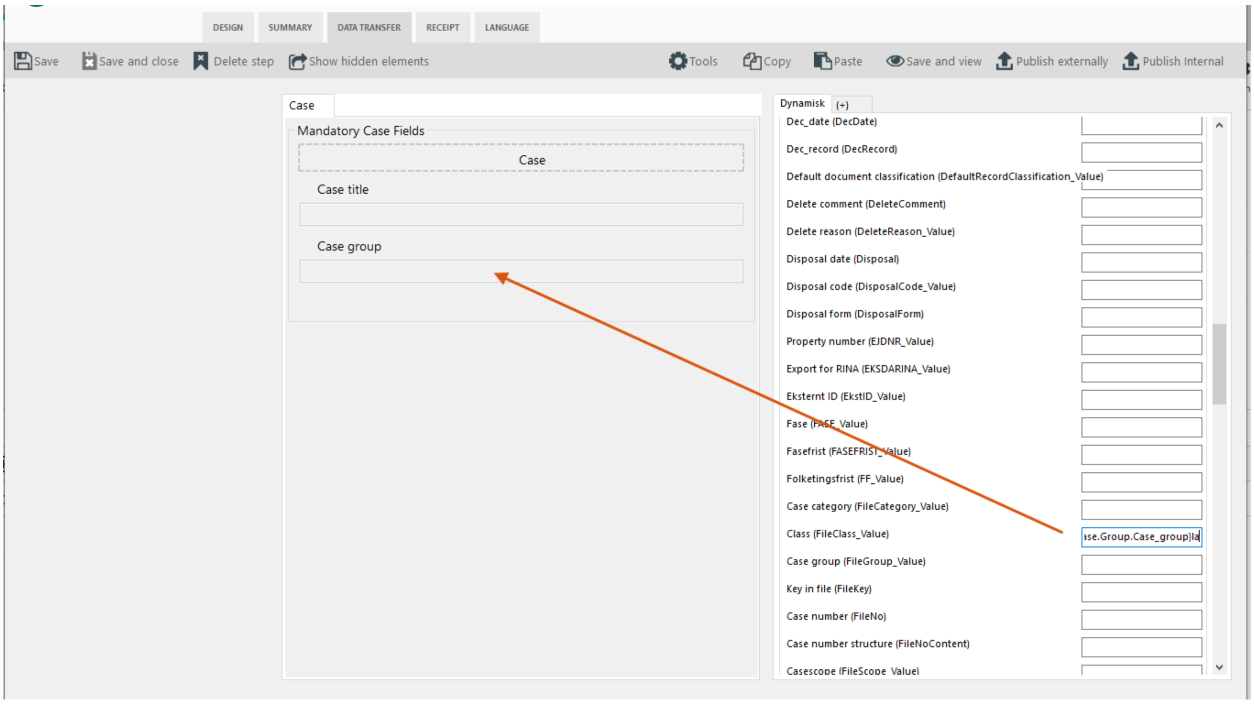
1. In the hosts file (on the interact server), add an entry with the IP address of the WorkZone server mapped to the host name of the WorkZone server.
2. In Interact, click **Settings** > **Integration**. In the OData section, use the host name in the **URL** field.
3. To verify access to OData. open a browser on the Interact server and paste the URL of the WorkZone server, for example https://[host]/odata. If you receive an OData XML response, the access is provided.

Map fields

1. Open the Interact form.
2. Click the **DATA TRANSFER** tab.
3. On the Dynamic tab, select the **Activate delivery** check box.
4. Select the WorkZone entity you want to use, for example **Cases (Files)**, and click the **+** button.

> Tip: The list is sorted by the OData field IDs in the brackets.

5. Find the ID of the field you want to map in the list, for example **Class (FileClass_ Value)**.
6. Click in the field next to the ID that you want to map. In this example **Class (FileClass_Value)**.
7. Press the Ctrl key and click in the field in the form that you want to map the ID to. In this example the **Case group** field.



Mapping examples

Set a contact as primary party on a case

To set an existing contact as the primary party on a case at case creation, you must map the following fields in Interact:

- **NameCode**
- **NameType_Value**, for example 'M' for Employee.
- **NCustomLabel_Value**. Optional, if you want to specify the role, for example 'Sagspart'.

Mandatory fields and dependencies

Some fields are mandatory and some fields have dependencies to each other. Below you will find an overview of standard entities, mandatory fields, and dependencies between fields. If a field is mandatory, it must have a value. You can either specify a default hard-coded value in Interact Designer or you can make the field mandatory in the Interact form for end users to fill in.

> Important: If mandatory fields are left empty, the Interact Connector service workflow will fail to retrieve the data and perform actions in WorkZone.

Action: CREATE

Entity ID: Files

The Files entity defines meta data on cases.

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Files	Sager	Cases	Title	Titel	Title	-
			FileClass_Value	Sagsgrp.	Class	-

Guidelines:

- Cases can be created separately without any other entities (such as documents or contacts). In this case, do not map fields of other entities in the form.

Entity ID: Records

The Records entity defines meta data on documents.

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Records	Dokumenter	Documents	Title	Titel	Title	Attachment file name
			State_Value	Tilstand	State	
			RecordType_Value	Dokumenttype	Document type	

Guidelines:

- Documents can be created only in relation with a specific case. If the form lacks mapping for mandatory **Files** fields, the document creation will fail.
- The form must not contain mandatory mapped **Contacts** or **AddressMains** fields that are not filled in either with a hard-coded value or by the user when filling in the form. Mandatory fields cannot be empty.

Entity ID: Contacts

The Contacts entity contains meta data on contacts.

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Contacts	Adressater	Contacts	NameType_value	Adressattype	Contact type	-
			NameCode	Adressatkode	Contact code	-

Guidelines:

- Contacts can be created only in relation to a specific case. If the form lacks mapping for mandatory **Files** fields, the contact creation will fail.
- The form must not contain mapped **AddressMains** fields that are not filled in either with a hard-coded value or by the user when filling in the form. Mandatory fields cannot be empty.
- Filling only mandatory fields will create a contact without a name and with an empty main address field.

NameCode is mandatory for some contact types, for example:

- C (Person with CPR)
- J (Company with CVR)

And not mandatory for some other types, for example P (Person without CPR) and F (Companies without CVR).

Entity ID: AddressMains

The AddressMains entity contains contacts' main addresses.

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
AddressMains	Address_main	Address_main	AddressType_Value	Adressetype	Address type	-

Guidelines:

- Main address can be created only in relation to a specific contact. If the form lacks mapping of mandatory **Contact** fields, the main address creation will fail.
- Filling only the mandatory field will create a main address without an actual address.
- AddressType_Value should always be HA - main address.

Mapping of additional addresses is supported (entity ID: Addresses) but for the mapping to work you must make sure to map the main address first with the value HA. Additional addresses must not be of the type HA.

Action: UPDATE existing case

Entity ID: Files

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Files		Cases	FileKey or FileNo	Surrogatnøgle i SAG.	Key in file	-

Guidelines:

- All case fields sent in such a form will update values on the case that already exists in the database with the mentioned FileKey or FileNo.

Entity ID: Records

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Records	Dokumenter	Documents	Title	Titel	Title	Attachment file name
			State_Value	Tilstand	State	ARK
			RecordType_ Value	Dokumenttype	Document type	DOK

Guidelines

- No mandatory **Records** fields are required to be mapped. Mandatory values fall back to default values.
- Documents will be created on the case that already exists in the database with the mentioned FileKey or FileNo.

Entity ID: Contacts

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
Contacts	Adressater	Contacts	NameType_ value	Adressattype	Contact type	-

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
			NameCode	Adressatkode	Contact code	-

Guidelines:

- If a contact with the combination of **NameType_value + NameCode** is found in the database, its main address will be linked to the case that already exists in the databases with the mentioned FileKey or FileNo. No values Contact/adressMains will be changed (only linked to case).
- If a contact with the combination of **NameType_value + NameCode** is NOT found in the database, an attempt of creation of a new contact will be performed (with all values filled in for Contact/addressMains).

Entity ID: AddressMains

Entity ID	Entity label (Da)	Entity label (En)	Mandatory field IDs	Field labels (Da)	Field labels (En)	Fallback value
AddressMains	Address_main	Address_main	AddressType_Value	Adressetype	Address type	-

Guidelines:

- Do not add AddressMains mappings if you are <u>not</u> expecting it to be filled in (otherwise it will fail the dialogue submission).
- AddressType_Value should always be HA - main address.

View Interact connector errors

If retrieval of data from an Interact form fails, for example if fields in a form are mapped incorrectly in Interact, mandatory fields have not been filled in by the user, or fields cannot be found, a case is created with the error text shown in the **Case text** field. An error will also be returned to the Interact app.

Error cases

The cases that contain error messages are created with the title [INTERACT ERROR] and with the case group that is configured as the default case group in WorkZone Configurator. By default, it is SJ-TEMP but your organization may be using another case group.

The case contains the following information that can assist you in identifying the form in question and fixing the error:

- An error message in the **Case text** field.
- The PDF document with the content of the submitted form.
- The name of the form that caused the error in file name of the PDF document.
- The Interact reference ID on the **Information** tab.

For a better overview, you can create a search list in WorkZone Client that shows the Interact error cases.

Create a list of error cases

1. Search for cases with the title **[INTERACT ERROR]** in the **Title** field and the information type **Interact Ref. ID** in the **Information** field.
2. Save the list.
3. Add it to the navigation pane on the **Home** tab in the WorkZone Client. You can see the list under **My lists** in the **Available lists** pane. See Manage saved search lists in the WorkZone Client User Guide.

In addition to checking the error cases, you can check the workflow log to find out why the Interact service workflow failed. See Investigate failed processes in the workflow log in the WorkZone Operations Guide.

> **Tip:** You can set up a Process monitor service workflow to monitor whether processes fail. If an Interact service workflow fails, the process owner will by notified by an email. In this case, the process owner is the user you have specified in the **InteractUser** parameter when you configured the Interact service workflow. See Process Monitor and Create and configure an Interact connector service workflow

Troubleshooting Interact connector

Click an issue below to see the solution or workaround.

"Feltet 'Nøgle i sag' (db name = file_key) validerer mod register 'file', men system nøglen 149067 findes ikke i registeret."

Message in Danish: "Feltet 'Nøgle i sag' (db name = file_key) validerer mod register 'file', men system nøglen 149067 findes ikke i registeret."

If you get this message in the workflow log (WzpWorkflowLogs), it is probably because the user that is configured as the Interact executing user does not have an access code that allows creating cases in the selected case group. To solve this issue, assign the same access code that is configured for the case group to the executing user.

See ExecutingUser parameter.

Configuring SmartPost

The SmartPost package is an add-on package that supports sending messages from authorities, companies, and organizations to case parties in WorkZone as well as receiving replies to messages from case parties in an authority's or company's digital mailbox.

SmartPost prerequisites

Before you start setting up SmartPost, there are some prerequisites that need to be in place.

e-Boks and Strålfors certificates

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 administator 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.

Digital mail Prerequisites

Before you start the installation of the SmartPost process, you need to complete some configuration tasks for SmartPost to be able to communicate with 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: https://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.

Value name	Value	Description
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 person	Customer specific	The phone number on which the contact person can be contacted.

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

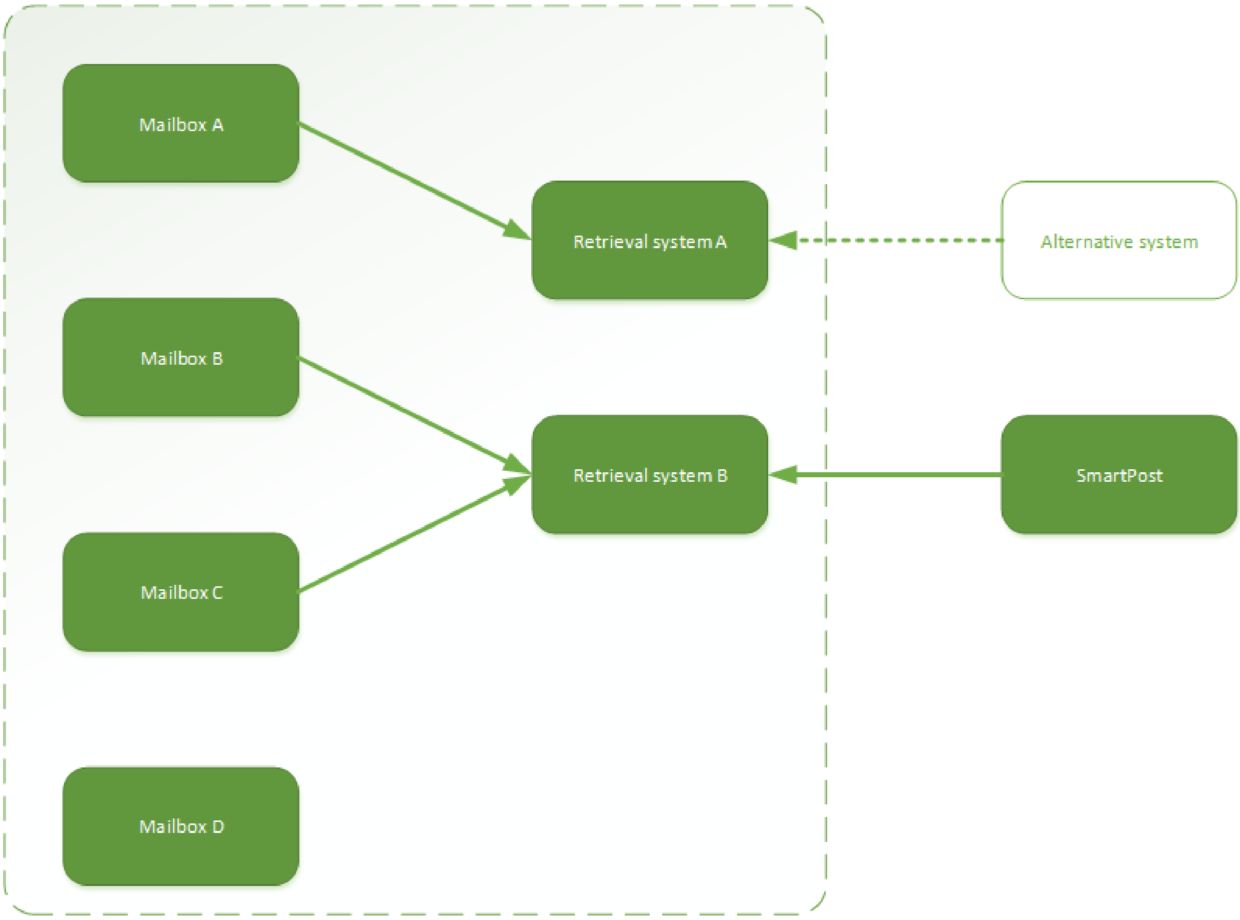
The organization needs to create at least one mailbox at e-Boks in which messages from citizens or an organization can be gathered, before they are collected by the SmartPost retrieval service. Subsequently, the mailbox needs to be connected to the Retrieval system.

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 organ-ization”	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.

Remote print

Before you can start setting up and configuring remote print, the organization must make an agreement with the selected print center, Strålfors or KMD Printcenter.

Strålfors agreement

Before you can start to use Strålfors Connect for remote print, 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 Configure remote print.

OneTooX agreement with KMD Printcenter

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.

See also Configure remote print.

Configure digital mail

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.

Note: SmartPost supports Digital Post 1 and 2.

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 certificates to SmartPost .

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 Digital Post Administration portal, you need to configure SmartPost to reflect the configuration of the dispatch system. See Configure SmartPost for sending messages.

For information about creating a dispatch system, refer to Vejledninger Digital Post from Digitaliseringsstyrelsen.

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.

Configure 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

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 certificates to SmartPost .

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

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

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.

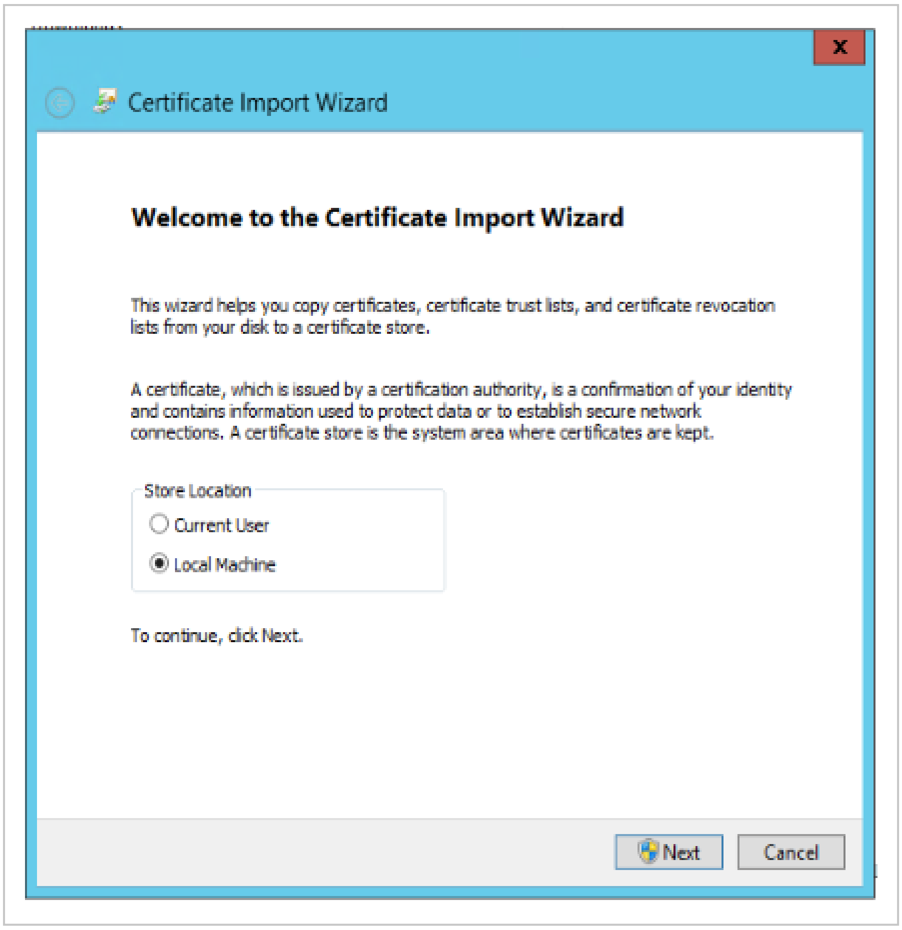
The employee starts the certificate process using the Nets link: https://www.nets-danid.dk/produkter/funktionssignatur/bestil_funktionssignatur/ and follow the instructions. When the process has been completed, the employee will receive an email with an installation code and a link to start the installation 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.

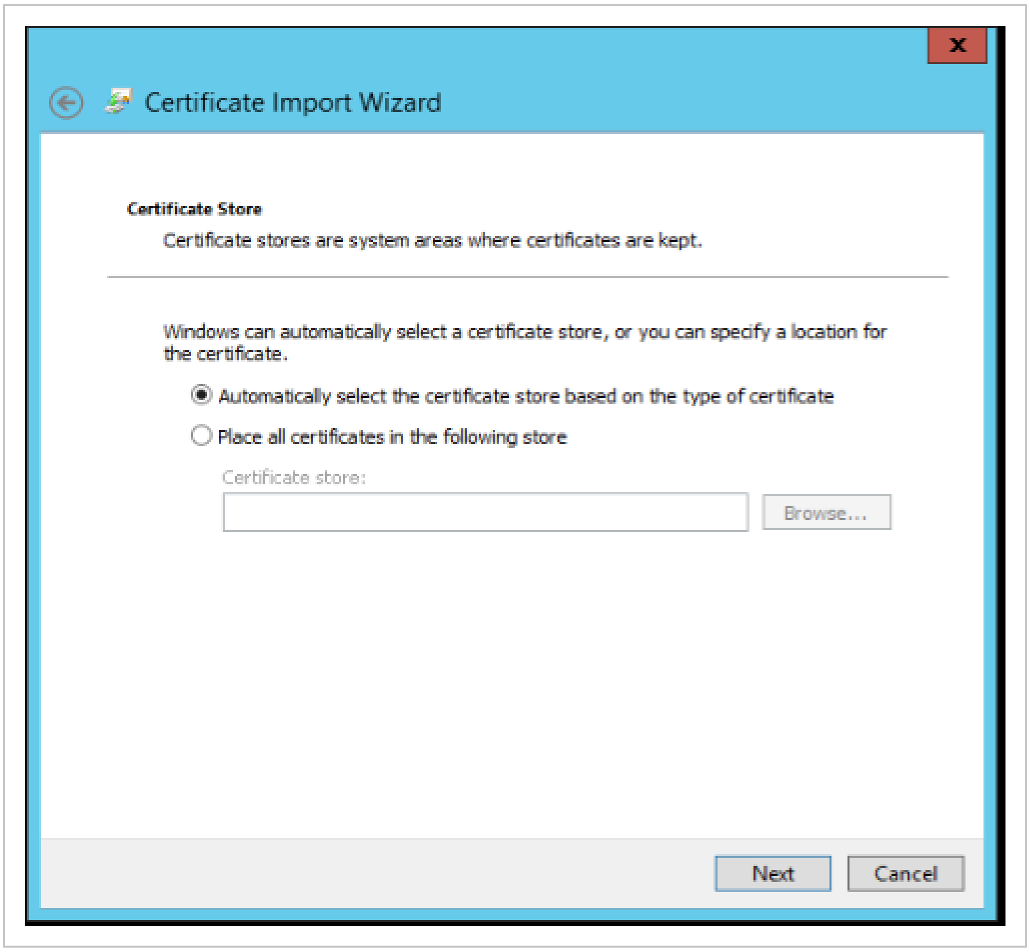
Import the certificate in to the certificate store

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

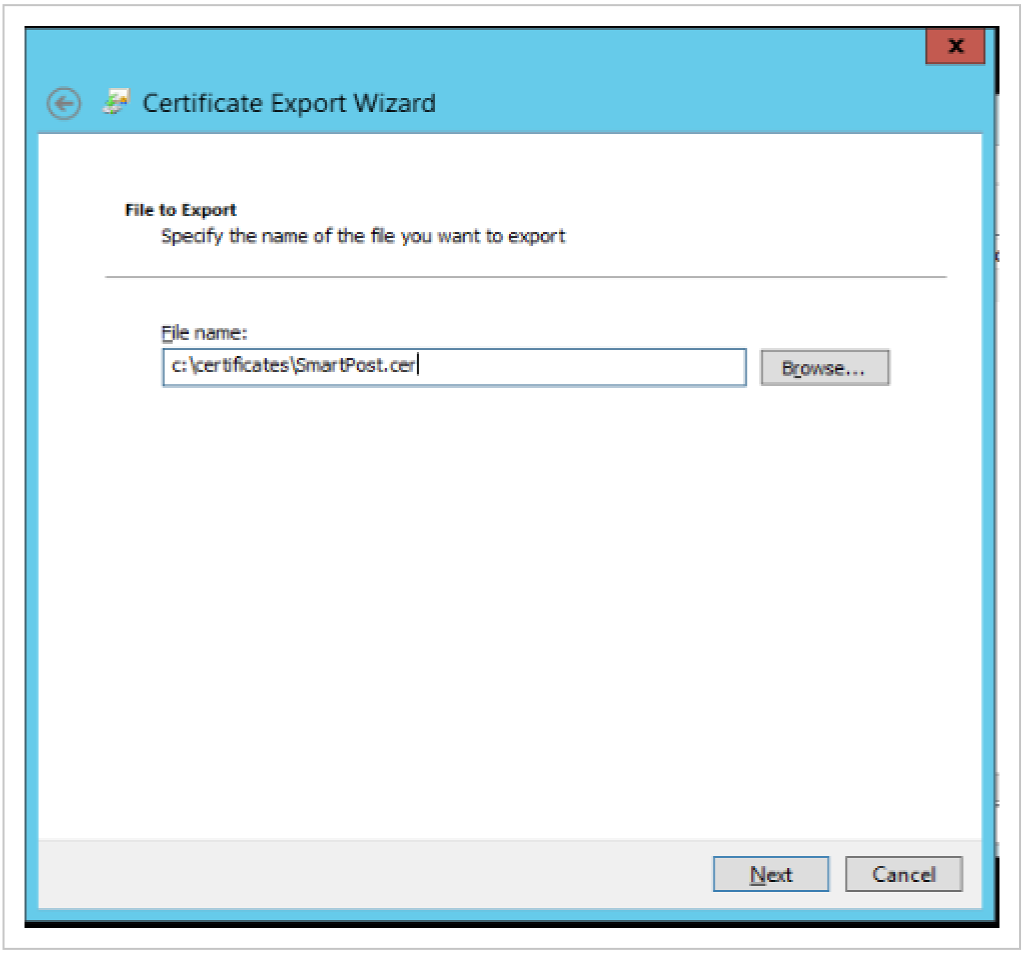
You must add the private key of the IIS user that runs the WzpSvc app pool, typically that is **IIS APPPOOL\WzpSvc**, to the SmartPost certificate. This is done in the **Certificate Manager**. See Apply certificates to SmartPost .

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.

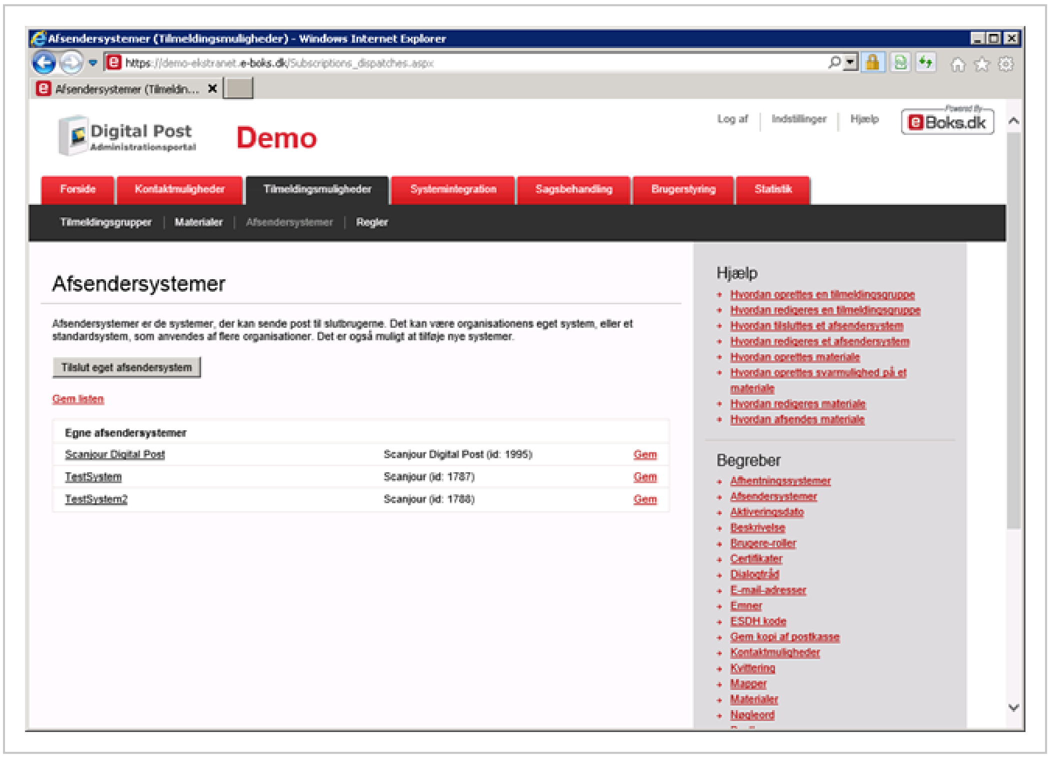
Upload certificate

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

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

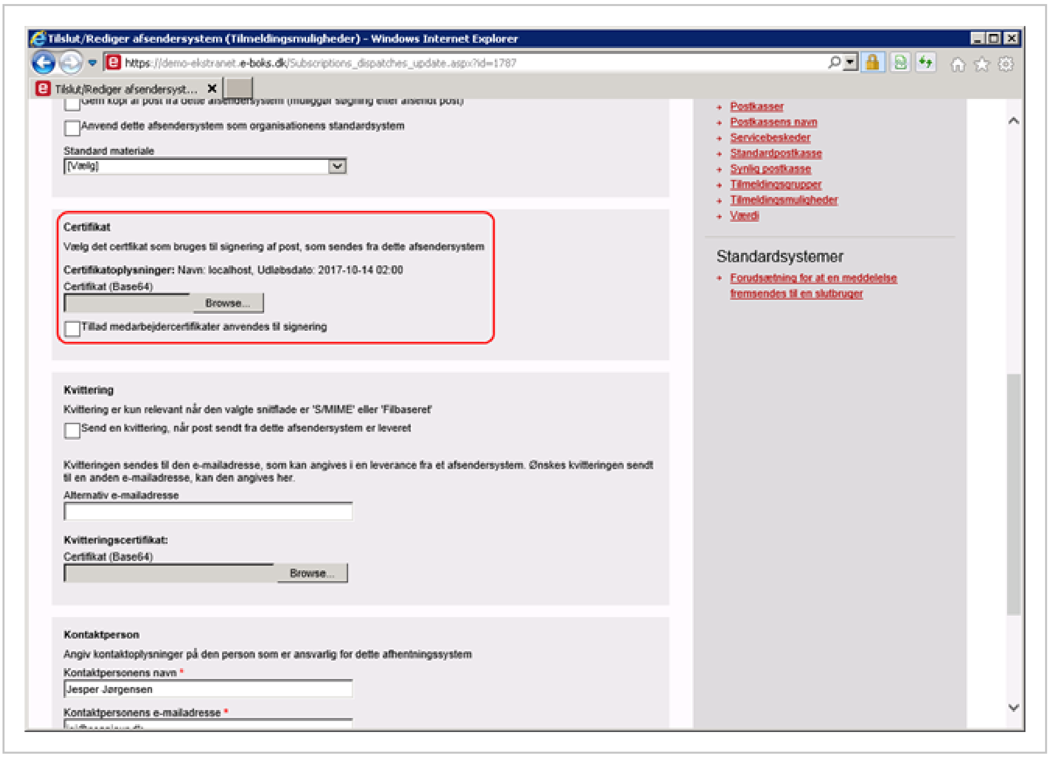
   Production: https://ekstranet.e-boks.dk

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 Administrator Guide.

Apply certificates to SmartPost

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

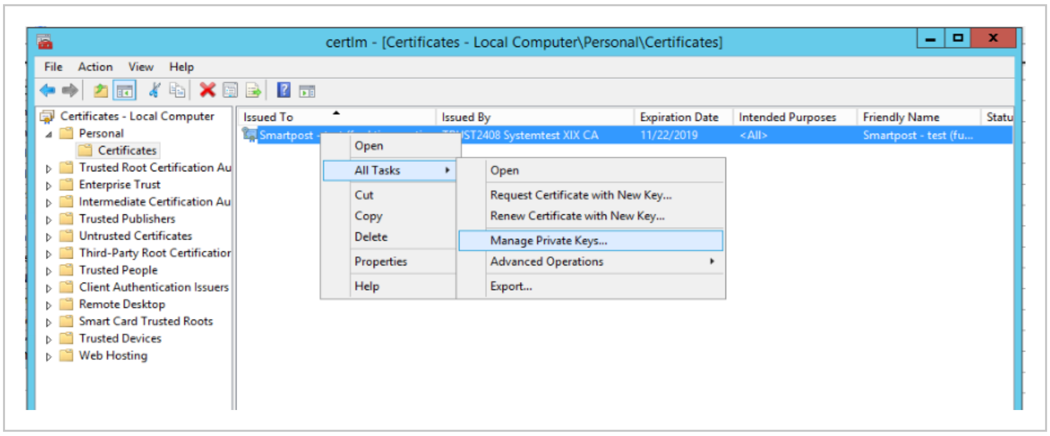
- Add the private key of the IIS user to the dispatcher certificate.
- Apply the certificate to the SmartPost dispatcher.

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

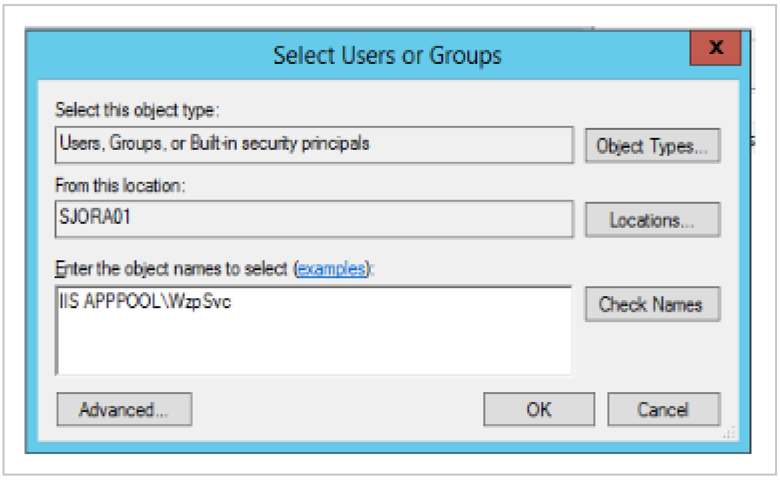
For the dispatchers, such as e-Boks and Strålfors, to work with SmartPost, you must add the private key of the IIS user that runs the WzpSvc app pool to the dispatcher certificates. Typically this is an **IIS APPPOOL\WzpSvc** user. This is done in the **Certificate Manager**. You need to locate the dispatcher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

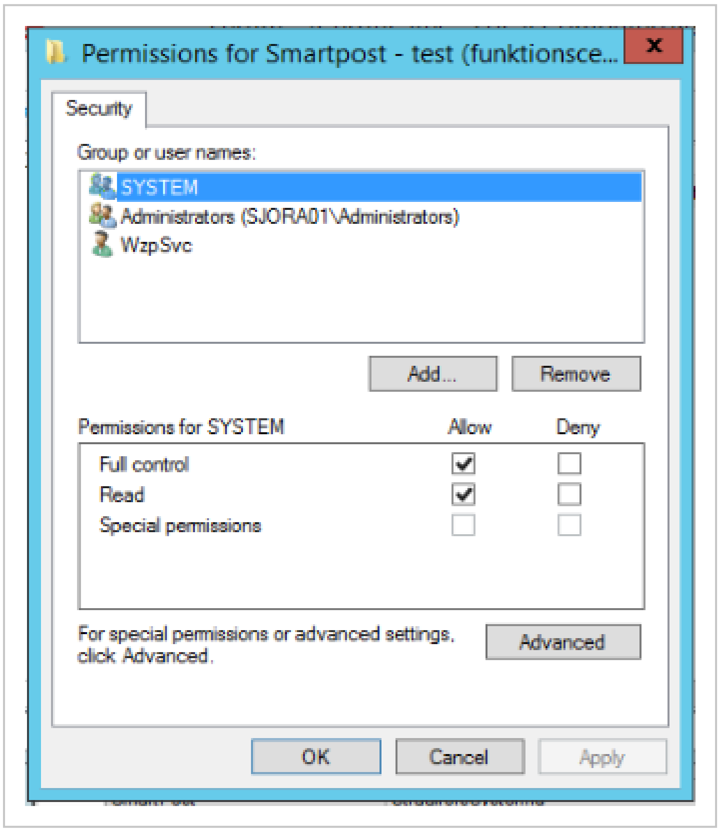
> Important: You need to re-add the private key after upgrading WorkZone Process.

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.



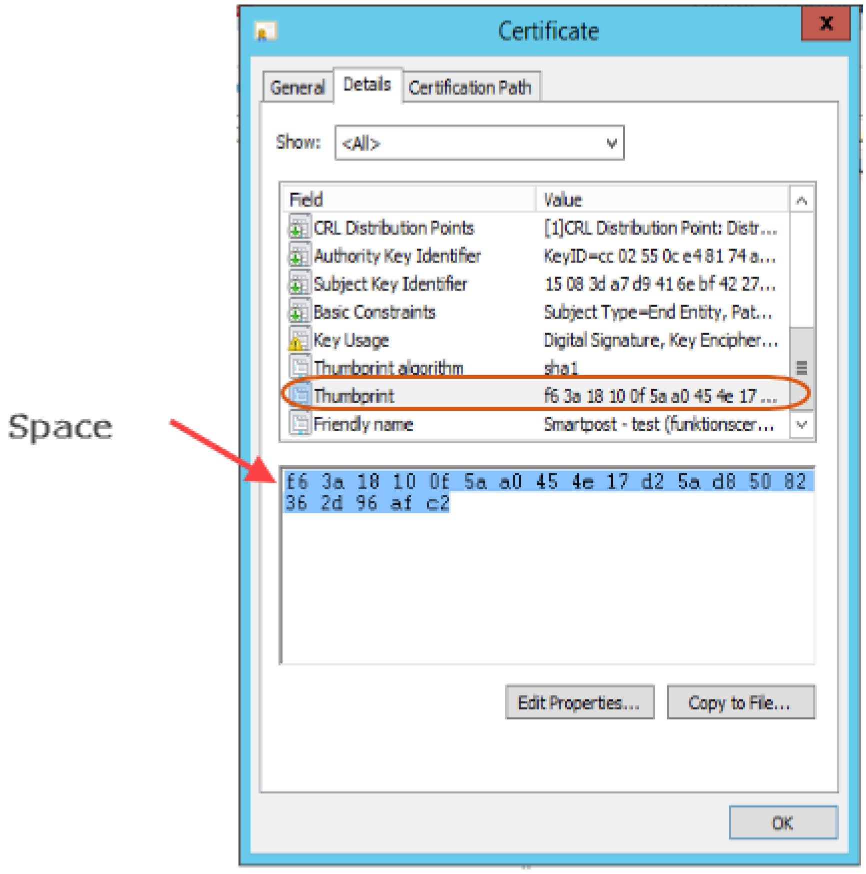


Copy thumbprint and apply the certificate to the dispatcher

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 **EboksCertificateThumbPrint** field.

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

Configure SmartPost

You configure SmartPost in WorkZone Configurator.

1. In WorkZone Configurator, go to **Process** > **Processes**.
2. Point to the **SmartPost** process.
3. Click **Edit process parameters**.
4. Enter values for the parameters.

Parameter	Default	Description
CopyCoverPageRecordId		The template that is used to create cover pages for copy recipients. If you leave the field empty, a default standard cover page will be used. The template must be saved in WorkZone. For more information about cover page templates, see Configure templates.
ProtectedCoverPageRecordId		The document that will be used as template for creating cover pages for copy recipients with protected addresses. If you leave the field empty, a default standard cover page will be used. The template must be saved in WorkZone.

Parameter	Default	Description
		See Configure templates.
DefaultMaterialId		The e-Boks material that will be selected by default in the **Send SmartPost** dialog box. To configure e-Boks materials, click **Process** > **E-boks material**. See Configure e-Boks materials and e-Boks materials in the WorkZone Configurator Administrator Guide.
AllowedNameTypes	CPJV	Select which contacts the users can select as recipients or copy recipients in the **Send SmartPost** dialog box. Allowed contact types are: C - Persons with CPR P - Persons without CPR J - Companies with CVR V - Production units with CVR
SPDocumentSource		Select the origin of the created SmartPost message. The possible settings correspond to the entries in the custom domain ACTOPR, for example SP, SmartPost, DP, Digital Post, and so on. The organization must provide this information. The setting is shown on the document in the **Origin** field in WorkZone Client.
MaxCombinedMessageLength	10485760 (10 MB)	When a user starts a SmartPost pro-

Parameter	Default	Description
		cess, SmartPost calculates an estimated size of each of the messages sent to the recipients. Before SmartPost continues the process, the estimated size is compared with the **MaxCombinedMessageLength** setting. If the estimated size exceeds the specified value, the user is asked to reduce the size of the documents and then try to send the message again. The reason for this is that large documents may cause the Workflow Host to run out of memory later in the flow, which causes workflows to be terminated without the user being notified. Generally, the default value is used.
DefaultDispatcherSequenceId		The default dispatch sequence that will be selected by default in the **Send SmartPost** dialog box. To configure dispatch sequences, click **Process** > **Dispatch sequences**. See Configure dispatch sequences and Dispatch Sequences in the WorkZone Configurator Administrator Guide. **Important:** Verify this value after successful installation. After installation, the dis-

Parameter	Default	Description
		patch sequences may have been renumbered.
DefaultRemotePrintTypeId		The print type that will be selected by default in the **Send SmartPost** dialog box. To create or reconfigure print types, click **Process** > **Print types**. See Configure remote print and Print types in the WorkZone Configurator Administrator Guide.
StandardLetterFileNo		The case number of the case that contains standard letters. See Configure standard letters.
ReportID		Select the report you want to use for the history document.
RecordType	PROHIST	The document type of the history document that is generated by the SmartPost process.
RecordState		The document state of the history document that is generated by the SmartPost process.
CopyWatermark	Copy	The text that will be used as watermark on copies. The maximum length of the watermark is 60 characters. If the text exceeds 60 characters, the text will be cut.
TitleTemplate	{0}: {1} {2}	A template that is used to create the title of the history document. By default, the template has place-

Parameter	Default	Description
		holders for the process type {0}, the process title {1}, and a date stamp {2}.
ApprovalEnabled	Turned on	Shows or hides the **Approval** check box in the **Send SmartPost** dialog box. The parameter is turned on by default, which means that the user can select the **Approval** check box. You can turn off this parameter if your organization does not use the approval step in the SmartPost process.
RemergePDFEnabled	Turned off	Re-merges the **Letter date** field in PDF documents when SmartPost messages are previewed or approved. Turn on this parameter if you want the letter date in the PDF documents to be updated with the preview or approval date before sending the SmartPost messages. The **Letter date** field on the meta data of the PDF document will also be updated with the date of approval. The letter date of the original letter document is not changed.
ValidationProperty		Select the custom document field that holds the values.
ValidationValues		Specify which custom document values are allowed. Users will only be able to select documents (letter

Parameter	Default	Description
		document and attachments) with these values in the **Send SmartPost** dialog box.
DocClassificationThresHold		The maximum document classification that is allowed to be used with SmartPost. Documents with higher classifications than specified for this parameter will not be available for selection in the SmartPost dialog box.
AllowSendingSeparateDocuments		Tun on this parameter if you want to allow that users send attachments as separate PDF documents in messages when using the e-Boks dispatcher. A **Send attachment as separate documents (only e-Boks)** check box will be shown in the **Send SmartPost** dialog box. By default, this parameter is turned on. The parameter is closely connected with the **MergeAllDocuments** parameter.
DefaultSendSeparateDocuments		Turn on this parameter if you want the **Send attachment as separate documents (only e-Boks)** check box to be selected by default in the **Send SmartPost** dialog box.
MergeAllDocuments		The parameter only has effect if you have turned on the **AllowSendingSeparateDocuments** para-

Parameter	Default	Description
		meter. If turned on, the SmartPost message will include: • The letter and attachments in one PDF document. • The attachments as separate PDF documents. If turned off, the SmartPost message will include: • The letter in a PDF document. • The attachments as separate PDF documents. Note that messages sent to recipients with protected addresses will not include a cover page, if this parameter is turned off. By default, this parameter is turned on.
SendAttention		Turn on this parameter if you want to send a task that will notify the process owner about a failed dispatch. By default, this parameter is turned on.
TerminateOnFailedDispatch		Turn on this parameter if you want to set the state of failed SmartPost dispatches to **Terminated**. By default, this parameter is turned

Parameter	Default	Description
		off and failed dispatches get the status **Completed**.
AllowOfficeRemerge		Turn on this parameter if the content controls have already been merged in Word and you want to merge the content controls again when sending the message. For example, a case handler has merged address content controls in a letter document in Word but want to send the letter to multiple recipients. In this case, the address content controls will have to be merged again to insert each of the recipients' address information in to the different letter documents. **Note:** An empty content control in Word that results in a blank line will be removed and is therefore not remerged. By default, this parameter is turned off.
PdfFailIfOutOfBounds		Turn on this parameter if you do not want to send messages that include documents with content that do not fit to the page, for example, a Word document with a table that exceeds the page bounds. If the parameter is turned

Parameter	Default	Description
		on, the PDF conversion will fail and thus the dispatch will fail. The history document will show an error message. By default this parameter is turned off. Documents will be converted to PDF despite the content being out of bounds and the message will be sent.

See also Processes in the WorkZone Configurator Administrator Guide.

Configure CPR and CVR

When the SmartPost process sends or receives messages, it identifies the sender in the messages based on the addresses.

In WorkZone Configurator, two parameters, **PartyIdentifierSources** and **ContactAddressKeySources**, are used to identify sender information.

- In WorkZone Configurator, click **Process** > **Process settings**.

Parameter	Description
PartyIdentifierSources	Specifies where the SmartPost sending process looks up sender information such as CVR or CPR numbers.
ContactAddressKeySources	Specifies where the receiver workflow looks up sender addresses based on the CVR and CPR numbers provided by e-Boks. For example, for the purpose of linking the received documents to the addresses of the senders.

The values of these settings are XML elements that identify where SmartPost looks up sender information. By default the standard location of CPR and CVR data is specified in the XML elements.

Handling multiple addresses in received messages

When SmartPost receives a message with a CPR or CVR number, the CPR or CVR number may be connected with several contacts and addresses. The e-Boks receiver workflow retrieves the data and registers the contact information on the contact that is associated with the document that is created when a message is received. The following rules apply:

- **If no addresses are found**, no parties are associated with the document.

  Example

  An unsolicited message with an unknown identifier is received. No contacts can be identified based on the CPR or CVR number because the contact does not exist as a WorkZone contact. Therefore, no parties are associated with the document that was created.

- **If only one address is found**, the contact is associated with the document using this address . The role **Sender** (**Afsender**).

  Example

  An unsolicited message is received. It has a known identifier (CPR or CVR number), which is associated with one contact with one address. This is the simple situation, for example when a small business or a person sends a message from e-Boks. The address is used to create a party on the document with the role **Sender**.

- **If two or more addresses are found**, no parties are associated with the document. An information field is added to the document, which informs the user about the number of addresses found. Based on the information in this field, the user can make a query for documents created by this situation, and then do corrections manually. By default, the custom label is named MULTIADDR but it is configurable.

  Example

  An unsolicited message is received. It has a known identifier with one contact with multiple addresses. One contact is identified with several active addresses. The message is from a company where multiple addresses are registered in WorkZone.

  No contacts will be associated with the document. The MULTIADDRESS information field is added to the document and shows the number of addresses found.

Example

An unsolicited message is received. It has a known identifier with multiple contacts with multiple addresses.

Multiple contacts can be identified from the identifier. There are multiple addresses associated with the contact. For example a large company where WorkZone Client has registered the same CVR number on multiple contacts, where each contact has a unique P-number (production unit), for example subsidiaries of the company. Some of the production units have several addresses registered in WorkZone.

No contacts will associated with the record. The information field MULTIADDRESS is added to the document and shows the number of addresses found.

CPR and CVR data in other locations

Some organizations store CPR and CVR data in other locations than the default WorkZone location. In this case, you can set up the SmartPost process to look up data in these locations by customizing or extending the XML elements in the **PartyIdentifierSources** and **ContactAddressKeySources** parameters in the **Process settings** in WorkZone Configurator.

For example, your organization may store CPR data in a custom field in the **Contacts** register rather than using the standard **ID** field. In this example, you must:

1. Create a new contact type in the WorkZone database. Note that you can view and edit contact types in WorkZone Configurator but you cannot create contact types. You must add new contact type to the `Contacts` register.
2. Create a custom field in WorkZone Configurator to hold the CPR number.
3. In WorkZone Configurator, go to **Process** > **Process settings** and add a new `<party-identifier-source>` element to the XML in the **PartyIdentifierSources** parameter. You can copy an existing `<party-identifier-source>` element and modify it to match the new storage of CPR numbers.

   In this example, the new contact type (`name-type`) has the code `8`, the custom field has the code `CPR_Value`.

<party-identifier-source name-type="8" class-s="WorkZone.Dispatcher.Base.ODataPartyIdentifierSource">

<register-name>Contacts</register-name>

<query-template>?$filter=ID eq '{}'&$select=CPR_Value,NameType_Value</query-template>

<field-name>CPR_Value</field-name>

</party-identifier-source>

Parameter	Description
name-type	Code of the contact type.
register-name	The name of the register that the OData query will be based on.
query-template	The template that used to form the OData query. When the `GetPartyIdentifier(string, ODataService)` method is invoked, then two empty curly braces (`{}`) will be replaced with the party identifier, which is the first parameter in the method. You can specify a search criteria in the filter part of the query.
field-name	The name of the field which content will be returned by the method. The field is expected to contain the code of the Party Identifier.

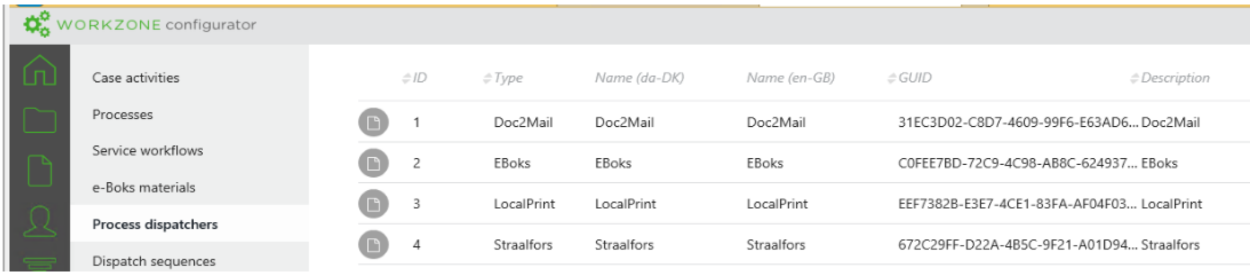
Advanced configuration

You can read more about the implementation and function of the **PartyIdentifierSources** instance and how you can customize the configuration and/or extend it in the WorkZone Process Developer Guide. See Configure PartyIdentifierSources and Configure SmartPost ContactAddressSources.

Configure SmartPost for sending messages

Configure dispatchers

You can configure a number of dispatchers to handle different ways of sending messages. SmartPost is delivered with 4 default dispatchers.



You can modify the default dispatchers to match your organization's needs or you can create new dispatchers.

You can create dispatchers of the following types:

- **e-Boks** - The message is sent to the recipient's digital mailbox in e-Boks.
- **Strålfors** - The message is sent to Strålfors that handles the printing, enveloping, and handover to PostNord.
- **OneTooX** - The message is sent to KMD Print Center that handles the printing, enveloping, and handover to PostNord.
- **Local print** - The WorkZone user receives a smarttask that includes the SmartPost messages in PDF format. The user handles printing, enveloping, and sending of the messages manually.

Configure dispatchers

You create and configure dispatchers in WorkZone Configurator.

1. In WorkZone Configurator, click **Process**
2. Click **Process dispatchers**.
3. Point to the dispatcher you want to use, for example **e-Boks**, and click  **Edit**. Change the values so that they match your organization, such as the

name and description of the dispatcher, start and end date, and access rights. See Process Dispatchers in the WorkZone ConfiguratorAdministrator Guide for a description of the dispatcher settings.

- Or -

Click to create a new dispatcher. In the **Select dispatcher** dialog box, select the type of dispatcher you want to create.

The dispatcher version number

The dispatcher version number, which is displayed next to the dispatcher type, corresponds to the WorkZone Process release that you are running. When you upgrade WorkZone Process, a new version of the dispatcher is created with a version number that corresponds to the new release, and the previous dispatcher version automatically gets an end date. Ongoing SmartPost processes will continue to run using the previous version, and new SmartPost processes will use the new version of the dispatcher. On the **Process dispatcher** tab in WorkZone Configurator, all dispatcher versions are listed.

Note: It is not recommended to make changes to old dispatchers nor remove the end dates of old dispatchers.

4. Click **Save** to save the changes you made to an existing dispatcher, or **Create** to create a new dispatcher.

The next step is to customize the default dispatcher parameters according to your organization, or if you created a new dispatcher, define the parameters from the start.

Edit dispatcher parameters

1. Point to , and click **Edit dispatcher parameters**.
2. Fill in the values for the parameters. The parameters are specific to the dispatcher type.

E-Boks parameters

Name	Default	Description
SenderSystemId		The sender system identifier, which is retrieved during the configuration of the system in the e-Boks administration portal.
ReceiverSystemId		The receiver system identifier, which is retrieved during the configuration of the system in the e-Boks administration portal.
URL	https://rest.e-boks.dk/v1.svc	The URL for the e-Boks service. Enter one of the URLs depending on whether the configuration is made for test or production. Test system: `https://demo-rest.e-boks.dk/v1.svc` Production system: `https://rest.e-boks.dk/v1.svc`
CertificateThumbPrint		The thumbprint that

Name	Default	Description
		identifies the e-Boks certificate.
MaxDocumentSize	78643200	The maximum size of an e-Boks message in bytes. Messages that exceed this limit will not be sent to e-Boks. The default value is 78643200 (75 MB). **Note:** e-Boks determines the maximum size. If e-Boks changes the size, you can change this configuration accordingly but due to encoding you must reduce the size set by e-Boks by 25%. For example, if the size set by e-Boks is 99,5 MB, you must set the **MaxEBoksDocu-**

Name	Default	Description
		mentSize parameter to 99,5 MB * 75% = 75 MB.
ResponseThreshold	1800	Defines the maximum time that SmartPost expects that it takes e-Boks to process a message. Specify the threshold in seconds. The default value is 1800 seconds (30 minutes). **Note:** The default value is most often used. In situations where the communication with e-Boks is slow, you can increase it.
SenderName	KMD	The name of the company.
ReceiverUrl	https://<host-or-database>/Ebok-	The URL for receiving messages using

Name	Default	Description
	sPushService/api/MeddelelseV2	Digital Post 2. If the parameter is left empty, the default URL in the **Url** parameter is used.
DP2Url	https://demo-api.e-boks.com/oio/rest/srv.svc/2	The URL for receiving messages using Digital Post 2. If the parameter is left empty, the default URL in the **Url** parameter is used.
NgDpGuid		The GUID of the NgDP combined sender/receiver system. You can see the GUID in the NgDP Portal. **Note:** This parameter is only relevant if you use the NgDP integration.
SenderCvr		CVR number of the organization that is sending messages. **Note:** This

Name	Default	Description
		parameter is only relevant if you use the NgDP integration.
NgDpConactPointGuid		The GUID of your organization's NgDP reply point (mailbox for replies). You can see the GUID in the ID field on the Kontraktstruktur page in the NgDP portal. To receive messages, it is required to set up a contact hierarchy in the NgDP portal. **Note:** This parameter is only relevant if you use the NgDP integration.
NgDpAuthorizationHeader		The AuthorizationHeader is generated by the **Administrativ**

Name	Default	Description
		Adgang portal when the sender/receiver system is defined. **Note:** This parameter is only relevant if you use the NgDP integration.
NgDpProtocol		Set to REST_PULL or REST_PUSH depending on which protocol you use. **Note:** This parameter is only relevant if you use the NgDP integration.
RemotePushServiceEndPoint		Point to point to a centralized push service. It must be the same push server that is configured to receive memos and receipts in the **Administrativ Adgang** portal.

Name	Default	Description
		Note: This parameter is only relevant if you use the NgDP integration and set up the dispatcher to use the PUSH model.

For more information about configuring an e-Boks dispatcher to NgDP, see Configure SmartPost to use NgDP.

Strålfors parameters

Name	Default	Description
SenderSystemID		The system identifier, which is provided when configuring the system in the Strålfors administration portal. Either Strålfors or the person, who configures the portal for Strålfors, must provide this identifier.
Url	https://prodprint.sconnect.dk/fjernprint/1.0.0	The URL for the Strålfors Connect service. Depending on whether the configuration is made for test or production, enter one of the two URLs. Test: https://testprint.sconnect.dk/fjernprint/1.0.0 Production: https://prodprint.sconnect.dk/fjernprint/1.0.0

Name	Default	Description
CertificateThumbprint		Enter the thumbprint that identifies the Strålfors certificate.
ResponseThreshold	-1	Defines the maximum time that SmartPost expects that it takes to send a message to Strålfors. This value is used to calculate the deadline (supervised by the deadline monitor). The value is an integer, which (if positive) specifies the threshold in seconds. Normally, the default setting is used. If the communication with Strålfors is very slow, you can specify a high value.
MaxDocumentSize	375000000	The maximum number of bytes that a message for remote print can contain. Messages that exceed this limit will not be sent for remote print. The default value is 375000000 bytes (375 MB). **Note:** Unless otherwise communicated, it is recommended to keep the values provided at the installation.
SenderName	KMD	The name of the company that is used in the postal address. The postal address is used when Strålfors produces the letters. The company name is taken from the address on which the authority will receive letters and returned mail.

OneTooX parameters

Name	Default	Description
URL	https://privat.-doc2mail.dk/ deliv-ery/FileUp-loader.asmx	The URL for the OneTooX service. Test: https://test.-doc2mail.dk/delivery/FileUploader.asmx Production: https://private.-doc2mail.dk/delivery/FileUploader.asmx
SystemKey		Enter the system key in clear text. Copy and paste the content of the system key file (PKE file) that you have received from KMD Printcenter in to this field. If you work with WorkZone Configurator in Microsoft Internet Explorer and encounter problems with the system key not being pasted correctly, please open WorkZone Configurator in Google Chrome and try to paste the key again.
Respon-seThreshold	600	The maximum time in seconds that a com-munication channel with OneTooX is open. Default is 600 seconds (10 minutes).
MaxDocu-mentSize	1000000	The maximum number of bytes that OneTooX will send. Numbers higher than 99600000 will be truncated.
SenderName	KMD	The name of the company.

Local print parameters

Name	Default	Description
LocalPrintResponseThreshold	1800	Defines the maximum time that SmartPost expects that it takes for local print to pro-cess a message. This value is used to cal-

Name	Default	Description
		culate the deadline (supervised by the deadline monitor). Specify the threshold in number of seconds. The default value is 1800 seconds (30 minutes). The default value is most often used.
SenderName	KMD	The name of the company.

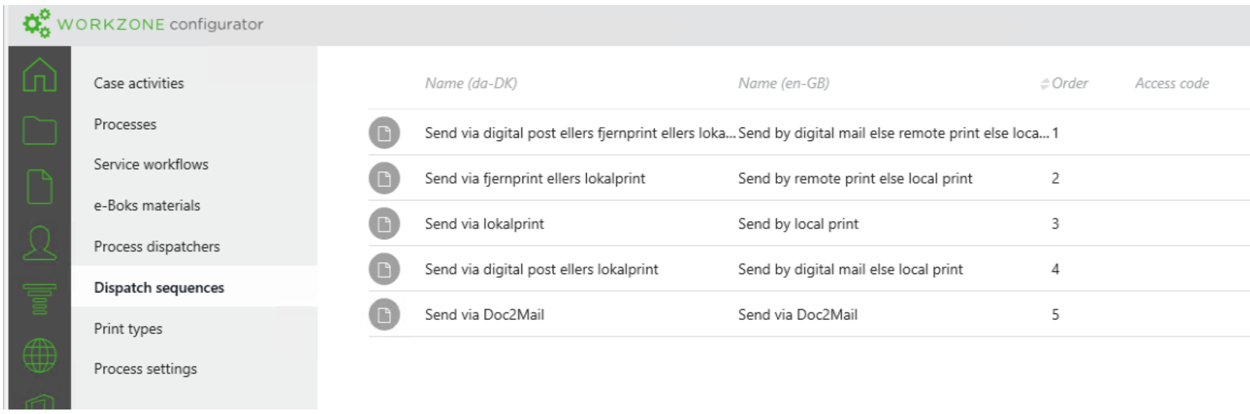
Configure dispatch sequences

A dispatch sequence is a prioritized set of dispatchers that the SmartPost user can select in the **Send SmartPost** dialog box. For example, a user may select a sequence named **Send by digital mail or else remote print else local print**. In this case, SmartPost tries to use e-Boks as the dispatcher to reach the recipient of a message. If the sending fails, SmartPost uses Strålfors instead, and finally if this sending also fails, SmartPost sends the message to the user for printing locally.

You can configure several dispatch sequences and define which sequence to display as the default dispatch sequence in the **Send SmartPost** dialog box.

Dispatch sequences in the SmartPost package

SmartPost is delivered with the 5 dispatch sequences shown below. The dispatch sequences are ordered according to the values in the **Order** column, and they display in this order in the **Send SmartPost** dialog box. You can use the dispatch sequences as is, modify the naming and order, or create new sequences that include dispatchers that match your organization.



Digital mail

When the e-Boks dispatcher is used, SmartPost sends the message to the recipient through e-Boks if the following criteria are met:

- SmartPost must have access to the recipient's CPR or CVR number.
- SmartPost verifies that the recipient subscribes to a registration group that matches the selected logical registration group. SmartPost also verifies that the registration group matches the recipient type, that is citizens or companies.
- The size of the message does not exceed the limit defined by e-Boks.

If the sending fails, SmartPost will try to send the message using the next dispatcher specified in the dispatch sequence, through Strålfors or OneTooX.

Remote print

When the Strålfors or OneTooX dispatcher is used, SmartPost sends the message to the recipient if the following criteria are met:

- The recipient has a valid postal address:
  - Name of the recipient.
  - At least one address line.
  - A postal code.
- The size of the message does not exceed the limit defined by the dispatcher.

If the sending fails, SmartPost will try to send the message by using the next dispatcher specified in the dispatch sequence, for example local print.

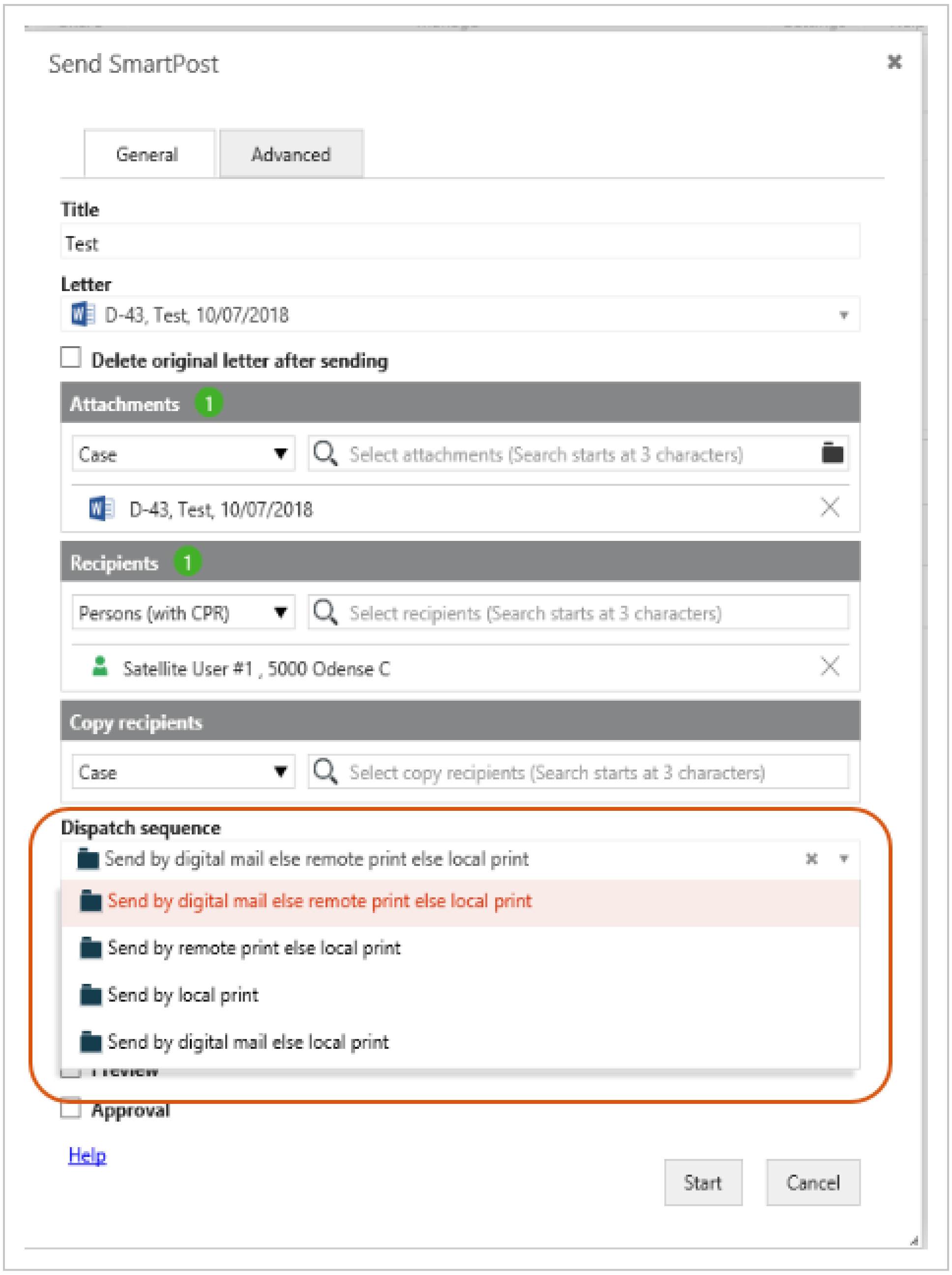
Local print

When the local print dispatcher is used, SmartPost generates an email with the message as an attachment. The email will be sent to the user, who started the SmartPost process. It is then up to the user to print the message and handle the dispatch manually.

Create or modify dispatch sequences

You create and configure dispatch sequences in WorkZone Configurator. The dispatch sequences that you create will be available to user in the **Dispatch sequence** field in the

Send SmartPost dialog box.



You can use the dispatch sequences as they are, modify the naming and order, or create new sequences that match your organization. To create a new dispatch sequence, you must first create the dispatch sequence, and then add dispatchers to it.

1. In WorkZone Configurator, click **Process**
2. Click **Dispatch sequences**.

3. Point to next to the dispatch sequence that you want to use, for example, **Send by digital mail else remote print else local print**, and click **Edit**. Change the values so that they match your organization, for example, change the names you want to display to the users in the **Localize name** fields and the order in the **Order** field.

   - Or -

   Click to create a new dispatch sequence, enter a name for the sequence in the **Name** field and a number in the **Order** field. The dispatch sequence will be displayed according to this number in the **Dispatch sequence** field in the **Send SmartPost** dialog box.

4. Fill in other parameters that are relevant for your organization. See Create a dispatch sequence in the WorkZone Configurator Administrator Guide for a description of each parameter.
5. Click **Save** to save changes you made to existing sequences or **Create** to create a new sequence.

If you created a new dispatch sequence, the next step is to add dispatchers and define the order of the dispatchers in the sequence.

Add dispatchers to a dispatch sequence

1. In WorkZone Configurator, click **Process** > **Dispatch sequences**.
2. Point to the dispatch sequence to which you want to add dispatchers, and click **Define dispatch sequence**.
3. Click **Add dispatcher**, select the dispatcher you want to add to the sequence, and specify its order in the dispatch sequence.

Remove a dispatcher from a sequence

- Click to remove a dispatcher from the dispatch sequence.

Set up a default dispatch sequence

You can specify a default dispatch sequence, which will be preselected in the **Send SmartPost** dialog box.

1. In WorkZone Configurator Click **Process**.
2. Click **Processes**.
3. Point to next to the **SmartPost** process, and click **Edit process parameters**.
4. In the **DefaultDispatcherSequenceId** field, select the dispatch sequence that you want to be preselected in the **Send SmartPost** dialog box.

Configure e-Boks materials

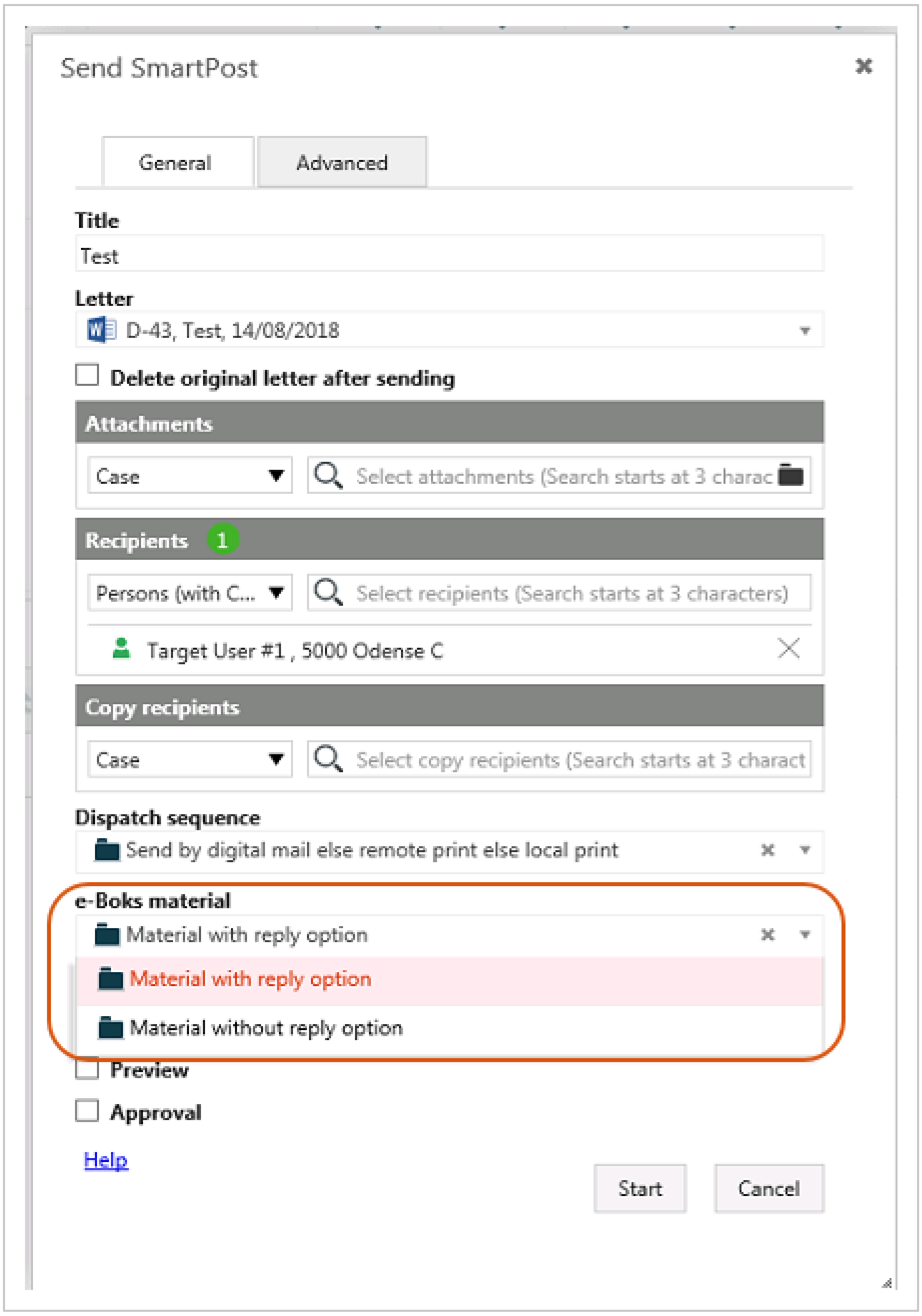
An e-Boks material is a configurable item in e-Boks that describes what to be communicated to the e-Boks user. SmartPost needs to know the materials in order to send messages though e-Boks.

The material determines if the user can reply to a message. Before you configure SmartPost, the organization needs to configure both the materials and the connection with registration groups the e-Boks Administration Portal. Registration groups use either a material that is enabled or disabled for replies. Several registration groups can use the same material at the same time, which means that a registration group can share materials with other registration groups. The organization decides if materials will be shared across registration groups.

When the organization creates a material in the e-Boks administration portal, the material is assigned a unique ID. You need this ID to set up materials in SmartPost. Please refer to the e-Boks brugersupport (e-Boks user support) for information about how to set up e-Boks materials in the e-Boks Administration Portal.

Configure e-Boks materials

You create and configure e-Boks materials in WorkZone Configurator. The e-Boks materials that you create are listed in the **e-Boks material** field in the **Send SmartPost** dialog box.



With the installation of SmartPost, two e-Boks materials are created by default in WorkZone Configurator:

- **Material without reply option**
- **Material with reply option**

You can edit the default materials to suit your organization's setup or create your own materials.

> **Prerequisite:** Make sure that materials are created in the e-Boks administration portal, and that you have the e-Boks material IDs.

1. In WorkZone Configurator, click **Process**.
2. Click **e-Boks materials**.
3. Point to next to the default material, **Material without reply option** or **Material with reply option**, you want to use. Click **Edit**, and enter the e-Boks material ID that corresponds to the material you have created in the e-Boks Administration Portal.

   - Or -

   Click to create a new e-Boks material, enter a name for the material and the e-Boks material ID that corresponds to the material you have created in the e-Boks Administration Portal.
4. Fill in other settings that are relevant for your organization. See Create an e-Boks material in the WorkZone Configurator Administrator Guide for a description of each settings.
5. Click **Save** to save changes you made to existing materials or **Create** to create a new material.

Set up a default e-Boks material

You can specify a default material that will be preselected in the **Send SmartPost** dialog box.

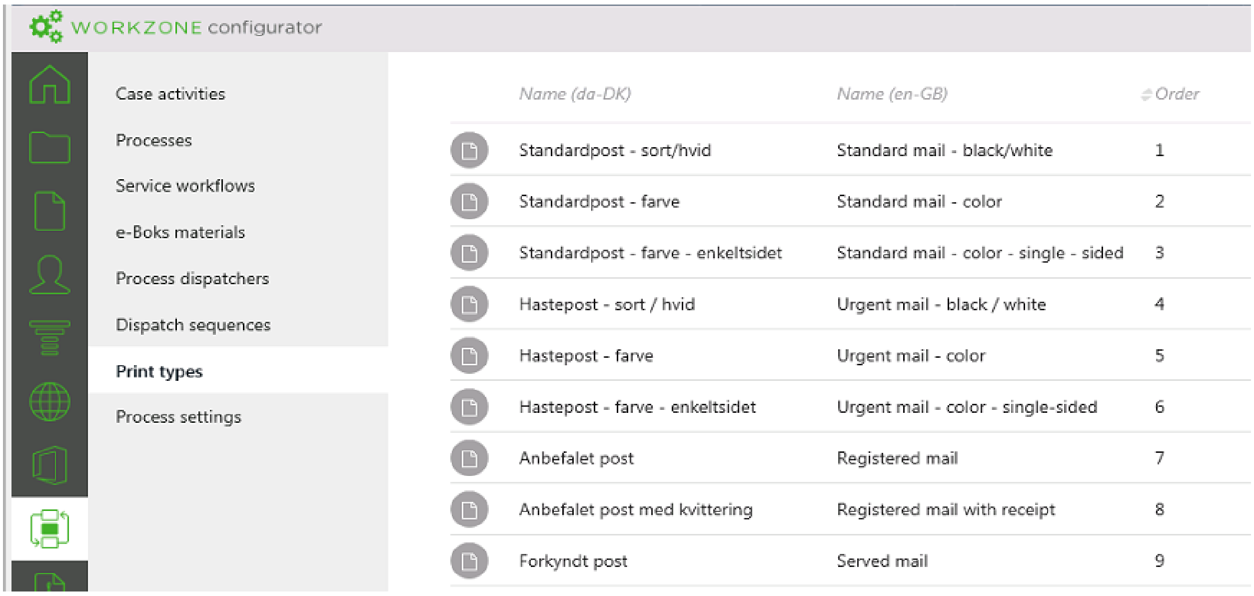
1. Open WorkZone Configurator, and click **Process** > **Processes**.
2. Point to the SmartPost process, and click **Edit process parameters**.
3. In the **DefaultMaterialID** field, select the material you want to display as default in the **Send SmartPost** dialog box.

Configure print types

A print type is a predefined configuration of how Strålfors or OneTooX print and handle a dispatch. For example, a print type defines the size of the page and envelope, A or B mail, single-sided or double-sided, and so on.

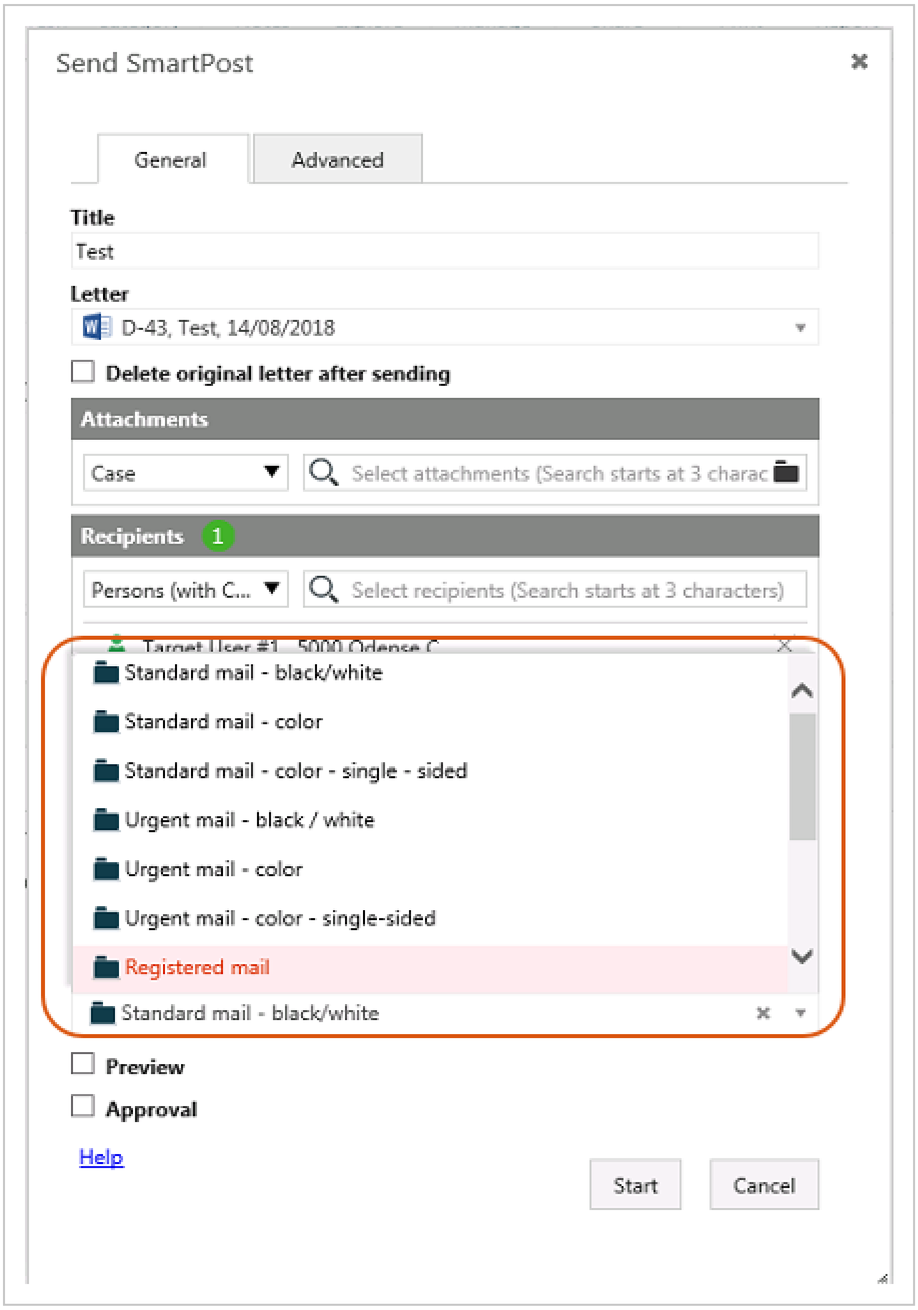
Print types in the SmartPost package

By default, the SmartPost package includes 9 print types as shown below. The print types are ordered according to the values in the **Order** column, and they are displayed in this order in the **Send SmartPost** dialog box. You can use the print types as they are, modify the naming and the configurations to match your organization, or you can create new print types.



Create or modify print types

You create and configure print types in WorkZone Configurator. The print types that you create are listed in the**Print type** field in the **Send** SmartPost dialog box.



1. In WorkZone Configurator, click **Process**
2. Click **Print types**.
3. Point to  next to the print type that you want to use, for example, **Standard mail - color**, and click  **Edit**. Change the values so that they match your organization. For example, you can change the names you want to display to the users in the **Localize name** fields, and you can change the order in the **Order** field.

   \- Or -

Click to create a new print type. In the **Create print type** dialog box, enter a name for the print type, and fill in other settings that are relevant for your organization. See Create print types in the WorkZone Configurator Administrator Guide for a description of each setting.

If you created a new dispatcher, the next step is to set up the print type parameters.

Edit print type parameters

1. Point to and click **Edit print type parameters**.
2. Fill in the values for the parameters. The table below describes the parameters and the dispatcher type they apply to.

Name	Description	Dispatcher type
PortoCategoryKey	Specify the postage category.	Strålfors
ReturnedLetter HandlingKey	Specifies how Strålfors handles letters that are returned to Strålfors in case PostNord has not been able to deliver the letter. If you select **true**, Strålfors destroys the letter. If you select **false**, Strålfors performs no action.	Strålfors
UrgencyLevelkey	Specify the level of urgency.	Strålfors
Simple/DuplexKey	Specify whether to print the letter single-sided or double-sided.	Strålfors
PrintColorOptionKey	Specify black/white or color print.	Strålfors
EnvelopeTypeKey	Specify the size of the envelope.	Strålfors
DocumentType	Enter the name of the OneTooX document type that you have received from KMD Printcenter.	OneTooX
AddReturnAddress	Select if you want to add a return address to the document before sending it. The return address is taken	OneTooX

Name	Description	Dispatcher type
	from the OneTooX system key that you have received from KMD Printcenter	
MailPriority	Select the mail priority, **Quick letter** (A Prioritaire) or **Ordinary letter** (B Economique).	OneTooX

Set up a default print type

You can specify a default print type that will be preselected in the **Send SmartPost** dialog box.

1. Open WorkZone Configurator, and click **Process** > **Processes**.
2. Point to the SmartPost process, and click **Edit process parameters**.
3. In the **DefaultRemotePrintypeIID** field, select the print type you want to display as default in the **Send SmartPost** dialog box.

Configure templates

The SmartPost package includes two default templates:

- Cover pages for recipients with protected addresses
- Cover pages for copy recipients

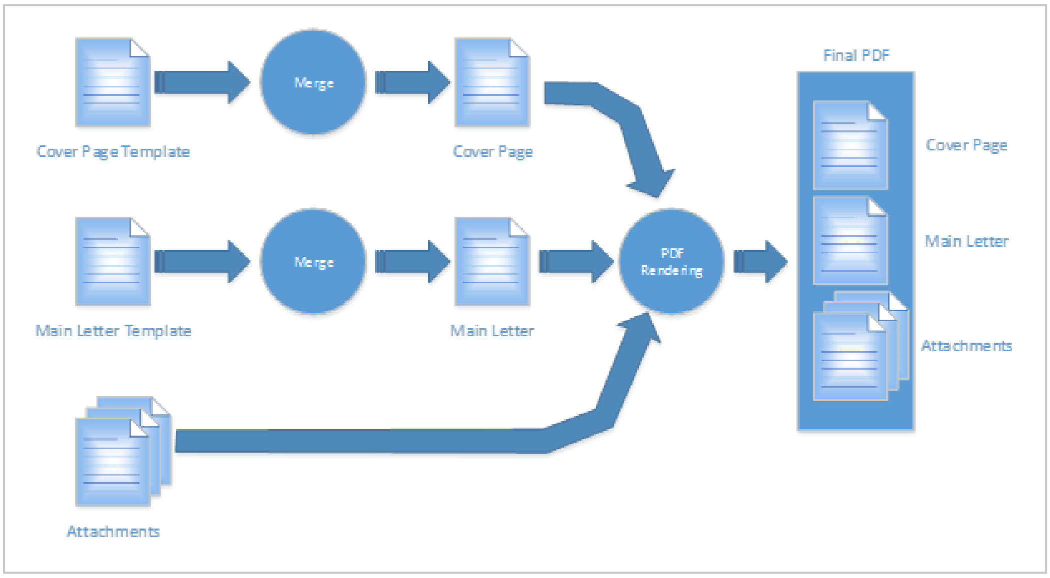
An organization can create and configure its own templates.

Cover page templates

The cover page is inserted at the beginning of the message that is sent to a recipient. The cover page must have a layout and content that can be used when the message is sent as a physical letter. For example, the recipient's name and address must be located at a specific position on the cover page in order to be visible through the window of the envelope, and no confidential information must be exposed.

Important: You must use content controls to create the cover pages in the same way as for the main letter in SmartPost.

The diagram below illustrates how SmartPost creates the cover page based on the cover page template. The cover page is merged at the same time as the rest of the message is merged.



The protected address cover page

When a recipient has a protected address, SmartPost inserts a protected address cover page as the first page of the message to the recipient.

The main letter document is then merged, but the information required to locate the recipient is left out. SmartPost does this by leaving the content controls that contain address information empty.

The reason for also leaving out the address information in the letter to the recipient is to minimize the risk of recipients questioning if the letters that are sent to the copy recipients provide information that makes it possible to locate the recipient.

If the address is protected, the following address information is left out:

Case parties

The contacts that are registered as parties on the case that a SmartPost message is sent from.

- Address 1
- Address 2
- Address 3
- Contact code
- Contact number
- Contact number (code)
- Country code
- Country (text)
- Country (name)
- E-mail
- Fax
- Postcode
- Mobile phone
- Postcode (code)
- Postcode (text)
- Post district

Document contacts

The contacts that a user selects as recipients and copy recipients in the **Send SmartPost** dialog box as well as the sender, who is the process owner.

- Postcode
- Address 1
- Address 2
- Address 3
- Fax
- Country name
- Country
- Country
- Contact number
- Email

- Contact code
- Mobile phone
- Phone
- Postcode (code)
- Postcode (text)
- Post district

> Important: If custom fields have been added on contacts, WorkZone cannot know if the fields are protected.

Default protected cover page:

Ang. sag:

23. maj 2017
J.nr.

De modtager dette brev, som hovedmodtager.
Da Deres adresse er beskyttet, vil <firmanavn> hermed forsikre Dem om, at eventuelle kopimodtagere IKKE vil modtage Deres adresse på de tilsendte kopier.

Såfremt de skulle have modtaget dette brev ved en fejl, bedes De destruere brevet og underrette <firmanavn> derom.

Venlig hilsen

<Firmanavn>
<Gadenavn og nummer>
Postboks <Postboksnr.>
1323 København K

Tlf.nr. +45 <Telefonnr.>
Fax +45 <Telefonnr.>

<E-mail>
<Hjemmeside>

EAN-nr:
<EAN-nr.>

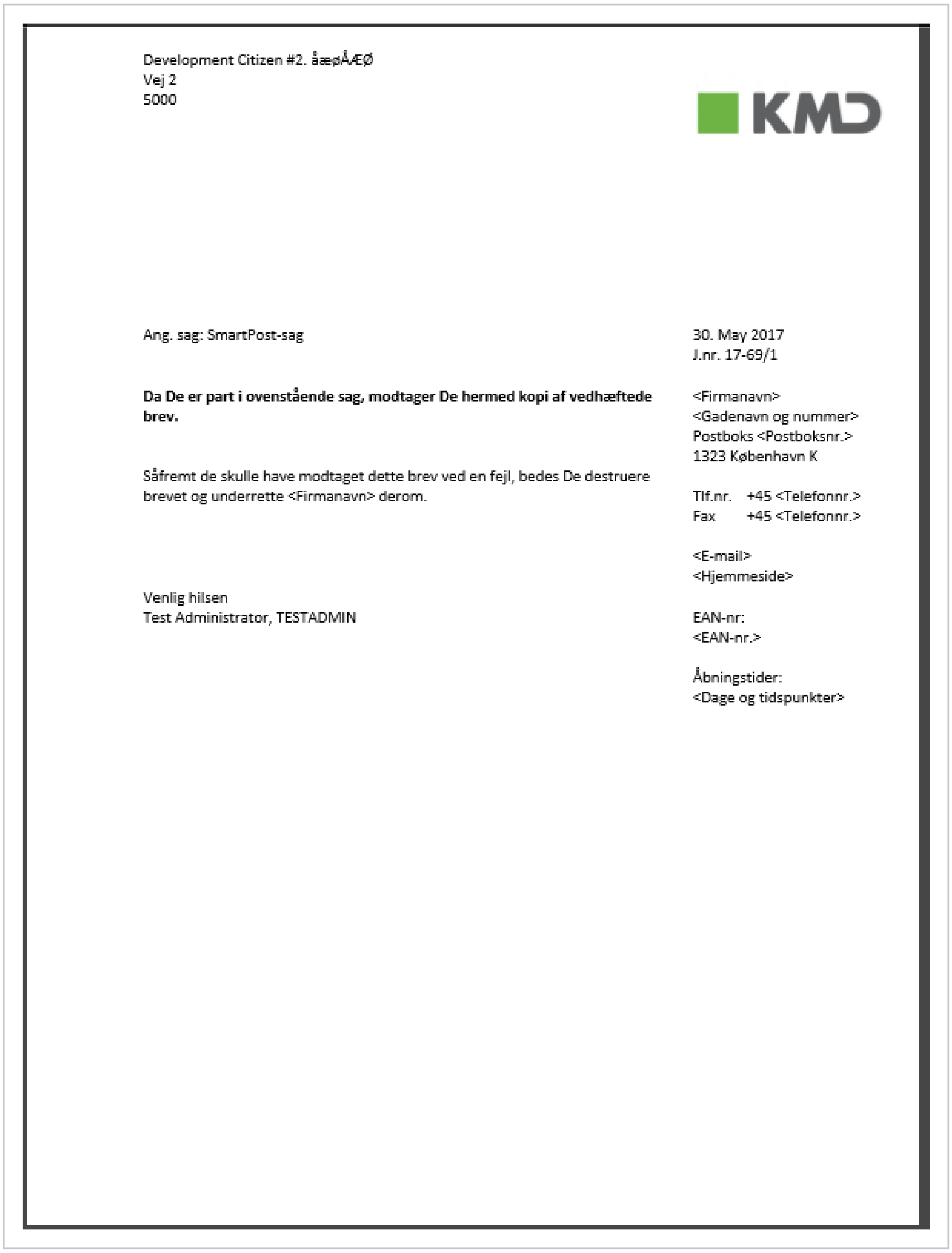
Åbningstider:
<Dage og tidspunkter>

Note: If you have turned on the **AllowSendingSeparateDocuments** parameter in the SmartPost parameters to allow users to send attachments as separate PDF documents through e-Boks, and you have turned off the **MergeAllDocuments** parameter, the messages will not include a protected address cover page. Any copy recipients will still receive one merged PDF document including the cover page.

The Copy Recipient Cover Page

When a contact is selected as a copy recipient of a message, SmartPost inserts a copy recipients cover page as the first page in the message to the copy recipient. The main letter is then merged. If the main recipient has a protected address, the merge is then made without the address information, which can be used to locate the main recipient. As for the protected address cover page, the address information is left out (see above). If the main recipient does not have a protected address, SmartPost uses the whole address information of the main recipient when merging the main letter.

Default copy recipient cover page:



Development Citizen #2. åæøÅÆØ
Vej 2
5000

Ang. sag: SmartPost-sag

30. May 2017
J.nr. 17-69/1

Da De er part i ovenstående sag, modtager De hermed kopi af vedhæftede brev.

Såfremt de skulle have modtaget dette brev ved en fejl, bedes De destruere brevet og underrette <Firmanavn> derom.

Venlig hilsen
Test Administrator, TESTADMIN

<Firmanavn>
<Gadenavn og nummer>
Postboks <Postboksnr.>
1323 København K

Tlf.nr. +45 <Telefonnr.>
Fax +45 <Telefonnr.>

<E-mail>
<Hjemmeside>

EAN-nr:
<EAN-nr.>

Åbningstider:
<Dage og tidspunkter>

Create a cover page template

1. Use Microsoft Word to create a template. The template document must be of the type docx or dotx. Insert content controls that correspond to the address information (or other variable information) at the correct positions in the document. Ensure that the address information is located in the right position on the page to make it visible for the postal worker through the window of the envelope.

> **Tip:** Strålfors provides an online test application (connect2.popwatch.com), which can be used to verify that the address information is located in the correct position.

2. Import the templates to a case in WorkZone using WorkZone Client. Typically, you have a specific case for template documents. After importing the templates, note the document number and name of the imported template document.
3. Open WorkZone Configurator.
4. Click **Process** > **Processes**.
5. Point to the **SmartPost** process, and click **Edit parameters**.
6. Select the template document for each of the parameters:
   - **CopyCoverPageRecordId** - The copy recipient cover page.
   - **ProtectedCoverPageRecordId** - The protected cover page.
6. Click **Save**. The SmartPost process will take the cover page templates in to use immediately.

For more information about how to configure WorkZone Process parameters, see Processes in the WorkZone Configurator Administrator Guide.

Update templates with Captia content controls

Captia content controls are not supported in WorkZone. To make templates with Captia content controls work, you need to replace the Captia content controls with WorkZone content controls. See Check for Captia content controls in the WorkZone for Office User Guide.

Configure standard letters

An organization may have standard letters that they want users to be able to include in SmartPost messages. A standard letter is a letter with predefined content that the user does not need to change before sending a message. The standard letter must be a Word document (docx or docm) or a Word template (dotx or dotm).

To make standard letters available to users in the **Send SmartPost** dialog box, you need to complete the following steps:

- Make sure that you have the TEMPLATEADM access code assigned.
- Create a specific case to hold the standard letter documents and assign the case group named TEMPLATES to it.
- Enter the case number of the case in the SmartPost process settings.

Create a case for standard letters

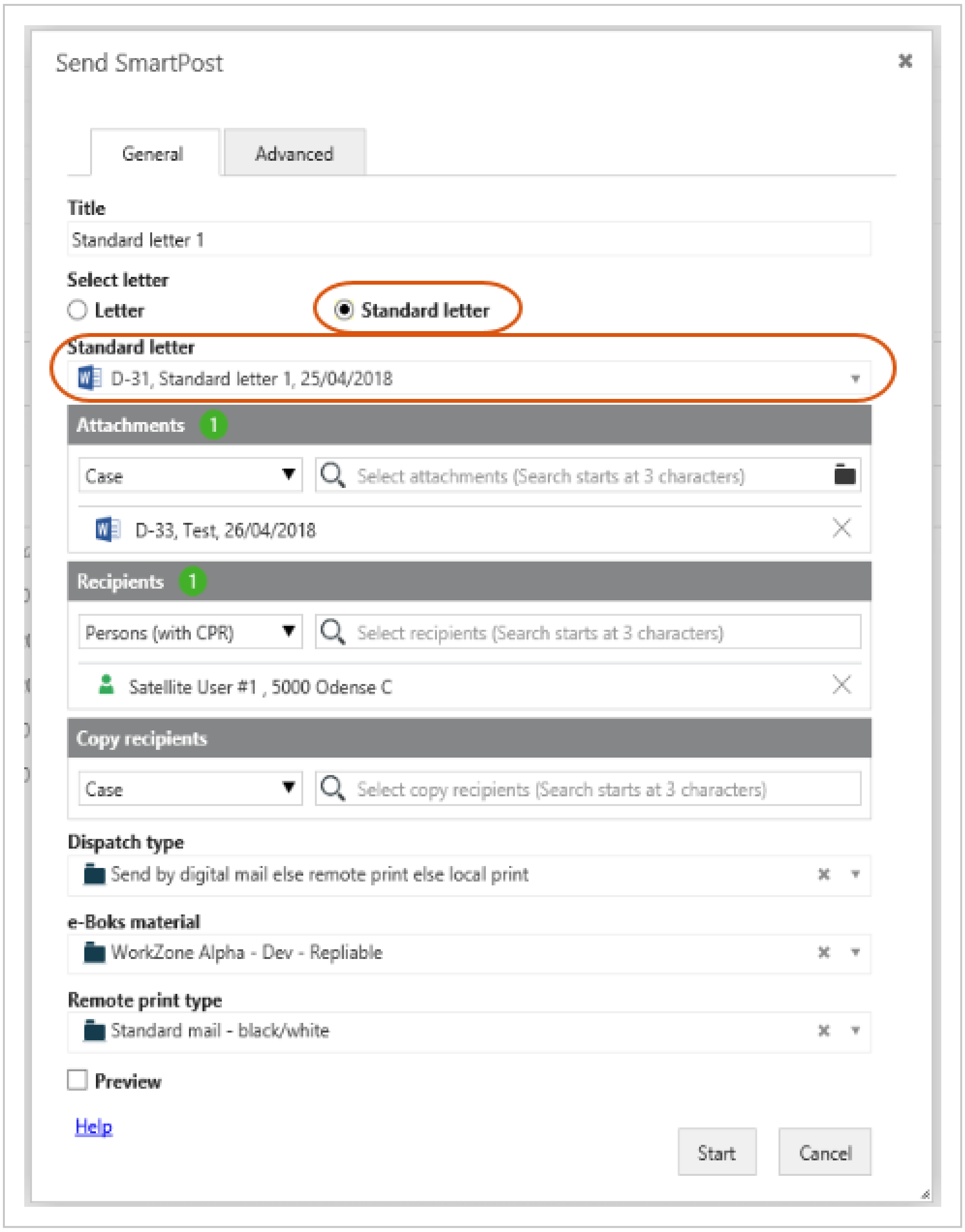
> **Prerequisite:** The TEMPLATEADM access code.

1. In WorkZone Client, create a case to hold the standard letters.
2. Assign the case group named **TEMPLATES** to the case.
3. Add the standard letter documents to the case.

Configure standard letters

1. In WorkZone Configurator, click **Process**.
2. Click **Processes**.
3. Point to the **SmartPost** process. A menu bar appears.
4. Click **Edit process parameters** .
5. In the **Edit process parameters** dialog box, select the case that contains the standard letters in the **StandardLetterFileNo** parameter.

When the setup is complete, the users will see a **Standard letter** option and a list of standard letters in the **Send SmartPost** dialog box.



Configure SmartPost and GDPR classification

You can configure SmartPost so that it supports the European Union's General Data Protection Regulation (GDPR). For SmartPost, it means that you can define which documents are allowed to send through SmartPost based on the classification of the documents. If GDPR support is configured, users will only be able to select documents in the **Send SmartPost** dialog box that comply with a maximum classification level.

You define classification levels by specifying a rank for each document classification in WorkZone, and then configure a maximum document classification rank that defines that only documents with the specified maximum rank or lower can be sent. Documents with higher classification ranks than specified for this parameter are not available for selection in the **Send SmartPost** dialog box.

If users start the SmartPost process from a document, which does not comply with the defined maximum rank, the document will not be preselected in the **Letter** field in the **Send SmartPost** dialog box.

> **Note:** It is not possible to include documents without classifications and documents with classifications but no rank in a SmartPost message. An error will be shown and it is not possible to start the SmartPost process.

When SmartPost merges the documents into the message that will be sent to the recipients, the merged PDF document gets the classification that corresponds to the aggregated classification based on the ranks of the selected documents (the letter and attachments). It means that the message gets the same classification as the document with the highest confidentiality level (the highest rank). The history document gets the same classification as the message.

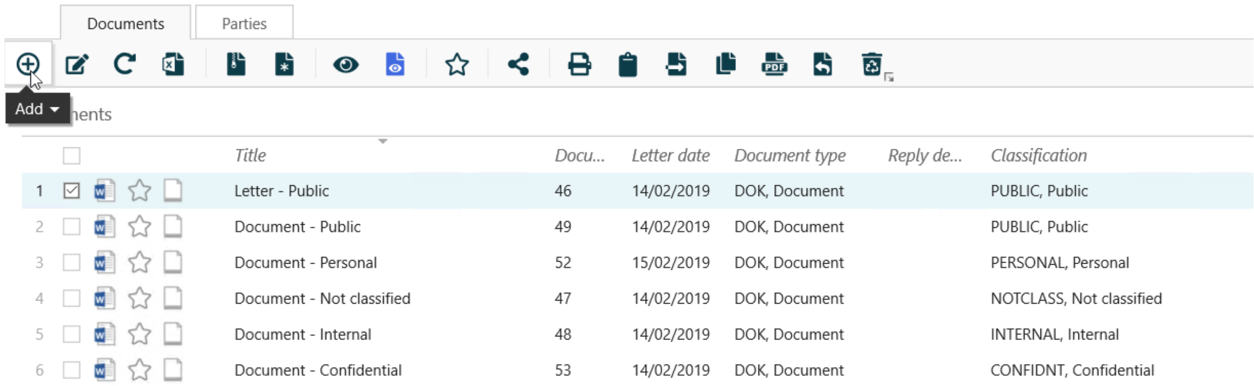
Example

An organization has created five document classifications with the ranks 1-5 where documents with the highest confidentiality level have the highest classification *Confidential* which has the rank *5*. The maximum classification rank (the threshold) is set to *3*.

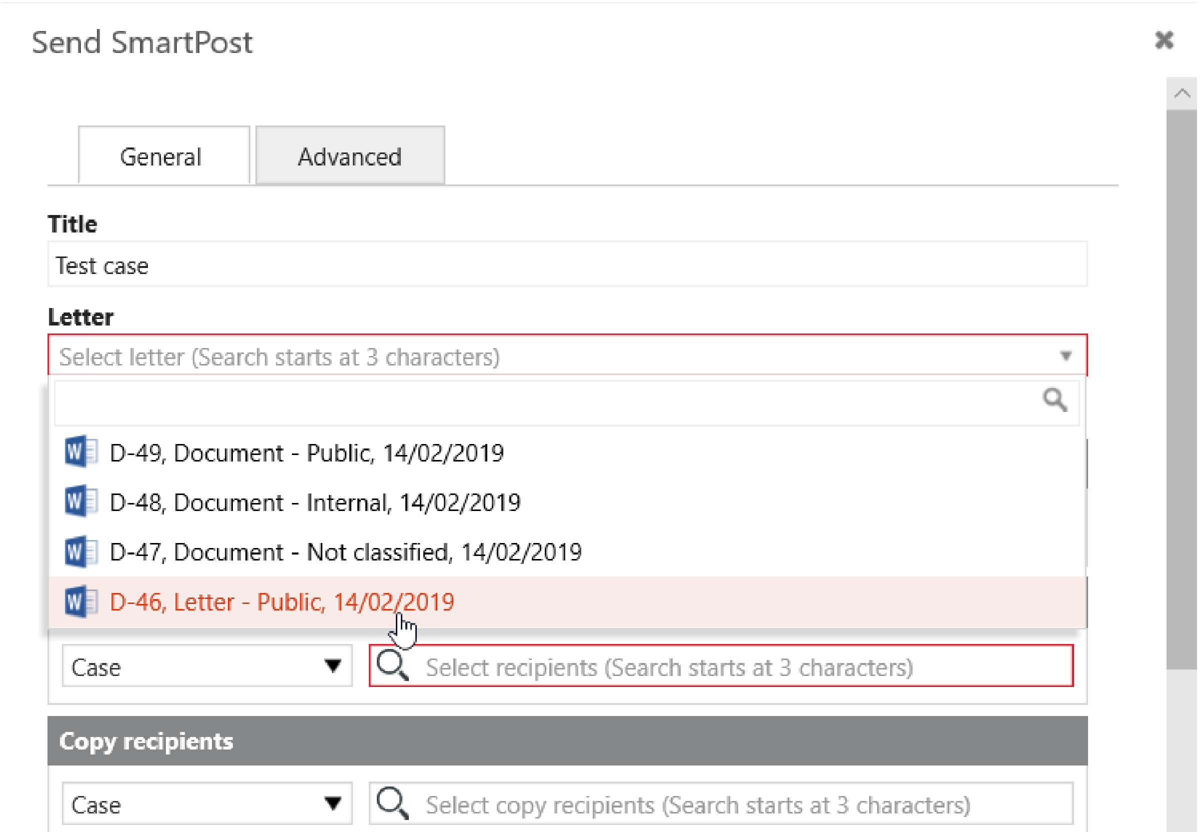
The document classifications as configured in WorkZone Configurator:

Code	Label (da-DK)	Label (en-GB)	Rank	Start date	End date	System
NOTCLASS	Ikke klassificeret	Not classified	1			No
PUBLIC	Offentlig	Public	2			No
INTERNAL	Intern	Internal	3			No
PERSONAL	Personfølsom	Personal	4			No
CONFIDNT	Fortrolig	Confidential	5			No

A user has a case with 6 documents with different classifications:



When the user starts a SmartPost process, only the documents with classification ranks below or equal to *3* (Internal) will be available for selection:



The user adds all 4 documents to the SmartPost message, a letter document and three attachments. The SmartPost message and the history document get the classification *Internal* with rank *3*.

Configure GDPR classification support

To configure GDPR support for SmartPost, make sure that:

- Documents have a classification.

  As of WorkZone Client 2017 SP1 this is a required field for all documents. For documents that are created with earlier releases, the documentation classification must be set manually. See Document classification in the WorkZone Configurator Administrator Guide.

- Document classifications are ranked.
- A document classification threshold is defined.

You configure the ranking and threshold in WorkZone Configurator.

Rank document classifications

1. In WorkZone Configurator, go to **Document** > **Document classification**.
2. Click **Edit**.
3. Enter a rank for each classification.

If a document classification does not have a rank, users will not be able to select documents with this classification in the **Send SmartPost** dialog box.

Define a document classification threshold

1. In WorkZone Configurator, go to **Process** > **Processes**.
2. Point to the **SmartPost** process.
3. Click **Edit process parameters**.
4. In the **DocClassificationThreshold** field, enter the document classification rank corresponding to the maximum classification level you want to use with SmartPost. See DocClassificationThresHold.

Note: By default, the **DocClassificationThreshold** field is empty, which means that all documents can be selected and sent in SmartPost messages.

Use SmartPost without GDPR support

If you want to use SmartPost without the GDPR support, which means that all documents will be available for selection in the **Send SmartPost** dialog box, do not specify a classification rank in **DocClassificationThreshold** field.

Configure allowed documents

You can configure which documents that users are allowed to select in the **Send SmartPost** dialog box based on a custom field and its values. If you have configured allowed documents, users will only be able to select the documents with the allowed values from the droplists in the **Letter** and the **Attachments** fields in the **Send SmartPost** dialog box.

> **Example**: An organization has marked their documents with different levels depending on the confidentiality of the documents. For this purpose, they have created a custom field named **Document level** that contains a droplist with the values **1**, **2**, **3**, **4**, and **Not specified**. The **Document level** field has been added to the document detail page in WorkZone Client. The employees are only allowed to send documents with level **4** and **Not specified** using SmartPost, which means that only documents with these levels are shown in the droplists for the **Letter** and **Attachments** fields in the **Send SmartPost** dialog box.

You configure which documents are allowed by configuring the **ValidationProperty** and the **ValidationValues** parameters in the SmartPost process parameters. In the above example, the **ValidationProperty** parameter must be set to the custom field **Document level** and the **ValidationValues** parameter must be set to the values **4** and **Not specified**.

Configure allowed documents

- A custom field of the type **Droplist**. The **Droplist** type allows you to add multiple values.

  See Custom fields in the WorkZone Configurator Administrator Guide.

- A custom droplist that contains values for the documents.

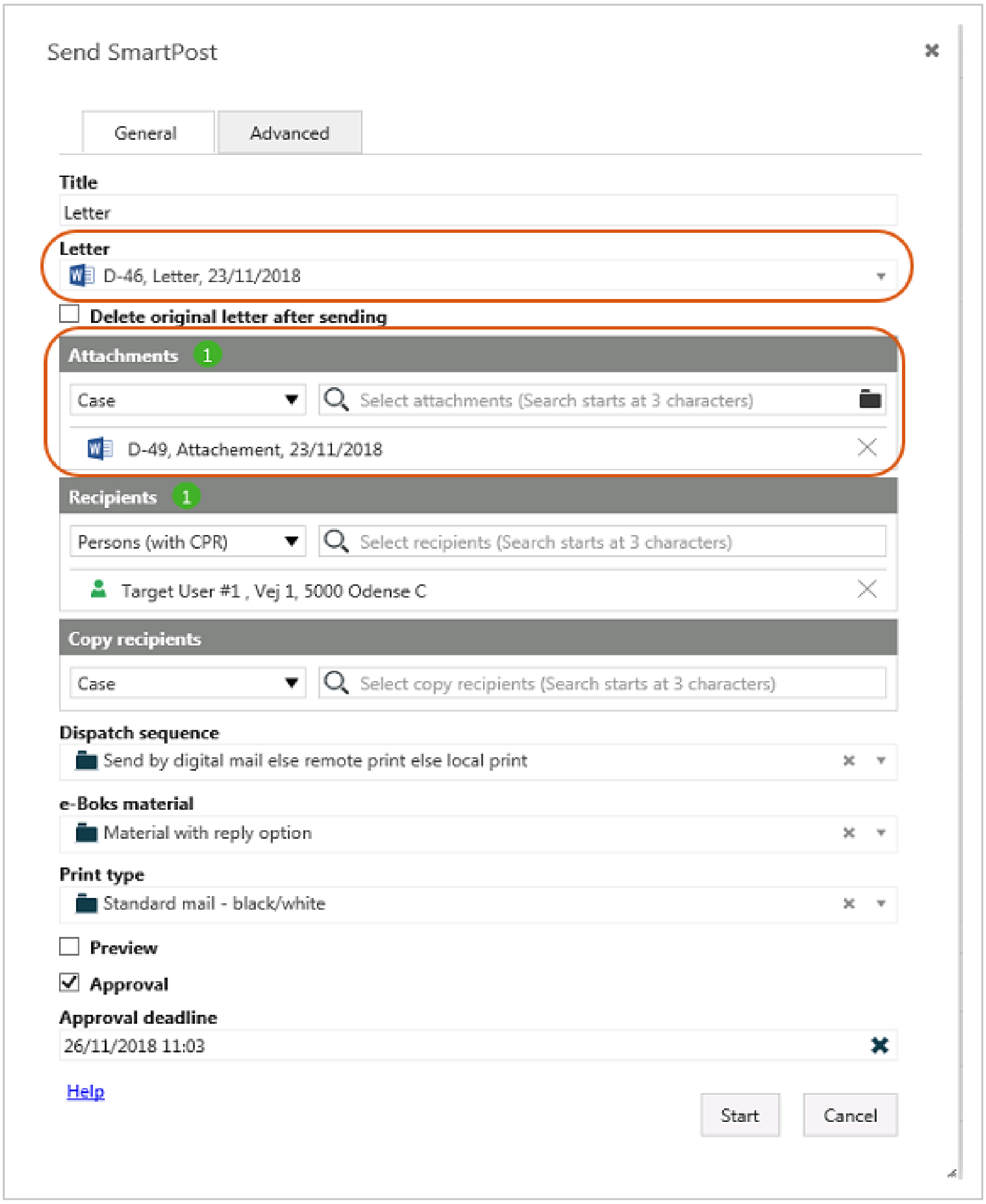
  See Custom droplists in the WorkZone Configurator Administrator Guide.

- The custom field is added to the document detail page in WorkZone Client.

  See Configure detail pages in the WorkZone Client Administrator Guide.

1. In WorkZone Configurator, click **Process**.
2. Click **Processes**.
3. Point to the **SmartPost** process. A menu bar appears.
4. In the **Edit process parameters** dialog box, select the custom field that you want to validate against in the **ValidationProperty** parameter.
5. Select allowed values in the **ValidationValues** parameter.

When the setup is complete, the users will only see the allowed documents when they click in the **Letter** and **Attachments** fields in the **Send SmartPost** dialog box.



Note: If the custom field is empty, the document will be considered as allowed.

Send messages status

SmartPost monitors all outgoing messages to ensure that the messages reach the recipients.

- Continuous status requests
- Time based monitoring

Continuous status requests

The monitoring is implemented differently depending on the selected provider, e-Boks or Strålfors.

e-Boks

SmartPost transfers messages to e-Boks and receives a reply immediately as part of the transaction. According to e-Boks, a positive reply is sufficient to accept that the message is received by the end user, as long as the messages is sent as a planned immediate delivery.

SmartPost reads the reply and determines based on the content whether the sending is successful or not. SmartPost does not request the status of the messages later.

> Note: Through the REST interface to e-Boks, it is possible to send messages that will be delivered at a specific time. The concept "immediate delivery" means that SmartPost requests that e-Boks delivers the message in the end user's inbox immediately.

Strålfors

When SmartPost transfers messages to Strålfors, it continually requests the status of messages. When SmartPost receives a status from Strålfors, which indicates that the message has been correctly received and handled, SmartPost assumes that the message is delivered.

Time based monitoring

When the user selects how to send a message (digital post, remote print, or local print), SmartPost estimates a deadline for when a the messages can be delivered.

If SmartPost does not assume that the messages have been delivered by the deadline, an email is sent to the user notifying the user that the deadline is exceeded. The user can then choose to extend the deadline, in which case the deadline will be extended by 2 hours, or cancel the dispatch. In the case of canceling a dispatch, SmartPost stops attempting to send the messages again. In this case, some of the messages may be sent correctly whereas others may be outstanding or not sent at all. SmartPost will try to clean this up.

Dispatch information

During the sending of messages, miscellaneous information is added to the generated PDF documents. This information allows you to extract documents that are sent through the SmartPost process based on different criteria. The information is added to the documents as free information.

Dispatch role (SHIP_ROLE)

Information about the dispatch role is added to documents during generation of the PDF documents before they are sent to end users. The role can be either recipient or copy recipient.

You can, for example, use this information to get statistics on how many documents have been sent to the main recipients compared with the number of documents sent to the copy recipients.

Document size (PDF_SIZE)

Information about document size is added to documents during the generation of the PDF documents before they are sent to end users. The information tells you the size of the PDF document in number of bytes (integer).

You can, for example, use this information to get statistics on size of the documents that are sent through SmartPost or on how much data is sent through SmartPost during a specific period of time.

Number of documents (PDF_COUNT)

Information about number of documents is added to documents during the generation of the PDF documents before they are sent to end users. The information tells you the number of generated PDF documents. This number corresponds to the total number of recipients and copy recipients that are part of a dispatch.

You can, for example, use this information to get statistics on the number of recipients by each SmartPost dispatch.

Dispatch date (SPSHIPPED)

Information about dispatch date is added to documents during the generation of the PDF documents before they are sent to end users.

As regards documents that are sent to local print, the value is added to the document when the document is sent as an email to the user.

As regards documents that are sent using other dispatch types (digital post or remote print), the value is added when SmartPost has verified that the document is sent to the service provider.

The dispatch date is the current date (excluding the time), and it is written as free date information.

You can, for example, use this information to narrow SmartPost queries to return results within a specific period of time.

Final dispatch type (CHANNEL)

Information about the final dispatch type is added to documents that are to be sent every time SmartPost decides to try out a new type of dispatch. It happens, for example, when SmartPost tries to send a dispatch through digital mail but then has to choose another dispatcher if the dispatch is rejected by the service provider.

When the information is added to a document, it overwrites the previous value. This way, the value after the sending has been completed will always be the dispatch type that SmartPost uses to send the message.

You can, for example, use this information to determine how many documents have been sent using the various dispatch types during a specific period of time.

Remote print type (PRINT_TYPE)

Information is added to documents that are sent through SmartPost using remote print. The information will be available even if SmartPost does not succeed in sending the document to remote print and then has to choose a different dispatcher.

The information is the name of the print type that the user has selected in the **Send SmartPost** dialog box.

You can, for example, use this information to get statistics on the typical choices of print types.

Workflow instance ID (WFIID)

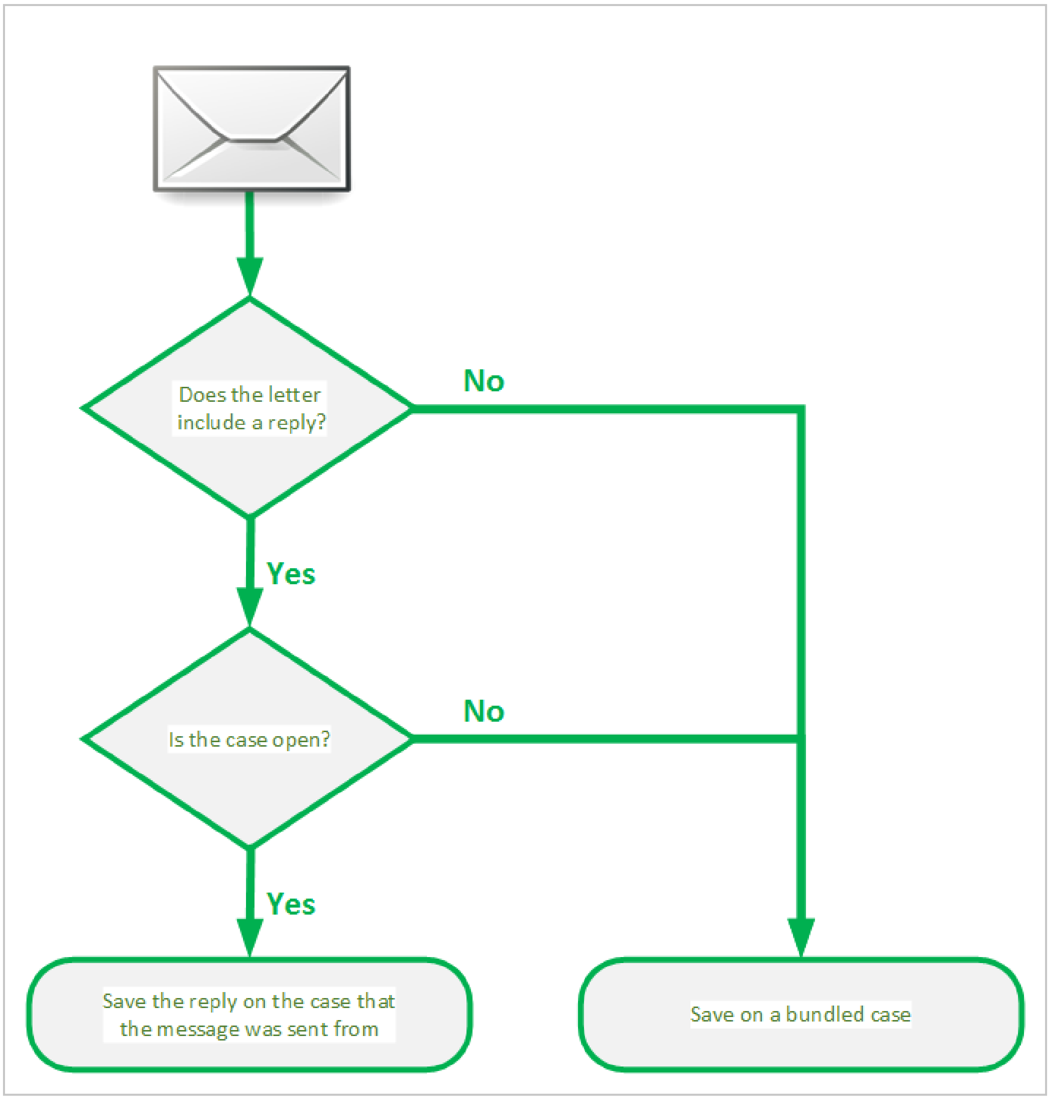
At the time of creation of the documents, this information is added to all documents that are generated by SmartPost. The information includes a GUID (Globally Unique Identifier) that identifies the WorkZone process that describes the current dispatch.

You can, for example, use the information if you suspect that something is wrong with a specific dispatch and you want to analyze the details of this dispatch.

Configure SmartPost for receiving messages

Configure SmartPost for receiving messages

A service workflow named e-Boks Message Handler handles the receiving of messages from e-Boks. The service workflow contacts e-Boks at regular intervals and checks for unread messages. In case of unread messages, a receipt workflow starts. When this workflow has been completed, the message is marked as read.



When SmartPost receives a message from e-Boks, SmartPost checks if the message is a reply to a message that was sent from SmartPost. If the message is not a reply but an unsolicited messages, the message is saved as a document with possible supplementary documents on a default case. If the unsolicited message is sent to a subunit in your organization, it is saved on a specific case, which is mapped to the subunit (the unit's dossier). See Handle e-Boks messages sent to subunits.

If the message is a reply, the message is saved as a document with possible supplementary documents on the case that the original SmartPost message was sent from. The case must be open. If the case is closed, the letter is saved as a document on the default case.

You can configure SmartPost for receiving messages in WorkZone Configurator.

See also Receive messages from SmartPost in the WorkZone Process User Guide.

Configure SmartPost settings for receiving messages

1. Open WorkZone Configurator, and click **Process** > **Process dispatchers**.
2. Point to next to the e-Boks dispatcher you use, and click **Edit dispatcher parameters**.
3. Specify the following parameters:

   - ReceiverSystemID
   - CertificateThumbprint

See Configure dispatchers.

Configure an e-Boks Message Handler service workflow

You set up the e-Boks Message Handler service workflow in WorkZone Configurator.

1. In WorkZone Configurator, click **Process**.
2. Click **Service workflows**.
3. Add a new service workflow of the type e-Boks message handler, and enter a name and description, and then click **Create**.
4. Point to the **e-Boks message handler** service workflow that you just created, and click **Edit parameters**, and fill in the parameters. For descriptions and examples, refer to the table below.

Name	Description	Value
DispatcherName	The dispatch type listed in the **Dispatch Type** list in the **Process Dispatchers**. It is used when retrieving unread messages.	
WatchInterval	Interval in seconds between SmartPost checking e-Boks for receipt of new messages.	300

Name	Description	Value
RetryCount	The number of retries before messages are abandoned.	5
DefaultCaseNo	The case number a predefined case (a dossier) on which incoming messages that cannot be saved on a specific case will be saved. The case must always be open.	
EBoksInboundMessagePartyRole	The role of the party on the received e-Boks message. If the setting is not specified, the **Sender** role (Afsender) will be used.	Sender
IncomingDocumentType	The document type that will be assigned to the e-Boks message when it is saved on a case. For example, I (Incoming). The setting must match the settings for the custom domain AT.	I
DPIncomingSource	Origin of the incoming messages and their attachments as retrieved from e-Boks. For example, DP (Digital Post). The setting must match the settings for the custom domain AKTOPR.	DP
UseEBoksMailMap	If turned on, unsolicited messages sent from e-Boks to subunits in your organization will be saved on specific cases that are defined for each of the subunits. You specify the cases when you map e-Boks mailboxes for subunits to cases in Configuration Management. **Note:** If the mapping of e-Boks mail-boxes and subdivisions does not work, the received messages will be saved on the default case that you have specified	

Name	Description	Value
	in the **DefaultCaseNo** parameter.	
ValidationHour	The time of the day when the validation of the contact hierarchy is scheduled. By default, it is 01:00 in the morning. e-Boks only allows access to the contact hierarchy once a day between midnight and 06:00. Enter time in the format 1 (01:00), 2 (02:00), and so on. See Configure validation of a contact hierarchy.	1
ValidateAtStartup	Starts the validation of the contact hierarchy when the service workflow is started. Use this parameter primarily for testing purposes. In production, this parameter has no effect. In production, the validation will only happen when the time specified in the **ValidationHour** parameter is met. By default, this parameter is turned off.	
OpenClosedCase	If turned on, a closed case is reopened if a message is received. The case will remain open.	

Handle e-Boks messages sent to subunits

If your organization receives unsolicited messages that are sent to subunits such as, for example, different authorities or subdivisions, you can configure the e-Boks message handler service workflow to save the messages on specific cases that are mapped to specific subunits.

To receive messages from the subunits' mailboxes in e-Boks and save the messages on specific cases in WorkZone, follow these steps:

1. Have mailbox names and IDs from e-Boks Administrationsportal at hand.
2. Create the cases you want to save received messages on.
3. Map e-Boks mailboxes and mailbox IDs to the cases on which you want the messages to be saved.
4. Enable receipt of messages from the subunits' mailboxes in an existing or a new e-Boks message handler service workflow.

Look up e-Boks mailbox names and IDs in Administrationsportal

To configure WorkZone Process to save received messages from the subunits' e-Boks mailboxes, you need to know the names and IDs of the e-Boks mailboxes as they have been defined in the e-Boks Administrationsportal.

1. Log in to e-Boks Administrationsportal as NemID-administrator (LRA), and click the **Kontaktmuligheder** tab.
2. Under **Postkasser**, click **Vis postkasser**.
3. Click **Info** next to the mailbox.
4. Note the mailbox ID (**Postkassens ID**) and the name (**Navn**).

Create default cases per subdivision mailbox

- In WorkZone Client, create a case per mailbox you want to save received messages on.

Map e-Boks mailboxes to cases

The next step is to map the e-Boks mailboxes to WorkZone units and cases.

1. Open WorkZone Configurator.
2. Go to **Process** > **e-Boks mail mapping**.
3. Enter the name of the e-Boks mailbox in the **Mailbox name** field and the corresponding ID in the **MailBox ID** field.

4. Select the responsible WorkZone unit.
5. Select the case that you want to save received messages on.

See also e-Boks mailbox mapping in the WorkZone Configurator Administrator Guide.

Enable receipt of messages from subunit mailboxes

1. In WorkZone Configurator, go to **Process** > **Service workflows**.
2. Point to an existing **e-Boks message handler** service workflow or create a new one, and click **Edit parameters**
3. Turn on the UseEBoksMailMapparameter.

To create a new service workflow, see Configure an e-Boks Message Handler service workflow.

Configure validation of a contact hierarchy

Each time the e-Boks message handler service workflow is started, it validates that the contact hierarchy in the e-Boks Administrationsportal matches the mapping of e-Boks mailboxes and cases that are configured in WorkZone Configuration Management. See the ValidationHour and ValidateAtStartup parameters and Map e-Boks mailboxes to cases.

If the validation finds an e-Boks mailbox that does not exist in the **WzpEboksMailMap** register, it is created and shown in WorkZone Configuration Management, and a warning is inserted in the event log:

"The contact mailbox <name of mailbox> with the mailbox <ID> is added to the e-Boks mail map. Must be configured."

If a mailbox already exists in the **WzpEboksMailMap** register and is shown in WorkZone Configuration Management but it is not yet configured, a warning is also added in the event log:

"The contact mailbox <name of mailbox> is not configured in the e-Boks mail map."

In both cases, you need to complete the configuration in WorkZone Configuration Management.

Handling receipt of messages on closed cases

In some situations, the e-Boks message handler service workflow may require updating closed cases.

There are three types of cases that messages can be saved on.

1. The default case. The case that is specified in the **DefaultCaseNo** parameter.
2. A predefined case that works as a dossier for all unsolicited messages sent to a specified subunit's mailbox. The case is mapped to a specific subunit's mailbox to receive unsolicited messages. See Handle e-Boks messages sent to subunits.
3. The case to which replies to a specific e-Boks message are saved. If the message is a reply, the message is saved on the same case that the original SmartPost message was sent from.

If any of these cases are closed, the service workflow will act differently depending on whether corporate access codes exist.

No corporate access codes

- If the default case (1) and a subunit's predefined case (2) are closed , they will be reopened and messages will be saved on these cases. If the cases have been closed by mistake, they will be reopened automatically and remain open. These cases must always be open.
- If the case to which replies to a specific e-Boks message are saved is closed (3), the case will be reopened and the reply message will be saved on it. This is the default behavior. If you have configured WorkZone to not allow reopening of closed cases (see OpenClosedCase parameter), the message will be saved on the default case (1).

Corporate access codes

- If the default case (1) and a subunit's predefined case (2) are closed, they will be reopened and messages will be saved on these cases. If the cases have been closed by mistake, they will be reopened automatically and remain open. These cases must always be open.
- If the case to which replies to a specific e-Boks message are saved is closed (3), the case will be reopened and the reply message will be saved on it. This is the default

behavior. If you have configured WorkZone to not allow reopening of closed cases (see OpenClosedCase parameter), the case mapped to the authority's mailbox is looked up and the message is saved on the authority's case (the dossier).

WorkZone identifies the authority's case based on the file key (`FileKey`) from the case that the original message was sent from. The authority on the case is identified, and if a a case exists for the authority, the message will be saved on this case.

> **Tip:** You can create a case for the authority that works as a dossier for all unsolicited messages sent to a specified subunit's mailbox. To do this, map the authority's mailbox to a case, and selecting the authority as responsible subunit. See Map e-Boks mailboxes to cases.

- If there is no mapping found for the subunit/authority, the message is saved on the default case (1).

Dispatcher error handling

If SmartPost fails due to e-Boks, KMD Printcenter, or Strålfors errors, error messages with error codes are written to the workflow log. See Process logging in the WorkZone Operations Guide. SmartPost performs actions according to the type of errors. See the topics below for a list of errors, descriptions, and actions.

---

e-Boks errors

If digital mail does not work due to e-Boks errors, e-Boks returns different error codes and messages. The error messages are written to the workflow log. See Investigate failed processes in the workflow log in the WorkZone Operations Guide.

SmartPost performs the following action depending on the type of error:

- **Notify**

  The dispatch failed and the workflow is ended. A notification email that informs about the failed dispatch is sent to the process owner.

- **Retry**

  SmartPost tries to send the message through the same dispatcher once more.

- **Try next**

  SmartPost tries to send the message to the next dispatcher in the dispatch sequence.

The table below lists possible e-Boks errors and describes how you can possibly handle the errors. Some types of errors can only be handled by KMD.

Error type 1: Not a SmartPost error

These error codes can only be part of replies on a request that is not used by SmartPost, and therefore these error messages should never occur. If you get an error message of this type anyway, please forward the message to your organization's WorkZone administrator or to KMD Support for further analysis and action.

Error type 2: Internal program error

These error codes occur in case of an internal program error. Please forward this type of error message to your organization's WorkZone administrator or to KMD Support for further analysis and action.

Error code	e-Boks error message	SmartPost action	To fix the error...
2001	XML ikke valid XML is not valid	Try next	No action required. SmartPost tries to send the message through another dispatcher.
2002	Max graense for data overskredet The max limit of data is exceeded	Notify	A notification email about the failed dispatch is sent to the process owner. Please check that the values of the **MaxCombinedMessageLength** parameter in the SmartPost process parameters and the **MaxDocumentSize** parameter for the e-Boks dispatcher are higher

Error code	e-Boks error message	SmartPost action	To fix the error...
			than the limit set by e-Boks. The values must be lower than the limit defined by e-Boks.
2003	Servicebesked indeholder flere tegn end tilladt The service message contains more characters than allowed	Try next	No action required. SmartPost tries to send the message through another dispatcher.
3000	Ingen adgang No access	Notify	The certificate does not provide access to the specified system. Please check your configuration of the e-Boks dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and then verify that the **SenderSystemId** setting aligns to your configuration in e-Boks.
3001	Angivne SystemId er ikke af forventet systemtype The specified SystemId does not correspond to a system of the expected type	Notify	SmartPost expects that the system, which is configured in e-Boks is a "Afsendersystem" (dispatch system). Please log into the e-Boks Administration Portal, and identify the "Afsendersystem" that you want SmartPost to use, and note the identity of the system. Next, open your configuration of e-Boks dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and ensure that value of the SenderSystemId

Error code	e-Boks error message	SmartPost action	To fix the error...
			settings is sat to that identity.
3002	Manglende rettighed til kald af operation Insufficient rights to calling the operation	Notify	See Error type 1: Not a SmartPost error.
3003	Certifikat mangler i request The certificate is missing in a request	Notify	• Check your configuration of the e-Boks dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and then verify the **CertificateThumbprint** setting. • Check that your certificate is valid.
3004	Certifikatet er ugyldigt The certificate is invalid	Notify	• Check your configuration of the e-Boks dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and then verify the **CertificateThumbprint** setting. • Check that your certificate is valid.

Error code	e-Boks error message	SmartPost action	To fix the error...
3005	Systemet er ikke opsat til REST The system is not configured to support the REST	Notify	Please log into the e-Boks Administration Portal and identify the "Afsendersystem" (dispatch system) that you want SmartPost to use. Open the configuration page of the system, and verify that the interface to send messages (Hvilken snitflade anvendes til at afsende post?” is configured to System-til-system.
3006	Systemet er ikke opsat til SMIME The system is not set up for SMIME	Notify	See Error type 1: Not a SmartPost error.
3007	X-On-Behalf-Of header er påkrævet for dette kald X-On-Behalf-Of header is required for this call	Notify	See Error type 1: Not a SmartPost error.
3008	Slutbruger er ikke dokumentboksmodtager og har ikke adgang The end user is not a document box recipient and has no access	Try next	No action required. SmartPost tries to send the message through another dispatcher.
3009	Slutbruger er hverken servicebeskedmodtager eller dokumentboksmodtager The end user is neither a service messages recipient or a document box recipient	Try next	No action required. SmartPost tries to send the message through another dispatcher.
3010	Operation kaldt i ugyldigt tidsrum The operation is called in an invalid	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
	time span		
4000	Ugyldig queryparameter Invalid queryparameter	Notify	See Error type 1: Not a SmartPost error.
4003	Ukendt bilagId. Unknown supplementary document ID	Notify	See Error type 1: Not a SmartPost error.
4005	Default indholdstype ikke opsat på system The default content type is not set up on the system	Notify	See Error type 1: Not a SmartPost error.
4007	Ukendt slutbruger Unknown end user	Try next	No action required. SmartPost tries to send the message through another dispatcher.
4008	Antal vedhæftninger ikke lovlig Number of attachments is invalid	Try next	No action required. SmartPost tries to send the message through another dispatcher.
4010	Ukendt meddelelsesid Unknown message ID	Notify	See Error type 2: Internal program error.
4011	Ukendt vedhaeftningsid Unknown attachment ID	Notify	See Error type 2: Internal program error.
4012	Ukendt indholdstype Unknown content type	Notify	See Error type 2: Internal program error.
4013	Ukendt tilmeldingsgruppe Unknown subscription group	Notify	See Error type 1: Not a SmartPost error.
4016	Ukendt postkasse Unknow mailbox	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
4017	Ukendt postkasseEmne Unknown mailbox subject	Notify	See Error type 1: Not a SmartPost error.
4018	Hverken CPR eller CVR nummer er angivet Neither a CPR nor a CVR number is registered	Notify	A recipient does not have CPR or CVR number. Please check the contact information on the **Contact** detail page in WorkZone Client, and add missing information.
4019	Både CPR og CVR nummer er angivet Both CPR and CVR number is registered	Notify	A recipient has both a CPR or CVR number. Please check the contact information on the **Contact** detail page in WorkZone Client, and remove incorrect information.
4020	Dialogtråd er ikke i korrekt format Dialog thread is not in the correct format	Notify	See Error type 1: Not a SmartPost error.
4021	Ukendt dialogtråd Unknown dialog thread	Notify	See Error type 1: Not a SmartPost error.
4022	Afhentningssystem er opsat til at hente fra indbakke The dispatch system is set up to load from the inbox	Notify	See Error type 1: Not a SmartPost error.
4023	Afhentningssystem er opsat til at tømme postkasse The dispatch system is set up to empty the mailbox	Notify	See Error type 1: Not a SmartPost error.
4024	Ugyldig CVR nummer format Invalid CVR number format	Notify	A recipient has an invalid CVR number. Please check the con-

Error code	e-Boks error message	SmartPost action	To fix the error...
			tact information on the **Contact** detail page in WorkZone Client, and correct the CVR number.
4025	Fællesoffentlige portal forventer angivelse af myndighed The common public portal expects specification of authority	Notify	See Error type 1: Not a SmartPost error.
4026	Ugyldig format på meddelelsesId Invalid format on meddelsesId	Notify	See Error type 2: Internal program error.
4027	Angiv mindst et af felterne MobilNummer / EpostAdresseFoerste Specify at least one of the MobilNummer / EpostAdresseFoerste fields	Notify	See Error type 1: Not a SmartPost error.
4028	Svarpostkasse skal angives når svartype er sat til 'angivet' The reply mailbox must be specified when the reply type is set to 'angivet'	Notify	See Error type 1: Not a SmartPost error.
4029	Ingen kvitteringsliste tilgængelig No receipt list is available	Notify	See Error type 1: Not a SmartPost error.
4030	Ukendt kviteringslisteId No receipt list is available	Notify	See Error type 1: Not a SmartPost error.
4031	Tilmeldingsliste er ikke opsat for system Subscription list is not set up for the system	Notify	See Error type 1: Not a SmartPost error.
4032	Ukendt tilmeldingslisteId Unknown tilmeldingslisteId	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
4033	Ukendt dellisteId Unknown dellisteId	Notify	See Error type 1: Not a SmartPost error.
4034	Listen er blevet forældet - start forfra The list is out of date - start over again	Notify	
4035	Liste ikke tilgængelig The list is not accessible	Notify	See Error type 1: Not a SmartPost error.
4036	Kvittering ikke muligt for komplette lister Receipt is not possible for complete lists.	Notify	See Error type 1: Not a SmartPost error.
4037	Registret har ikke tilkøbt adgang til slutbrugerlister The register has not purchased access to end user lists	Notify	See Error type 1: Not a SmartPost error.
4038	StartDato mangler - påkrævet søge-parameter StartDato is missing - required search parameter	Notify	See Error type 1: Not a SmartPost error.
4039	SlutDato mangler - påkrævet søge-parameter SlutDato is missing - required search parameter.	Notify	See Error type 1: Not a SmartPost error.
4040	IkkeTilmeldte - ugyldig format IkkeTilmeldte - invalid format	Notify	See Error type 1: Not a SmartPost error.
4041	Myndighed - ugyldig format Myndighed - unknown format	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
4042	CPR - ugyldig format The format of the CPR number on a recipient is invalid	Notify	See Error type 2: Internal program error.
4043	CVR - ugyldig format The format of the CVR number on a recipient is invalid	Notify	See Error type 2: Internal program error.
4044	Indholdstype og tilmeldingsgruppe kan ikke angives samtidig The content type and subscription group cannot be used at the same time	Notify	See Error type 1: Not a SmartPost error.
4045	StartDato - ugyldig format StartDato - invalid format	Notify	
4046	SlutDato - ugyldig format SlutDato - invalid format	Notify	
4047	Ukendt slutbrugerlisteId Unknown slutbrugerlisteId	Notify	See Error type 1: Not a SmartPost error.
4048	Netop et af felterne MyndighedTilmeldtIndikator og AlleMyndighederTilmeldtIndikator skal være udfyldt At least one of the fields MyndighedTilmeldtIndikator or AlleMyndighederTilmeldtIndikator must be filled in	Notify	See Error type 1: Not a SmartPost error.
4049	Registret er ikke opsat til at modtage slutbrugerlister The register is not set up to receive	Notify	

Error code	e-Boks error message	SmartPost action	To fix the error...
	end user lists		
4050	Hverken VedhaeftningNavn eller Fil-formatNavn må være udfyldt for en vedhæftning som refererer et bilag Neither VedhaeftningNavn nor Fil-formatNavn need to be filled for an attachment that refers to a sup-plementary document	Notify	See Error type 1: Not a SmartPost error.
4051	Feltet SlutbrugerNavn skal være udfyldt The SlutbrugerNavn field must be filled in	Notify	See Error type 1: Not a SmartPost error.
4052	Indholdsdata mangler for en afsendelse / vedhæftning Content data is missing for a dispatch / attachment	Notify	See Error type 2: Internal pro-gram error.
4053	Materialet er ikke tilknyttet systemet The material is not registered in the system.	Notify	Check that your configuration of the e-Boks material in WorkZone Configurator aligns to the configuration in e-Boks. Click **Process** > **e-Boks mater-ials**.
4054	Vedhæftninger må ikke optræde med samme navn Attachments must not have the same name	Notify	See Error type 2: Internal pro-gram error.
4055	Afvist pga. virus Rejected due to virus	Notify	See Error type 2: Internal pro-gram error.
4056	Ugyldig tilmeldingsgruppe	Notify	See Error type 1: Not a

Error code	e-Boks error message	SmartPost action	To fix the error...
	(tilhørsforhold privat / virksomhed) Invalid subscription group (affiliation private / company)		SmartPost error.
4057	Ugyldigt tegn i ved vedhæftningsfilnavn Invalid character in attachment file name	Notify	See Error type 2: Internal program error.
4059	Materiale findes ikke The material cannot be found	Notify	Check that your configuration of the e-Boks material in WorkZone Configurator aligns to the configuration made in e-Boks. Click **Process** > **e-Boks materials**, and check if the e-Boks material has been configured.
4060	Kunden findes ikke The customer does not exist	Notify	Please contact e-Boks for verification of your legal agreement and the state of your registration.
4061	Samme bilag er angivet flere gange The same supplementary document is attached several times	Notify	This error cannot occur in the current version of SmartPost. SmartPost merges all attachments into one main PDF document. However, two additional meta data documents are attached (DKALAfsenderMetadata.xml and Attention.xml). The user has no control of these attachments nor their content.
4062	Dokument er ikke ejet af kunde	Notify	See Error type 1: Not a

Error code	e-Boks error message	SmartPost action	To fix the error...
	The document is not owned by the customer		SmartPost error.
4063	Tidsfrist er ikke angivet No deadline is specified	Notify	See Error type 1: Not a SmartPost error.
4064	Emnet tilhører ikke den angivne postkasse The subject does not belong to the specified maillbox	Notify	See Error type 1: Not a SmartPost error.
4065	Angivet bilags nr findes ikke eller bilaget tilhører ikke kunden The specified supplementary document No. does not exist or the supplementary document does not belong to the customer.	Notify	See Error type 1: Not a SmartPost error.
4066	Servicebesked kan ikke have bilag eller vedhæftning A service message cannot have supplementary documents or attachments	Notify	See Error type 1: Not a SmartPost error.
4067	Antal bilag og vedhæftninger maks 10 stk ialt The number of documents and supplementary documents exceeds the maximum number of 10 documents	Notify	Error type 2: Internal program error.
4068	Afsendelsestidspunkt kan ikke ændres, når bruger ikke er tilmeldt materialet The dispatch time cannot be changed when the user is not subscribed to the	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
	material		
4069	Vedhæftningen indeholder et ugyldigt navn The attachment contains an invalid name	Notify	See Error type 2: Internal program error.
4070	Ukendt SystemNr Unknown SystemNr	Notify	See Error type 1: Not a SmartPost error.
4071	Feltet MeddelelsesTitelTekst indeholder mere end 50 tegn The MeddelelsesTitelTekst field contains more than 50 characters	Notify	In the **Send SmartPost** dialog box, reduce the size of the title, and resubmit the dispatch.
4072	Et register kan ikke afmelde tilmeldingsgrupper som indeholder meddelelser A register cannot unsubscribe subscription groups that contain messages	Notify	See Error type 1: Not a SmartPost error.
4073	Ugyldig email Invalid email	Notify	See Error type 1: Not a SmartPost error.
4074	Ugyldig brug af AutoTitel i Titelfelt Invalid of use of AutoTitel in Titelfelt	Notify	See Error type 1: Not a SmartPost error.
4075	Ugyldig format på AutoTitel Invalid format on AutoTitel	Notify	See Error type 1: Not a SmartPost error.
4076	Systemet er opsat til Push The system is set to Push	Notify	See Error type 1: Not a SmartPost error.
4080	For at slutbruger kan tilmeldes Nem SMS skal vedkommende have	Notify	See Error type 1: Not a SmartPost error.

Error code	e-Boks error message	SmartPost action	To fix the error...
	opgivet et mobilnummer For the end user to subscribe to Nem SMS, the end user must have provided a mobile number		
4086	Slutbruger er blevet fritaget. The end user has been exempted	Try next	See Error type 1: Not a SmartPost error.
6001	Ikke muligt at foretage opdateringer - afsendelsen er afsendt Not possible to perform updates - the dispatch has been sent	Notify	See Error type 1: Not a SmartPost error.
6002	Arkiveringsmappe er ikke opsat The archive folder has not been set up	Notify	See Error type 1: Not a SmartPost error.
6003	Slutbrugeren er ikke tilmeldt ind-holdstypen The end user is not subscribed to the content type	Try next	See Error type 1: Not a SmartPost error.
6004	Afsendelsesdato må højest være 5 dage frem i tiden The dispatch date must only be 5 days from now	Notify	See Error type 1: Not a SmartPost error.
1000	Serverfejl Server error	Notify	The e-Boks server has reported an internal server error. The SmartPost process cannot detect if the message has been sent or not. The process owner must investigate if the message has been sent.

Error code	e-Boks error message	SmartPost action	To fix the error...
			For example, the server error may occur after the message is received but before the status/receipt is reported back to WorkZone. In this case, the process owner will be notified about the failed dispatch. The process will be completed and the history document will be generated and show status of each dispatch.

Strålfors errors

If remote print does not work due to Strålfors errors, Strålfors returns different error codes and messages. The error messages are written to the workflow log. See Investigate failed processes in the workflow log in the WorkZone Operations Guide.

SmartPost performs the following action depending on the type of error:

- **Notify**

  The dispatch failed and the workflow is ended. A notification email that informs about the failed dispatch is sent to the process owner.

- **Retry**

  SmartPost tries to send the message through the same dispatcher once more.

- **Try next**

  SmartPost tries to send the message to the next dispatcher in the dispatch order.

- **Complete**

  The workflow continues and is ended successfully.

The table below lists possible Strålfors errors and describes how you can possibly handle the errors. Some types of errors can only be handled by KMD.

Error type 1: Not a SmartPost error

These error codes can only be part of replies on a request that is not used by SmartPost, and therefore these error messages should never occur. If you get an error message of this type anyway, please forward the message to your organization's WorkZone administrator or to KMD Support for further analysis and action.

Error type 2: Internal program error

These error codes occur in case of an internal program error. Please forward this type of error message to your organization's WorkZone administrator or to KMD Support for further analysis and action.

> **Note:** When support is mentioned in the **Strålfors error description** column below, it refers to the Strålfors support.

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
100-2	Uventet systemfejl	Kontakt supporten.	Retry	
101-0	Afsendersystem kunne ikke findes The dispatch system cannot be found	Afsendersystem kendes ikke af Strålfors Connect. Hvis aftale er indgået, så kontakt venligst supporten.	Notify	Check the Strålfors dispatcher configuration in WorkZone Configurator. Click **Process** > **dispatcher** > Strålfors, and then check the

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
				SenderSystemID setting.
101-2	Tilslutningsaftalen for afsendersystemet er ikke godkendt The agreement for the dispatch system is not approved	Afsendersystem har ikke en godkendt aftale. Hvis aftalen allerede er indgået, så kontakt venligst supporten.	Notify	See Error type 1: Not a SmartPost error.
101-3	Skemafejl i afsendt besked Schema error in the dispatched message	Xml'en skal overholde XSD skemaet.	Notify	See Error type 1: Not a SmartPost error.
110-0	Forsendelse type kunne ikke findes The dispatch type could not be found	Den anvendte forsendelsestype på forsendelsen findes ikke i Strålfors Connect. Benyt en anden forsendelsestype og send forsendelsen igen. Eller kontakt support, hvis forsendelsestypen burde eksistere.	Notify	See Error type 2: Internal program error.
111-2	Forsendelsestypen har ikke en gyldig version The dispatch type does not have a valid version	Tjek i administrationsportalen, at den angivne forsendelsestype har en gyldig version.	Notify	See Error type 1: Not a SmartPost error.
111-3	Det angivne ForsendelsesTypeID passer ikke med default forsendelsestypen, der er	Forsendelsestypen er låst på afsendersystem. Find den låste forsendelsestype i administrationsportalen	Notify	

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
	låst på afsendersystemet The specified ForsendelsesTypeID does not match the default dispatch type that is locked in the dispatch system	og angiv denne eller undlad at angive forsendelsestypeID. Send forsndelsen igen.		
111-4	Forsendelsestype ikke angivet, og der er ikke angivet en default forsendelsestype på afsendersystemet The dispatch type is not specified, and the default dispatch type is not specified in the dispatch system	Angiv forsendelsestype eller opsæt en default-forsendelses på afsender-systemet i administrationportalen.	Notify	
120-0	JMS fejler JMS fails	Intern fejl i Strålfors Connect. Kontakt venligst supporten.	Retry	No action required. WorkZone tries to resend the message.
120-9	Indholdet i StreetBuildingIdentifier kan ikke fortolkes som husnummer og bogstav The content of the StreetBuildingIdentifier cannot be interpreted as house number and letter	Husnummer og bogstav kan ikke fortolkes til et nummer og et bogstav. Tjek at husnummer og bogstav er angivet korrekt.	Try next	See Error type 2: Internal program error.

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error…
121-1	SideKvantitet skal angives når meddelelsen kommer fra PrinterApp SideKvantitet must be specified when the message comes from PrinterApp	Fejlbesked, der kun gælder printerapplikationer.	Notify	See Error type 2: Internal program error.
121-2	AfsendelseIdentifikator allerede modtaget AfsendelseIdentifikator is already received	Det ID, der er angivet på Forsendelsen er allerede modtaget af Strålfors Connect. Angiv et andet id eller kontakt support.	Complete	No action required. WorkZone continues sending.
123-4	Landekoden skal indeholde en valid Landekode. Landekode <xxxx> er ikke valid The country code must contain a valid country code. The country code <xxxx> is not valid	Landekoden overholder ikke standarden i XML-schemaet. Ret op og send igen.	Notify	A recipient has an invalid address. Please check the contact information on the **Contact** detail page in WorkZone Client, and correct the country code.
123-5	Modtageradressen skal indeholde et validt dansk postnummer, hvis modtager adressen er dansk. Postnummer <xxxx> er ikke et validt dansk postnummer The recipient address must	Angiv et dansk postnummer for modtager.	Notify	A recipient has an invalid address. Please check the contact information on the **Contact** detail page in WorkZone Client, and correct the

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
	contain a valid Danish postal code, if the recipient address is Danish. The postal code <xxxx> is not a valid postal code			postal code.
123-7	Struktureret modtager adresse skal have dansk landekode A structured recipient address must have a Danish country code	Angiv dansk landekode for modtager	Notify	See Error type 2: Internal program error.
124-1	En adresse skal være angivet i Modtager-Adresse, når PaatrykModtager-AdresseIndikator er sat til true An address must be specified in i ModtagerAdresse when PaatrykModtager-AdresseIndikator is set to true	Sæt PaatrykModtager-AdresseIndikator til false eller angiv adresse på modtaget (struktureret eller ustruktureret).	Notify	See Error type 2: Internal program error.
124-3	AfsendelsesDatoTid må højst være 5 dage ud i fremtiden AfsendelsesDatoTid must only be 5 days from now	For at kunne sende til digital post må AfsendelsesDatoTid højst være 5 dage ud i fremtiden. Ret dato til en tidligere dato eller afvendt med at	Notify	See Error type 2: Internal program error.

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
		sende forsendelsen.		
124-5	Der forsøges at oprette forsendelser til en Masse-forsendelse, der har status lukket eller masse-forsendelsen findes ikke An attempt to create dispatches for a bulk dispatch, which has the status closed or the bulk dispatch does not exist	Der forsøges at oprette forsendelser til en Masse-forsendelse, der har status lukket. Opret en ny masse-forsendelse eller send forsendelsen som enkelt-forsendelse.	Notify	See Error type 1: Not a SmartPost error.
124-7	Der må ikke oprettes en forsendelse, der er del af en masseforsendelse med reference til en forsendelsestype, der er i test. You must not create a dispatch, which is part of a bulk dispatch with reference to a dispatch type, that is in test	Anvend en forsendelsestype der ikke er i test.	Notify	See Error type 1: Not a SmartPost error.
125-1	Der er ikke angivet materiale for test-afsender-system til digital post No material is specified for the test dispatch system for digital mail	Når en forsendelsestype er i test skal der være angivet et defafult materiale for test-afsendersystem til digital post. Angiv materiale under myndighed på admininistrationsportalen.	Notify	See Error type 2: Internal program error.

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
125-4	Landekodeidentifikationsskemaet er ukendt. Kun ISO_3166_ALPHA_2 og ISO_3166_ALPHA_3 er tilladt The country ode schema is unknown. Only ISO_3166_ALPHA_2 and ISO_3166_ALPHA_3 is allowed	Anvend landekode ISO 3166 ALPHA 2 eller ALPHA 3.	Notify	A recipient has an invalid address. Please check the contact information on the **Contact** detail page in WorkZone Client, and correct the country code.
126-1	Hastebrev kan ikke sendes som economique eller bulkmail Urgent letter cannot be sent as economique or bulkmail	Angiv en anden postkategori for forsendelsen. Postkategorien kan være Prioritaire, Rekommanderet, Rekommanderet med modtagerbevis eller Forkyndelse.	Notify	The print type selected in the **Send SmartPost** dialog box defines an invalid combination of postage category and urgency level. The print type defines an Economique combined with an urgency level set to High. This combination is not allowed. Please check your configuration of the Strålfors dispatcher in WorkZone Con-

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
				figurator. Click **Process** > **Print Types**, locate the invalid value, and correct it.
128-0	Den angivne produktionsplan (AllokeringsID) eksisterer ikke for forsendelsestypen (ForsendelsesTypeID) The specified production plan(AllokeringsID) does not exist for the dispatch type (ForsendelsesTypeID)	Tjek at produktionsplan og tilhørende forsendelsestype i Administrationsportalen, og angiv de korrekte værdier.	Notify	See Error type 1: Not a SmartPost error.
170-0	Intet klient certifikat medsendt No client certificated is sent	Medsend certifikat. Hvis certifikat er medsendt, så kontakt support.	Notify	Check your configuration of the Strålfors dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and then verify the **CertificateThumbprint** setting.
170-1	Ingen adgang No access	Kontakt supporten	Notify	

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
170-2	Certifikatet er blevet revokeret The certifivate has been revoked	Certifikatet er blevet revokeret. Tjek hvilket certifikat der er anvnedt til at oprette afsendesystemet og benyt dette certifikat til, at kalde servicen. Ellers kontakt support.	Notify	Check your configuration of the Strålfors dispatcher in WorkZone Configurator. Click **Process** > **Process dispatchers**, and then verify the **CertificateThumbprint** setting.
170-3	Certifikatet er ikke gyldigt The certificate is not valid	Certifikatetet er ikke fyldigt. Tjek hvilket certifikat der er anvnedt til at oprette afsendesystemet og benyt dette certifikat til, at kalde servicen. Ellers kontakt support.	Notify	Check your configuration of the Strålfors dispatcher in Work. Click **Process** > **Process dispatchers**, and then verify the **CertificateThumbprint** setting.
170-4	Certifikatet er ikke et VOCES, MOCES eller FOCES certifikat The certificate is not a VOCES, MOCES eller	Der anvnedes at andet certifikat, end de tilladte certifikat-typer (VOCES, MOCES og FOCES). Tjek hvilket certifikat der er anvnedt til at oprette	Notify	Please retrieve a VOCES, MOVES, or FOCES certificate, upload the public part to

Error code	Strålfors error message	Strålfors error description	SmartPost action	To fix the error...
	FOCES certifikat	afsendesystemet og benyt dette certifikat til, at kalde servicen. Ellers kontakt support.		Strålfors, and then add the private part to the certificate store of the machine on which WorkZone Process is installed.

OneTooX errors

If remote print does not work due to OneTooX errors, OneTooX returns various error codes and messages. The error messages are written to the workflow log and to the event log of the web server. See Investigate failed processes in the workflow log in the WorkZone Operations Guide..

SmartPost performs the following action depending on the type of error:

- **Notify**

  The dispatch failed and the workflow is ended. A notification email that informs about the failed dispatch is sent to the process owner.

- **Retry**

  SmartPost tries to send the message through the same dispatcher again.

- **Try next**

  SmartPost tries to send the message to the next dispatcher in the dispatch sequence.

- **Complete**

  The workflow continues and is ended successfully.

The table below lists possible OneTooX errors and describes how you can handle the errors. Some types of errors can only be handled by KMD. These error codes occur in case of an internal program error. Please forward this type of error message to your organization's WorkZone administrator or to KMD Support for further analysis and action.

Error code	OneTooX error message	SmartPost action	To fix the error...
10030	Dokumentet har ikke det rigtige format. Første side i et hoveddokument skal være A4 stående. The document does not have the correct format. The cover page in a main document must be A4 portrait.	Try next	Change the page layout of the main document before sending the SmartPost message. The first page of the document must be formatted as A4 portrait. If the first page is a protected address cover page or a copy recipient cover page, the cover page template must be corrected accordingly. See Configure templates.
	Destination is not allowed.	Notify	This error only occurs when a change has been made to the protocol that SmartPost and KMD Printcenter uses to communicate. This error can only be solved by a software update from KMD.
	DocumentType could not be found.	Try next	A valid document type must be configured, or a designated document type must be created. To achieve the full functionality of SmartPost, four document types must be created and configured. Contact KMD Printcenter who will create the document types. The configuration is made using WorkZone Configurator. The four document types must cover all combinations of color, black and white, and single or double-sided print. See OneTooX.
9300	Forsendelsen er	Try next	SmartPost messages sent to KMD Printcenter can-

Error code	OneTooX error message	SmartPost action	To fix the error...
	for stor til print. Det maksimalt tilladte antal ark er 240. The dispatch is too large for printing. Maximum allowed is 240 pages. Maximum allowed is 240 pages.		not contain more than 240 pages. If your dispatch exceeds 240 pages and you want to use KMD Printcenter, you must split your dispatch into several individual dispatches.
9207	Ukendt postmodtagerland. Unknown receiver country.	Notify	The recipient's address contains an unknown country code and therefore the dispatch cannot be sent. Country codes are standardized (ISO 3166-1). You can find the complete list of all valid country codes at https://countrycode.org/. The country code is part of the recipient's address information in WorkZone, and it is generally configured in WorkZone. To identify and correct unknown country codes, verify the configured country codes.
	Protocol URL schema or content type is not allowed.	Notify	This error only occurs when a change has been made to the protocol that SmartPost and KMD Printcenter uses to communicate. This error can only be solved by a software update from KMD.

Configure SmartPost to Digital Post 2

Configure e-Boks dispatcher to use Digital Post 2

To use the push service in SmartPost, the e-Boks end point must be changed for the e-Boks dispatcher to use the push service.

1. In WorkZone Configurator, click **Process**.
2. Click **Process dispatchers**.
3. Point to next to the e-Boks dispatcher you want to use and click **Edit**.
4. Change the values for the **ReceiverUrl** and **DP2Url** parameters.

Parameter	Description	Example
ReceiverUrl	The URL for receiving messages using Digital Post 2. If the parameter is left empty, the default URL in the **Url** parameter is used.	https://<host-or-data-base>/EboksPushService/api/MeddelelseV2
DP2Url	The URL for sending messages using Digital Post 2 API methods. If the parameter is left empty, the Digital Post 1 API methods will be used.	https://demo-api.e-boks.com/oio/rest/srv.svc/2

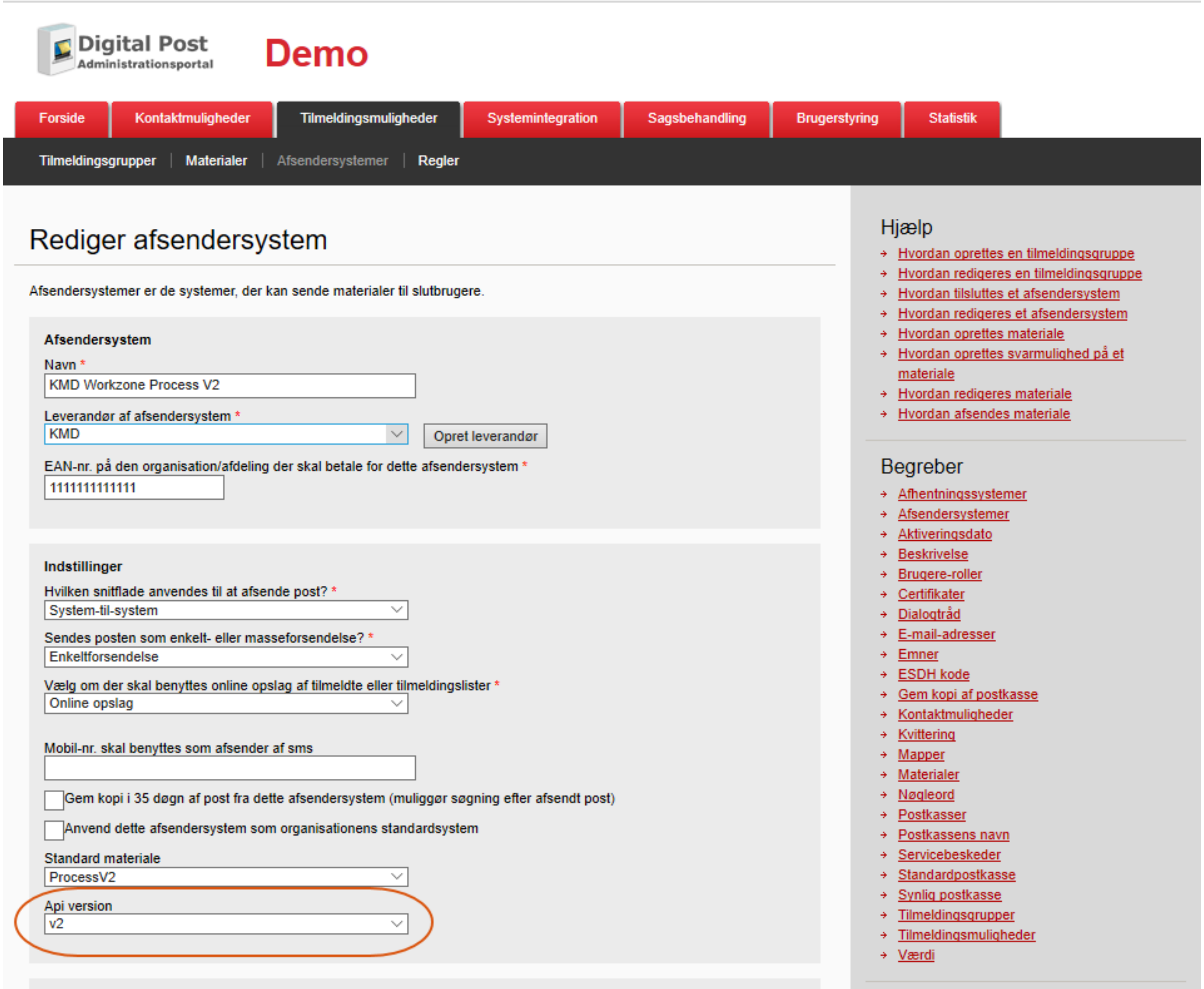
Configure the e-Boks Administrationsportal to use Digital Post 2

You create or update a e-Boks dispatch systems and retrieval systems in the e-Boks Administrationsportal.

Set up the dispatch system to use Digital Post 2

1. In the e-Boks Administrationsportal, go **Tilmeldingsmuligheder** > **Vis afsender-systemer** (View dispatch systems).
2. Click the dispatch system you want to configure and set up the API version to

use v2 in the **API Version** field.

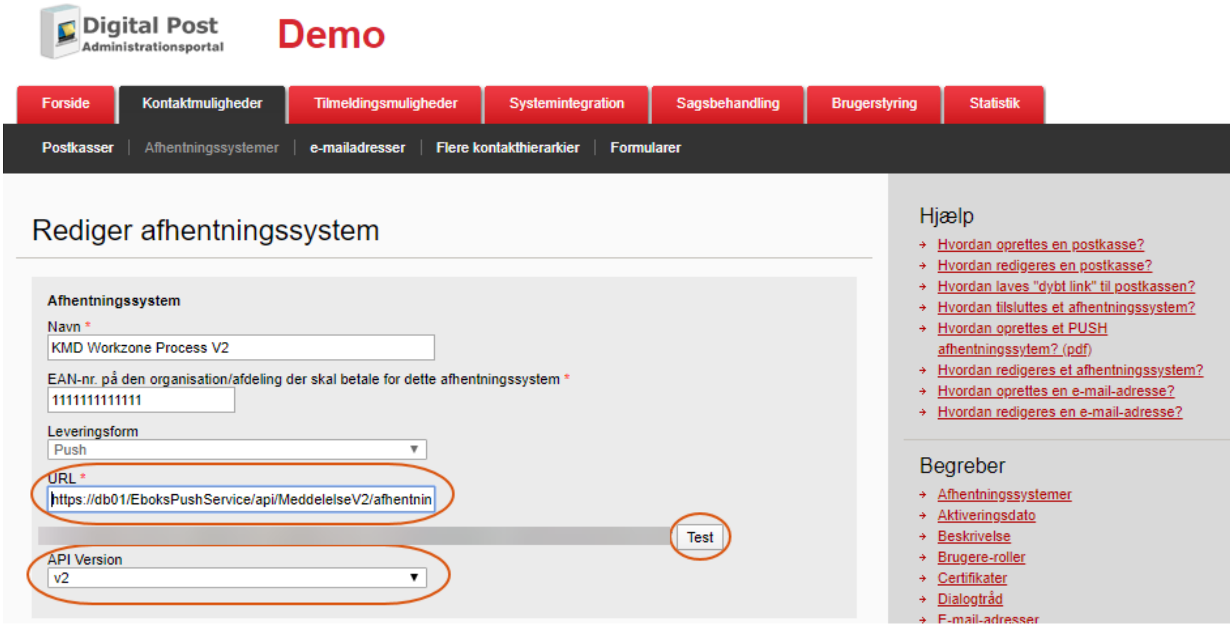


Set up the retrival system to use Digital Post 2

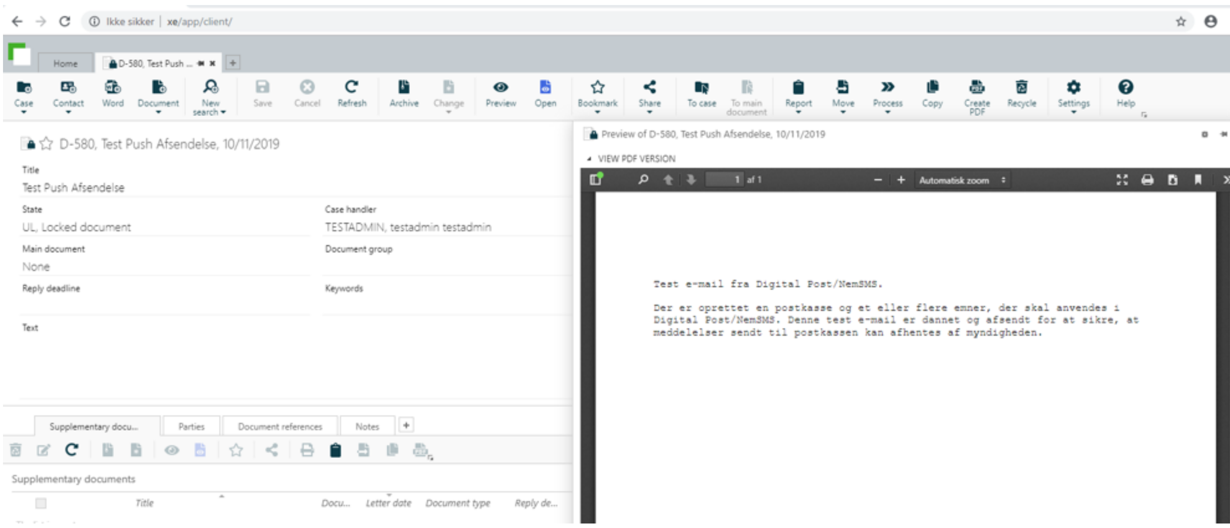
1. In the e-Boks Administrationsportal, go to **Kontaktmuligheder** > **Vis afhentningssystemer** (View retrieval systems).
2. Click the retrieval system you want to configure and set up the URL to use the v2 end point of the push service:

```
https://<data-
base>/Ebok-
sPushSer-
vice/api/MeddelelseV2/afhentningssystem/<systemid>
```

3. Set up the API version to use v2 in the **API Version** field.
4. To verify the whole setup, click the **Test** button.



If the call to the push service does not return OK (http 200), the http error message is shown in the top of the page in the Administrationportal. If the configuration is correct, the test letter should be received in WorkZone Process.



Configure SmartPost to use NgDP

In this article, you can read about how to configure SmartPost to use NgDP instead of Digital Post 2. The WorkZone integration to NgDP supports sending and receiving messages using the PULL model.

It is also possible to use the WorkZone integration with the PUSH model, but it is not recommended because both the infrastructure and the configuration is more complex than for the PUSH model.

For more information about NgDP, please refer to Next generation Digital Post (Næste generation Digital Post) on the Agency for Digitisation's website (Digitaliseringsstyrelsen).

Note: The SmartPost configurations that are described in this article also apply to WorkZone Mass Dispatch.

About the NgDP flow

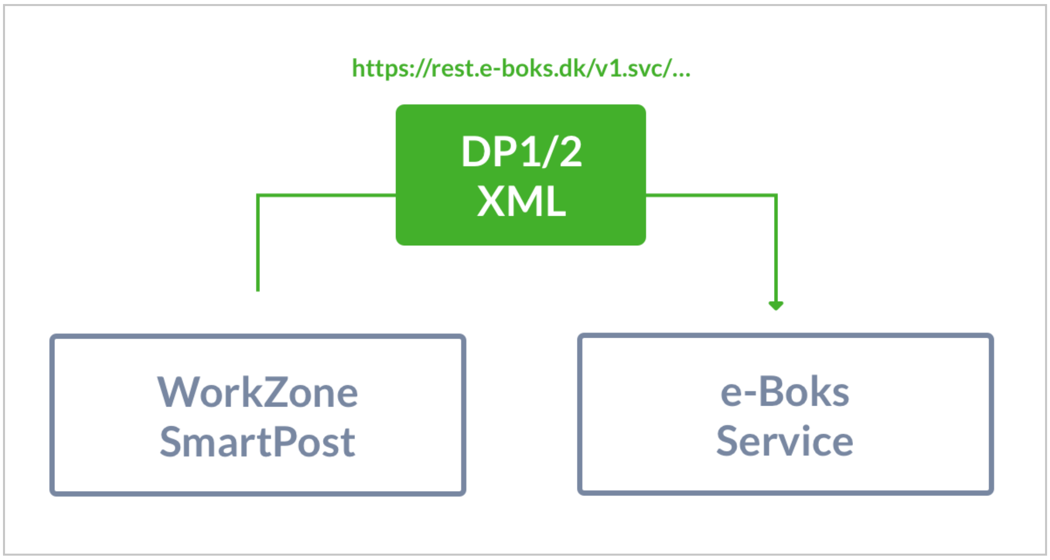
There are only minor changes to the integration between SmartPost and NgDP compared to the DP1 and DP2 integration. The sending and receiving messages functionality has been adjusted to ensure that all systems that use the DigitalPost 1 or 2 interfaces can be upgraded to use NgDP.

WorkZone now transfers additional meta data when sending messages to ensure support of NgDP ContactPoints. It is also possible to store the attributes that are associated with e-Boks materials in the WorkZone database and make them available to the push service when transforming messages to MeMo (message format used by NgDP).

For more information about MeMO, please refer to Det nye meddelelsesformat on the Agency for Digitisation's website.

Sending messages using the SmartPost flow without NgDP

In previous releases, the SmartPost flow for sending messages is illustrated below:

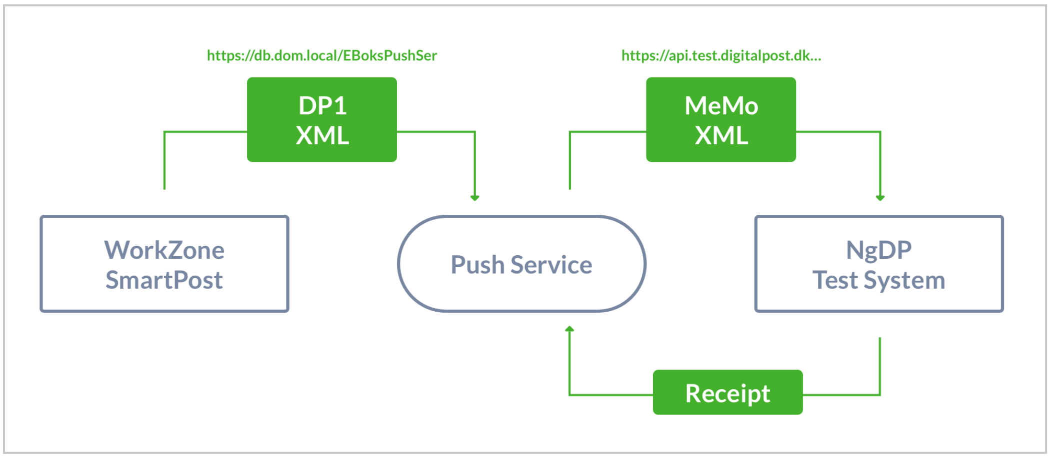


SmartPost uses an e-Boks dispatcher configuration to connect to the e-Boks endpoint. You can create dispatcher configurations in WorkZone Configurator. See Configure dispatchers.

NgDP flow when sending messages using SmartPost

When using NgDP to send messages from SmartPost, the e-Boks Push Service acts as a middle layer that converts outgoing messages to the MeMo format before sending the messages.

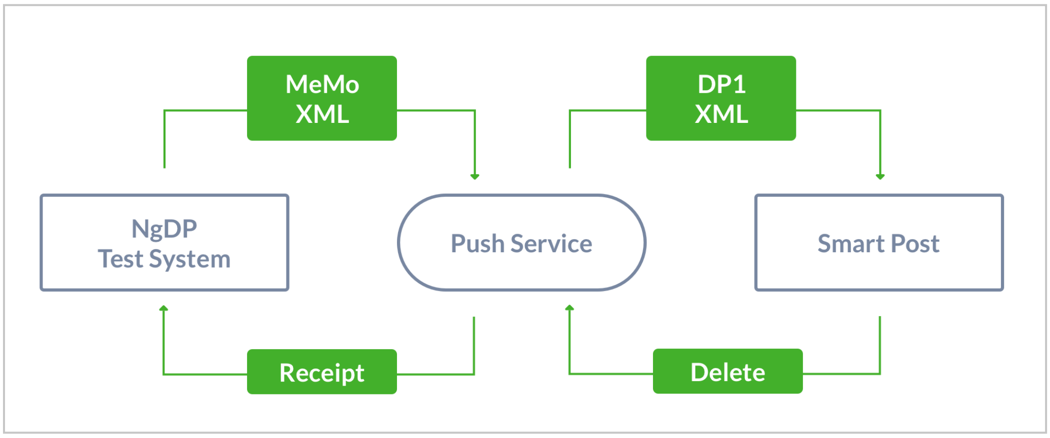
The NgDP flow that is used to send messages from SmartPost is illustrated below:



For more information about the WorkZone e-Boks Push Service, see Install and configure WorkZone e-Boks Push Service.

NgDP flow when receiving messages in SmartPost

When receiving messages from the NgDP system, the push service also acts as a middle layer and converts the incoming MeMo messages to DigitalPost 1 XML format that SmartPost can retrieve. When the messages have been handled, SmartPost invokes a DELETE request to the push service, and the push service then sends a receipt to NgDPreceiver system.



Prerequisites

To upgrade an installation from e-Boks to NgDP, the prerequisites listed below must be fulfilled.

Prerequisite:

- e-Boks Push Service must be installed on all WorkZone servers and on an external server if the PUSH model is used. See [Install and configure WorkZone e-Boks Push Service].
- The existing SmartPost e-Boks integration must be working before you start upgrading to NgDP.
- Access to the Agency for Digitisation's administrative portal named **Administrativ Adgang**. See Access to the Administrativ Adgang portal.
- Internet access to NgDP. See Internet access to NgDP.
- Certificates must be issued. See Certificates.

> - A combined sender and receiver system must be configured in the Agency for Digitisation's administrative portal named **Administrativ Adgang**. You can access the **Administrativ Adgang** portal with the link: https://admin.test.digitalpost.dk/login. For information about using and maintaining the portal, please refer to NgDP Ressourcer on the Agency for Digitisation's website (Digitaliseringsstyrelsen).
> - If you use SmartPost to receive incoming emails and you have configured mailboxes, you must create the contact hierarchy in the **Administrativ Adgang** portal.

Access to the Administrativ Adgang portal

You organization has received an email from the Agency for Digitisation that describes how to get access to the **Administrativ Adgang** portal.

To log in to the portal, you need to have an employee certificate (MOCES-certifikat) and you must be granted access rights to the portal. Please refer to Adgang til NgDP testmiljøet on the Agency for Digitisation's website (Digitaliseringsstyrelsen).

Internet access to NgDP

For SmartPost to be able to communicate with NgDP, it is required that both the web and agent server has Internet access to NgDP for NgDP to be able to access the WorkZonee-Boks Push Service that handles digital mail.

Environment	IP address/URL	Port	Protocol	Direction
Test	80.198.95.44 https://api.test.digitalpost.dk	443	HTTPS REST	Outgoing
Production	80.198.95.23 https://api.digitalpost.dk	443	HTTPS REST	Outgoing

Certificates

To establish the connection between WorkZone and NgDP, you need to install a FOCES certificate (Funktionscertifikat) on all WorkZone web and agent servers that communicate with NgDP. The certificates must be private versions (.p12 or .pfx) that require an access code during the installation. Each environment must have a unique certificate. For installation of certificates, follow the instructions for e-Boks and Strålfors certificates in the WorkZone Installation Guide.

Configure SmartPost to use NgDP

To configure SmartPost to use NgDP, you need to do the following:

- Create a sender/receiver system
- Configure contact points
- Configure an e-Boks dispatcher to use NgDP
- Configure a dispatch sequence to use NgDP
- Configure an e-Boks material to use NgDP
- Configure a service workflow to receive messages through NgDP
- Configure mail boxes for incoming messages

Create a sender/receiver system

When you upgrade from e-Boks to NgDP, there are specific requirements to IP addresses, creation of endpoints, and configuration of contact points.

IP addresses of WorkZone servers

When you create a sender/receiver system in the **Administrativ Adgang** portal, you need to specify the IP address of the WorkZone web and agent servers from which digital mail is received. If you have access to the Internet from the server, you can find the IP address by entering `myip.com`, which will list the public IP addresses of the server. Alternatively, contact your organization's operations service provider to get the IP addresses.

When you have created the sender/receiver system, you can download a PDF document that documents the configuration of the system. You should be aware of the following information that you will need in order to configure a WorkZone e-Boks dispatcher.

- **ID** of the sender/receiver system (for the **NgDpGuid** parameter).
- **API-Key** (for the **NgDpAuthorizationHeader** parameter).

See Configure an e-Boks dispatcher to use NgDP.

Create endpoints (applies to the PUSH model only)

The sender/receiver system requires an endpoint for receipts (kvitteringer) and an endpoint for messages (MeMo). Both of these endpoints must point to a public HTTPS endpoint that is exposed to the push service. You set up endpoints in the **Administrativ Adgang** portal. Depending on whether you use the PULL or the PUSH model, define the protocol as REST_PULL or REST_PUSH.

The receipt endpoint must be declared as:

```
<base address of push service>/api/MeMoV1/<systemid>/receipt
```

The message endpoint must be declared as:

```
<base address of push service>/api/MeMoV1/memos/?system-uuid-
d=<systemid>
```

When you have set up the sender/receiver system, make a note of the system ID and the authorization header as you will need them when you configure the WorkZone e-Boks dispatcher.

Configure contact points

Your organization must also define a contact point that specifies how citizens, companies, and authorities can send messages and replies to messages to your organization. The following applies to contact points:

- Always create a least one contact point for the receiver system. If you do not create a contact point, replies to messages will be sent to your standard mailbox, which may result in replies not being saved on cases in WorkZone.
- You can create and map multiple contact points to the same receiver system.
- You can configure contact points for citizens, companies, and authorities. You must specify at least one of the three options.

- If your organization only wants citizens, companies, and authorities to be able to reply to messages, it is possible to hide the contact point.

You can create and configure contact points in the **Administrativ Adgang** portal. A contact point has a GUID. When you have created the contact points and the GUIDs have been created, note down the GUIDs. You will need the GUIDs when you configure the WorkZone e-Boks dispatcher (the **NgDpConactPointGuid** parameter).

When you upgrade from e-Boks to NgDP, mailboxes must be mapped to contact points. See Configure mail boxes for incoming messages.

Configure an e-Boks dispatcher to use NgDP

Depending on whether you use the PULL or the PUSH model, you must configure specific NgDP parameters in the e-Boks dispatcher.

Configure an e-Boks dispatcher to use the NgDP PULL model

To use an NgDP pull system that is configured in the Agency for Digitisation's administrative portal **Administrativ Adgang**, you must create a new dispatcher that is configured to use the PULL model or change an existing dispatcher to use the PULL model.

1. In WorkZone Configurator, go to **Process** > **Process dispatchers**.
2. Fill in the following parameters:

Parameter	Description
SenderSystemId	The ID of the sender system. Enter an integer between 1000 and 99999999. If the integer is less than or equal to 9999, the system is considered as a test system and the test end point will be used. Important: The IDs must be unique. No other dispatcher can use the same number as the one specified in the **SenderSystemId** parameter. Note that the ID is not validated.

Parameter	Description
	The original purpose of the ID was a reference to the e-Boks system ID but because the NgDP system IDs are GUIDs, the IDs are only used by the e-Boks push service to identify the sender and receiver systems.
ReceiverSystemId	The ID of the receiver system. Enter an integer between 1000 and 99999999. If the integer is less than or equal to 9999, the system is considered as a test system and the test end point is used. Important: The IDs must be unique. No other dispatcher can use the same number as the one specified in the **ReceiverSystemId** parameter. Note that the ID is not validated. The original purpose of the ID was a reference to the e-Boks system ID but because the NgDP system IDs are GUIDs, the IDs are only used by the e-Boks push service to identify the sender and receiver systems.
Url	The URI for the Digital Post 1 interface of the local system, for example: `https://<database>/EboksPushService/api/MeddelelseV1`
CertificateThumbprint	The thumbprint that identifies a legal FOCES certificate (function certificate) or a VOCES certificate (company certificate). The certificate must be installed on all web and agent servers.
MaxDocumentSize	Same as e-Boks configuration. The maximum size of an e-Boks message specified in bytes. Messages that exceed this limit will not be sent to e-Boks. The default value is 78643200 (75 MB).

Parameter	Description
	Note: e-Boks determines the maximum size. If e-Boks changes the size, you can change this configuration accordingly but due to encoding you must reduce the size set by e-Boks by 25%. For example, if the size set by e-Boks is 99,5 MB, you must set the **MaxEBok-sDocumentSize** parameter to 99,5 MB * 75% = 75 MB.
SenderName	The short name of your organization that is used when present-ing the messages to the receiver in NgDP.
ReceiverUri	Do not fill in.
DP2Uri	Do not fill in.
NgDpGuid	The GUID of your sender/receiver system as defined in the **Administrativ Adgang** portal. You can see the GUID in the **ID** field on the **Afsender/modtagersystem** (Sender/receiver system) page in the **Administrativ Adgang** portal.
SenderCvr	The CVR number of your organization.
NgDpConactPointGuid	Your organization's contact point for replies to messages. Fill in this field if you have configured the e-Boks material to allow replies to messages. See Configure an e-Boks material to use NgDP. You can see the GUID of your organization's default reply point in the **Administrativ Adgang** portal on the **Kontaktstruktur** (Contact hierarchy) page.
NgDpAuthor-izationHeader	The AuthorizationHeader that has been generated by the **Admin-istrativ Adgang** portal when the sender/receiver system is defined. You can see the value in the **API-key** field on the **Afsender/modtagersystem** (Sender/receiver system) page in the **Administrativ Adgang** portal.
NgDpProtocol	Set to REST_PULL.
RemotePushSer-viceEndPoint	Do not fill in.


9, NgDP Pull - Dispatcher parameters
SenderSystemId
1111
ReceiverSystemId
2222
Url
http://db01/EboksPushService/api/MeddelelseV1
CertificateThumbprint
344CDEA8138E11AB1CB216A0AB6FAA07E08F19DD
MaxDocumentSize
7864320
SenderName
KMD
ReceiverUrl
DP2Url
NgDpGuid
040b2789-830d-4b9b-8ad6-318bbbe16bc7
SenderCvr
26911745
NgDpContactPointGuid
d75bb01a-a5ff-48e0-b95f-9d128dca7a68
NgDpAuthorizationHeader
Basic MDQwYjI3ODktODMwZC00YjliLThhZDYtMzE4YmJiZTE2YmM3OmVjODhjYzlkLTZjMWEtNGVIN
NgDpProtocol
REST_PULL
RemotePushServiceEndPoint

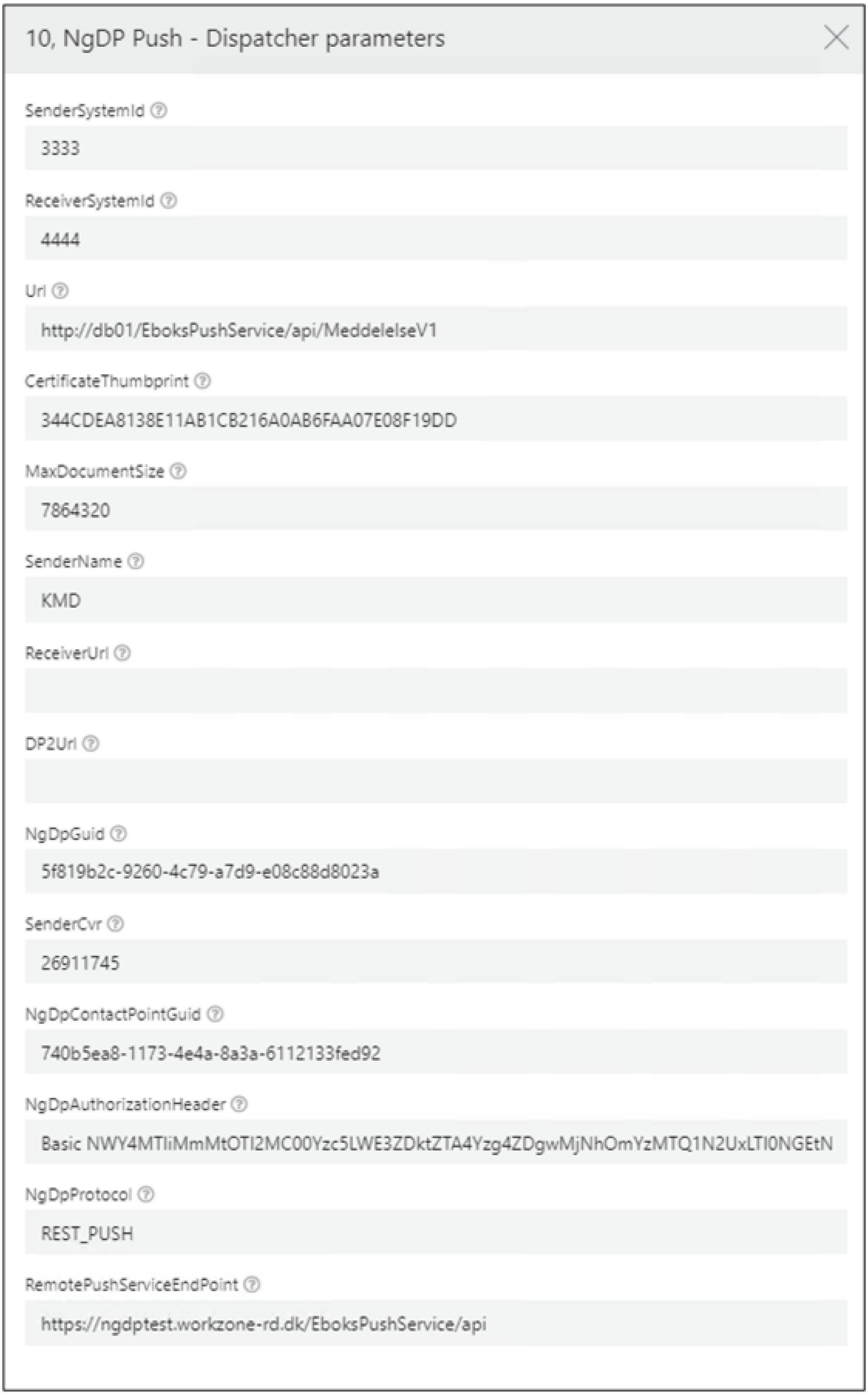
Configure an e-Boks dispatcher to use the NgDP PUSH model

To use an NgDP push system that is configured in the Agency for Digitisation's administrative portal **Administrativ Adgang** portal, you must create a new dispatcher that is configured to use the PUSH model.

Except for the **NgDPProtocol** and **RemotePushServiceEndPoint** parameters, you must configure a dispatcher that uses the NgDP PUSH model in the same way as a dispatcher that uses an NgDP pull system .

1. In WorkZone Configurator, go to **Process** > **Process dispatchers**.
2. Fill in the **NgDPProtocol** and **RemotePushServiceEndPoint** parameters:

Parameter	Description
NgDpProtocol	Set to REST_PUSH.
RemotePushServiceEndPoint	Point to a centralized push service. It must be the same push server that is configured to receive memos and receipts in the **Administrativ Adgang** portal.


10, NgDP Push - Dispatcher parameters
SenderSystemId
3333
ReceiverSystemId
4444
Url
http://db01/EboksPushService/api/MeddelelseV1
CertificateThumbprint
344CDEA8138E11AB1CB216A0AB6FAA07E08F19DD
MaxDocumentSize
7864320
SenderName
KMD
ReceiverUrl
DP2Url
NgDpGuid
5f819b2c-9260-4c79-a7d9-e08c88d8023a
SenderCvr
26911745
NgDpContactPointGuid
740b5ea8-1173-4e4a-8a3a-6112133fed92
NgDpAuthorizationHeader
Basic NWY4MTliMmMtOTI2MC00Yzc5LWE3ZDktZTA4Yzg4ZDgwMjNhOmYzMTQ1N2UxLTI0NGEtN
NgDpProtocol
REST_PUSH
RemotePushServiceEndPoint
https://ngdptest.workzone-rd.dk/EboksPushService/api

Configure a dispatch sequence to use NgDP

When you have created an NgDP specific dispatcher, you must add it to a new or existing dispatch sequence.

See Configure dispatch sequences.

Configure an e-Boks material to use NgDP

NgDP uses the material ID from e-Boks but the configuration that was previously done in the e-Boks Administration Portal is now done in WorkZone. You can create a new e-Boks material or fill in the NgDP related fields for an existing material.

1. In WorkZone Configurator, go to **Process** > **e-Boks materials**.
2. Create a new material or edit an existing material. The following fields are specific to NgDP:

Parameter	Description
Optional title prefix on shipped messages	Add a text that will prefix all titles on messages.
Permit users to reply	Turn on to allow recipients to reply to messages.
Messages are mandatory for the receiver	Turn on if the sender is allowed to send mandatory messages.
Messages are regarded as from an authority	Turn on if the sender is a public authority.
Messages are legal notifications	Turn on if the sender is allowed to send legal notifications.

See also Configure e-Boks materials.

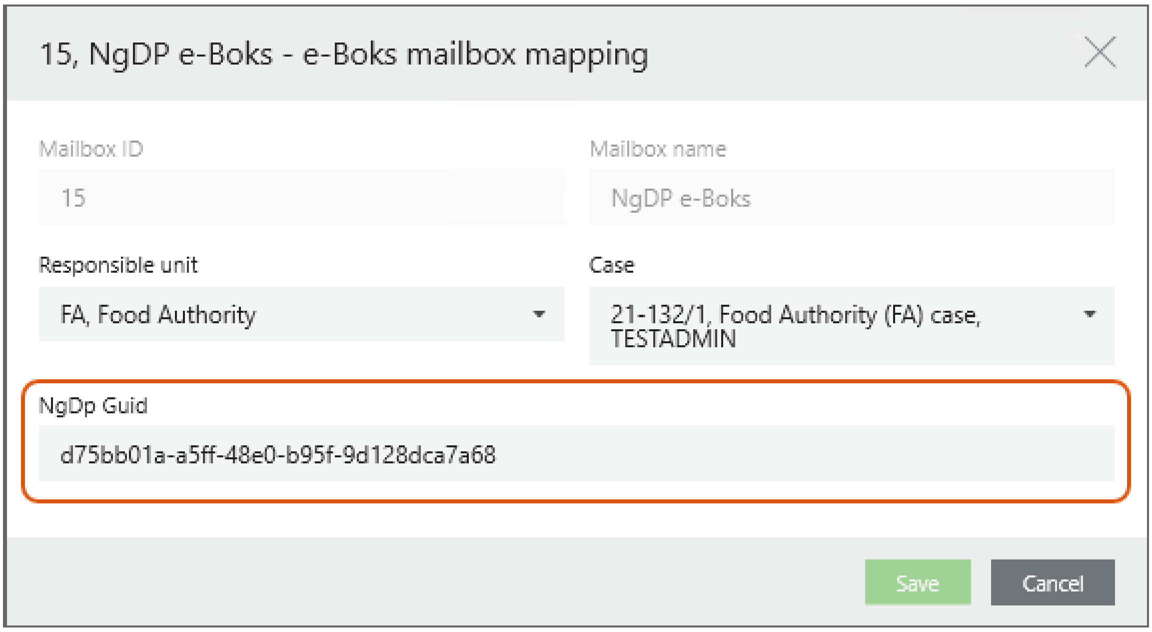
Configure a service workflow to receive messages through NgDP

To receive messages from e-Boks, you need to configure an e-Boks Message Handler service workflow.

See Configure an e-Boks Message Handler service workflow.

Configure mail boxes for incoming messages

If your organization has multiple mailboxes that are mapped to specific cases, you must fill in a new **NgDP Guid** field with the GUID of the corresponding contact point for each mailbox mapping that has been configured. You can see the GUID in the **ID** field on the **Kontaktstruktur** (Contact structure) page in the **Administrativ Adgang** portal.

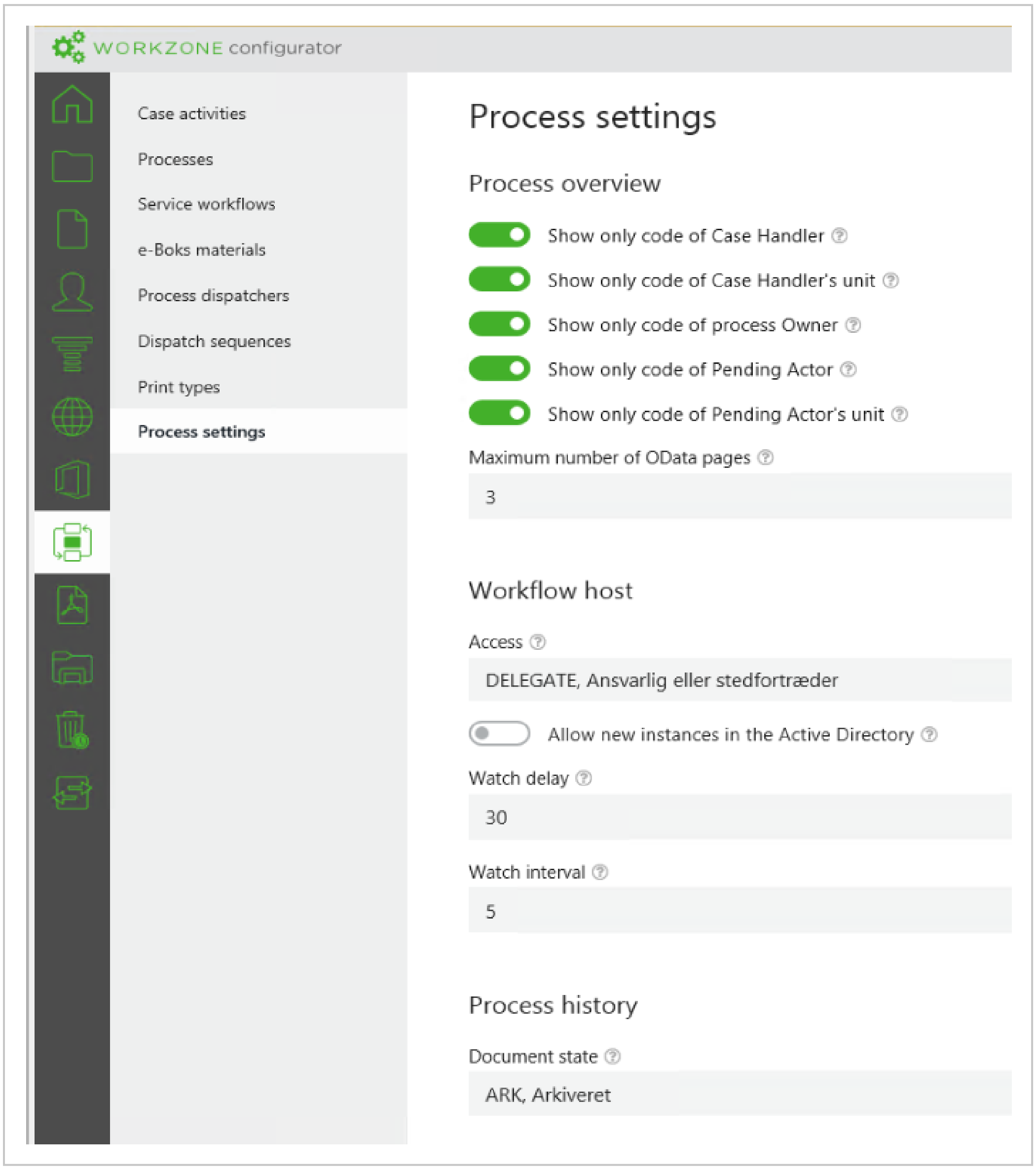


See also Handle e-Boks messages sent to subunits.

Other configurations

You can configure settings for WorkZone Process in WorkZone Configurator. The settings apply across process workflows and tasks.

- In WorkZone Configurator, click **Process** > **Process settings**.

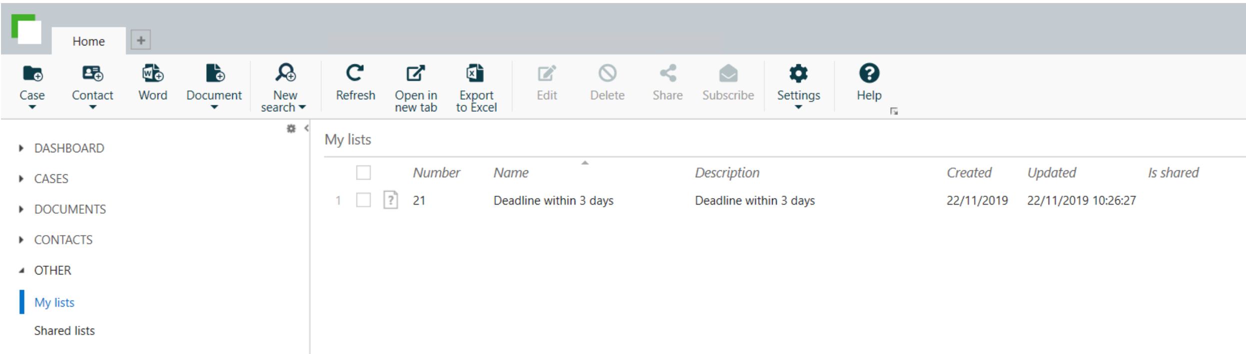


Create and share lists

If you have some knowledge of the WorkZone Process data model, you can create lists that are based on queries that you create using WorkZone QueryBuilder. When you save the queries, they appear under **My lists** in the **Processes Overview** and in the navigation pane of WorkZone Client.

You can share this type of lists with other users across your organization. Shared lists appear under **Shared lists** in the **Processes overview** and in the navigation pane of WorkZone Client.

In the WorkZone Client navigation pane, click **OTHER** > **My lists** or **Shared lists**.



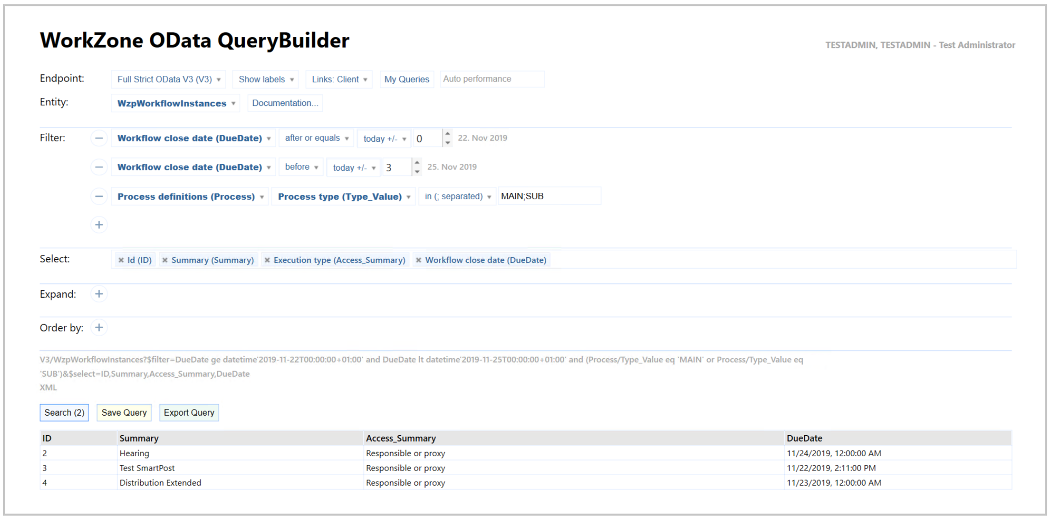
Create and save queries in WorkZone QueryBuilder

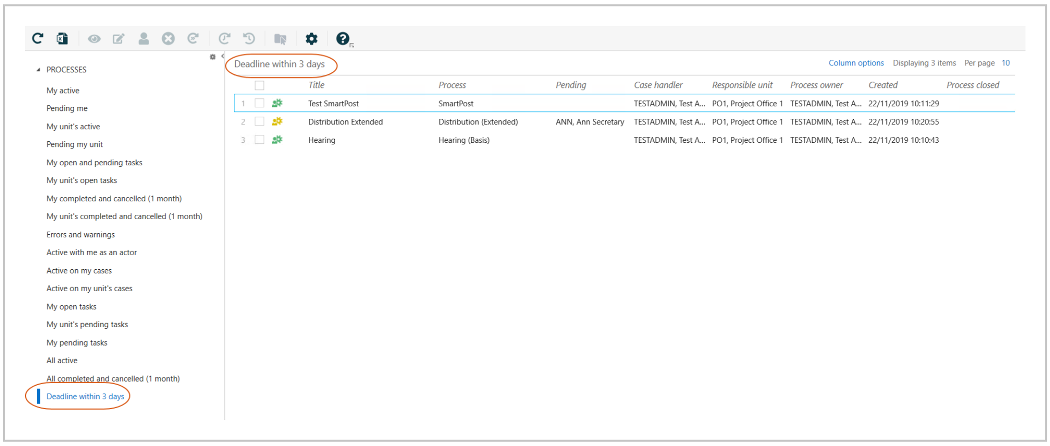
1. Open WorkZone QueryBuilder.
2. Select an entity from the list, for example **WzpWorkflowInstances**.
3. Apply a filter.
4. Click **Save Query** when your query is complete.
5. Enter a name and a description. The name of the query will be the name of the list that is shown on under **My lists** in the **Processes Overview** and under **My lists** in the navigation pane of WorkZone Client.

> **Tip:** To display the list in the **Processes Overview**, you must add it to the navigation pane first. In the **Processes Overview**, click to open the **Available lists** pane, and then double-click the list to add it to the navigation pane.

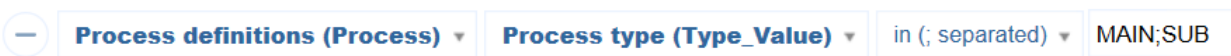
You can edit, share, and delete saved queries in WorkZone Client. The actions will be reflected in the **Processes Overview**. See Save and reuse search lists in the WorkZone Client User Guide. Note that when you edit a saved query in WorkZone Client, the query opens in WorkZone QueryBuilder for editing.

> **Example**: All processes that are due in 3 days





> **Important:** Always add the MAIN|SUB filter. This filter ensures that you will only display main and sub processes in the overview, and not service workflows and case activities, which are not supported in the overview.



Share a list

You can share lists that you have created with WorkZone QueryBuilder with other users, groups of users, or an entire organization. Sharing a list takes places in WorkZone Client. Once you have shared a list, it appears under **Shared list** in the **Processes Overview** and in the navigation pane of WorkZone Client.

See Share a saved search list in the WorkZone Client User Guide.

Configure workflow failover

Active workflows are persisted when they are idle, and a timer in the workflow host reactivates the workflow at next due date. The timer resides on the web server with the most recent workflow activity.

Workflow failover is controlled by two parameters in the **Process settings** in WorkZone Configurator.

1. Open WorkZone Configurator.
2. In WorkZone Configurator, click **Process** > **Process settings**.
3. Under **Workflow host**, specify the **WatchInterval** and **WatchDelay** parameters.

Parameter	Description
WatchInterval	Controls intervals between checks. If a web server is unavailable, workflows are not reactivated. In order to avoid this, all workflow hosts periodically check for workflows which are overdue. Enter a value between 5 minutes and 24 hours (1440 minutes). The default value is 5 minutes. This parameter applies to all service workflows.
WatchDelay	Controls the amount of time passed since the workflow should have been started. Enter value between 30 minutes and 24 hours (1440 minutes). The default value is 30 minutes.

The duration of the delay depends on the nature of the workflows. In some cases it is acceptable to have a delay of several hours, whereas in other cases only a shorter period is acceptable. The delay period should, however, be longer than the usual time required to reboot the server.

See Process settings in the WorkZone Configurator Administrator Guide

Configure default access to processes

To configure who can access processes on the current environment, you can change the default access setting in WorkZone Configurator.

1. Open WorkZone Configurator.
2. In WorkZone Configurator, click **Process** > **Process settings**.
3. Under **Workflow host**, select who should be able to access processes in the **Access** field. **DELEGATE** is selected by default.

Parameter	Description
ACTOR, Responsible	Only the current actor can access processes.
DELEGATE, Responsible or proxy	Both the current actor and the actor's delegate, if any, can access processes.
ALL, All	Access to processes is not limited to a specific actor.

See Process settings in the WorkZone Configurator Administrator Guide.

Configure notifications

You can configure when to send notifications. Users can receive notifications by email or as push notifications on mobile devices. WorkZone Process sends three types of notifications:

- Smarttasks as emails

  Emails that contain a task with response buttons.

- Email notifications

  Emails sent when a task is changed, for example, a task has been updated by another user.

- Push notifications

  Notifications sent to a mobile device when a task has changed.

You can configure which notifications to send in WorkZone Configurator.

1. Open WorkZone Configurator.
2. In WorkZone Configurator, click **Process** > **Process settings**.
3. Turn on the notifications that you want to apply to users in your organization.

By default, the following settings apply:

Notifications	Turned on/off
Send smarttasks as emails	On
Send push notifications	Off
Send email notifications	Off

Note: Before you decide which notifications to enable, consider the fact that the number of emails that are generated as notifications can easily get very high.

The settings apply to all users but individual users can change their own settings in WorkZone Client and WorkZone Mobile. See Your personal settings in the WorkZone Client User Guide and How can I receive notifications in the WorkZone MobileUser Guide.

Configure push notification certificates for WorkZone Mobile

If you want to send notifications from WorkZone Process to WorkZone Mobile, you need an Apple Push Services certificate. With the installation of WorkZone Process, two certificates are installed to the certificate store.

Usage	Certificate name
Unmanaged app	Apple Push Services: dk.kmd.WorkZone
Managed by Microsoft Intune	Apple Push Services: dk.kmd.workzone.intune

When you run WorkZone Process Configurator, the certificate used by the unmanaged app will be added to the config file by default.

If you run WorkZone Mobile as a managed app in Microsoft Intune, you need to change the default certificate to the Intune certificate. This is done in the config file.

Change the certificate in the config file

1. Open the **Scanjour.Process.Notification.AgentHost.exe.config** file located:

   ```
   C:\Program Files (x86)\KMD\WorkZone\Pro-
   cess\Bin\Scan-
   jour.Process.Notification.AgentHost.exe.config
   ```

2. Change the value of the **ApnsServerCertificateName** parameter to the name or the thumbprint of the Intune certificate.

If you upgrade WorkZone Process, the certificate in the config file will not be changed.

Configure availability of processes

You can hide a process by setting the end date of a process or restrict user access to a process by specifying access codes. This is done in WorkZone Configurator.

1. In WorkZone Configurator, click **Process** > **Processes**.
2. Point to the process you want to hide, and click **Edit parameters**.
3. Enter an end date or specify access codes.

Configure the process history document

When a process is complete, a history document is generated and saved on the current case. The history document summarizes the actions and results during the process. WorkZone Process includes a default history template document that is used for all process types. However, you can configure a specific history document for each type of process.

It is also possible to customize or create a new history document template but it requires developer assistance. See Custom reports in the WorkZone PDF Developer Guide e-Boks for information about how to create a new template and deploy it.

Note: Not all processes generate history documents. Phase processes, for example, do not generate history documents. For other process types, for example, the extended distribution process and the extended submission process, you can enable or disable generation of history documents. Except for the SmartPost process, no history document is generated if the process is canceled. The SmartPost process generates a history document but includes information about the process being canceled.

Configure a process-specific history document

You configure the history document in WorkZone Configurator as part of editing process parameters. See Edit process parameters in the WorkZone Configurator Administrator Guide.

1. In WorkZone Configurator, click **Process**.
2. Click **Processes**.
3. Point to the process for which you want to configure the history document. A menu bar appears.
4. Click **Edit process parameters**, and specify the history document parameters:

   - ReportID
   - RecordType
   - RecordState
   - TitleTemplate

The process history parameters and default values are described below.

Name	Default value	Description
ReportID	302c1bc6-7049-4759-b931-42ca6cc96f60	The ID (GUID) of the history document to generate.
RecordType	PROHIST	The document type of the history document that is generated by the process.

Name	Default value	Description
RecordState		The document state of the history document that is generated by the process. If you do not specify a document state, the document state specified in the **DocumentState** setting in the general process settings will be used. See Process settings in the WorkZone Configurator Administrator Guide.
TitleTemplate	{0}: {1} {2}	A template that is used to create the title of the history document. By default, the template has placeholders for the process type {0}, the process title {1}, and a date stamp {2}. **Example**: Hearing (Basis): Test case (25-06-2018) You can change this setting if you want to name the process history documents differently.

A history document generated by a hearing process:

KMD WORKZONE

Hearing

This is a hearing process

Process type: Hearing (Basis)

Case: 18-10/1

Started by: ANN

Case handler: Ann Secretary, ANN

Started: 25 Jan 2018 15:53

Process deadline: 1 Feb 2018 00:00

Completed: 25 Jan 2018 15:55

Documents included in this process

Number	Title
32	Results (D36)

Supplementary documents included in this process

Number	Title

History

Assignee: Ann Secretary, ANN

Started: 25 Jan 2018 15:53

Delegate:

Completed: 25 Jan 2018 15:54

Action: Answered

Task deadline: 1 Feb 2018 00:00

Type: Hearing

Comment:

Documents:

Assignee: Charlotte Record Manager, CHARLOTTE

Started: 25 Jan 2018 15:53

Delegate: Ann Secretary, ANN

Completed: 25 Jan 2018 15:54

Action: Answered

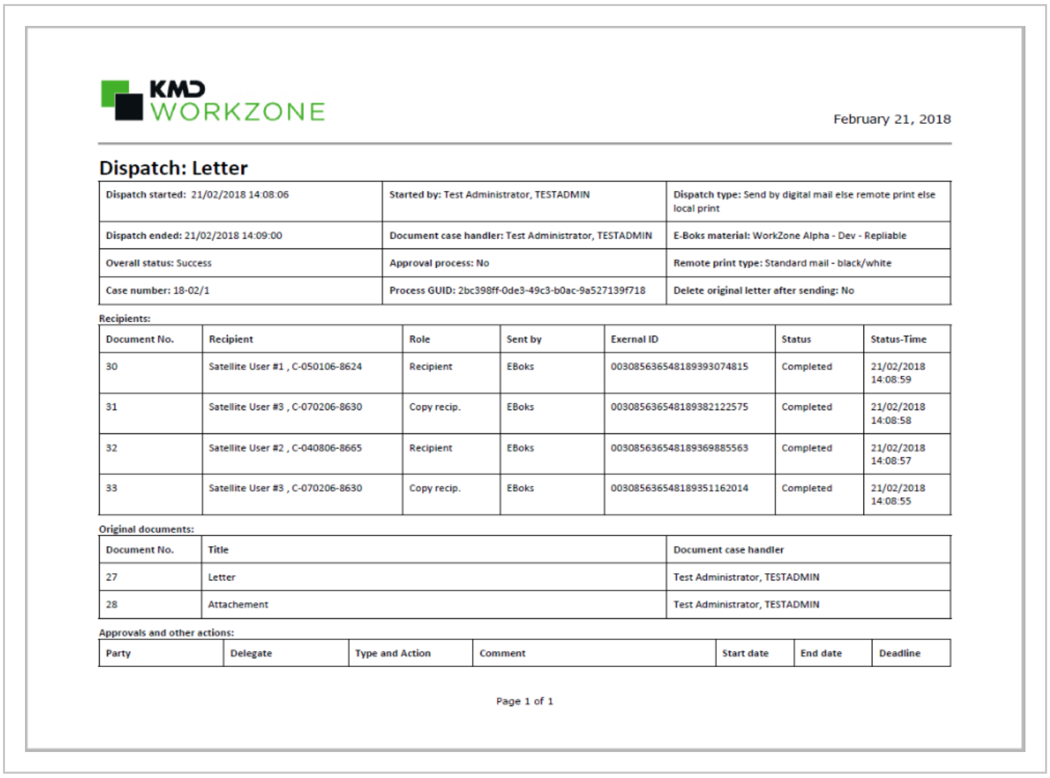
Task deadline: 1 Feb 2018 00:00

Type: Hearing

Comment:

Documents:

The SmartPost history document looks a bit different:



KMD WORKZONE

February 21, 2018

Dispatch: Letter

Dispatch started: 21/02/2018 14:08:06	Started by: Test Administrator, TESTADMIN	Dispatch type: Send by digital mail else remote print else local print
Dispatch ended: 21/02/2018 14:09:00	Document case handler: Test Administrator, TESTADMIN	E-Boks material: WorkZone Alpha - Dev - Repliable
Overall status: Success	Approval process: No	Remote print type: Standard mail - black/white
Case number: 18-02/1	Process GUID: 2bc398ff-0de3-49c3-b0ac-9a527139f718	Delete original letter after sending: No

Recipients:

Document No.	Recipient	Role	Sent by	Exernal ID	Status	Status-Time
30	Satellite User #1 , C-050106-8624	Recipient	EBoks	003085636548189393074815	Completed	21/02/2018 14:08:59
31	Satellite User #3 , C-070206-8630	Copy recip.	EBoks	003085636548189382122575	Completed	21/02/2018 14:08:58
32	Satellite User #2 , C-040806-8665	Recipient	EBoks	003085636548189369885563	Completed	21/02/2018 14:08:57
33	Satellite User #3 , C-070206-8630	Copy recip.	EBoks	003085636548189351162014	Completed	21/02/2018 14:08:55

Original documents:

Document No.	Title	Document case handler
27	Letter	Test Administrator, TESTADMIN
28	Attachement	Test Administrator, TESTADMIN

Approvals and other actions:

Party	Delegate	Type and Action	Comment	Start date	End date	Deadline

Page 1 of 1

Configure a process title

You can specify a title that will be suggested as default process title in the **Start process** dialog box when users start one of the following processes:

- Hearing (Basis)
- Submission (Basis)
- Submission (Extended)
- Distribution (Extended)

You define default titles for each process in WorkZone Configurator.

1. In WorkZone Configurator, click **Process** > **Processes**.
2. Point to the process you want to define a title for, and click **Edit parameters**.
3. In the **SuggestedTitle** field, enter the title you want to display as the default process title in the **Title** field in the **Send SmartPost** dialog box. The title can be maximum 256 characters long. You can leave the **SuggestedTitle** parameter empty, if you do not want to display a default title.

4. Turn on the **UseSuggestedTitle** parameter to use the title specified in the **SuggestedTitle** parameter. If the **UseSuggestedTitle** parameter is turned off, the case title will be suggested as the process title.

Configure the retry period for history document creation

HistoryDocRetryPeriod

You can configure the **HistoryDocRetryPeriod** parameter in the database. The **HistoryDocRetryPeriod** parameter defines the period of time that WorkZone retries creating a history document in case of failure.

You specify the time period using the format: d.hh:mm:ss

In ScanSQL, enter:

```
update wzp_settings set Value = '<d.hh:mm:ss>' where module
= 'CreateProcessHistoryDocument' AND key = 'His-
toryDocRetryPeriod'
```

if you do not configure this parameter, the default period of time is 1.00:00:00 (1 day).

Note: The retry period must be at least 5 minutes.

When the retry period expires, an error message is shown in the **Processes** overview.

Configure the use of new name instances

You can recycle names in WorkZone Process using Active Directory Replication.

To recycle names, complete the following steps:

1. Enable **AllowNewInstances** in the AD replicator.
2. In WorkZone Configurator, click **Process** > **Process settings**.
3. Turn on the **Allow new instances in Active Directory** parameter. The **Allow new instances in Active Directory** parameter is turned off by default.
4. For each Web server with WorkZone Process installed, open the IIS Manager and recycle the **WzpSvc** application pool.

Copy and rename a process

You can copy and rename a standard process if you want to use it in another context. For example, your organization may want to use the standard hearing process in a requisition working process. You can make a copy of the standard hearing process and rename the copied process as well as related labels that appear in the user interface so that the process matches the new context.

You can copy and rename all standard processes but note that if you copy and rename a main process, it will still use the standard sub process as opposed to a copied and renamed sub process. For example, if you copy and rename the ministerial process, the standard distribution sub process will still be used.

Copy a process

You copy processes in WorkZone Configurator.

1. Open WorkZone Configurator, and click **Process**.
2. Click **Processes**.
3. Point to the process you want to copy, and click **Copy** in the menu.
4. Enter a name and a description of the new process, and click **Copy**.
5. Point to the process you just copied, and click **Edit parameters** to configure the process.

Note: You cannot make a copy of a copied process.

Rename labels

You can rename labels in copied processes so that they match the name and context of the copied process, for example a requisition workflow. You can rename the labels that appear in:

- The **Start process** dialog box
- Smarttasks

- The **Processes** overview

1. Open WorkZone Configurator, and click **Process**.
2. Click **Processes**.
3. Point to the process you just copied and for which you want to rename labels, and click  **Edit labels** in the menu.
4. Change the standard labels as needed.

About case activities

Maintain best practices and update dynamically

Case activities can help you maintain best practices for handling ad-hoc tasks and tasks based on legal requirements.

With case activities you can map the possible events in a workflow and associate each event with a rule that calls for a certain action. You can also continue to update your case activities to reflect changes in work routines. In this way you preserve knowledge about work processes and you ensure that new best practices are implemented immediately in the handling of daily tasks and work routines.

Rule-based activities

With case activities you can create workflows based on activities that are connected by a set of rules. The rules define the relationship between the activities. For example, the rules can ensure that activities in a workflow are completed in a specific sequence or that specific activities exclude other activities.

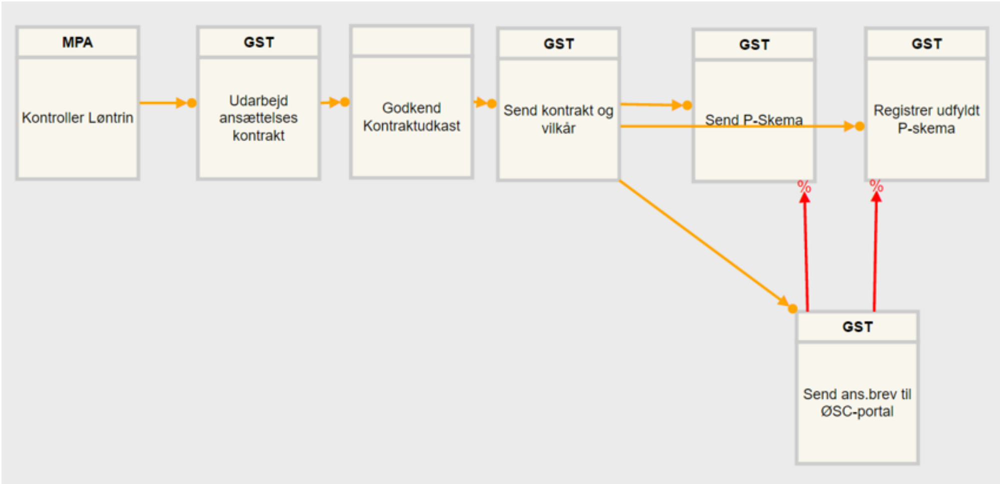
The case activity process

Case activities are modeled in a case activity process and once the process is deployed, the case activities can be executed in WorkZone Client.

In the following illustration, you see a case activity process with tasks, roles, and connections. The roles MPA and GST specify which employees are to execute the tasks, and the connections define the rules of the flow.

 - Condition: Indicates that a second activity can only be executed if the previous activity has been addressed.

 - Exclude: Excludes other activities upon execution

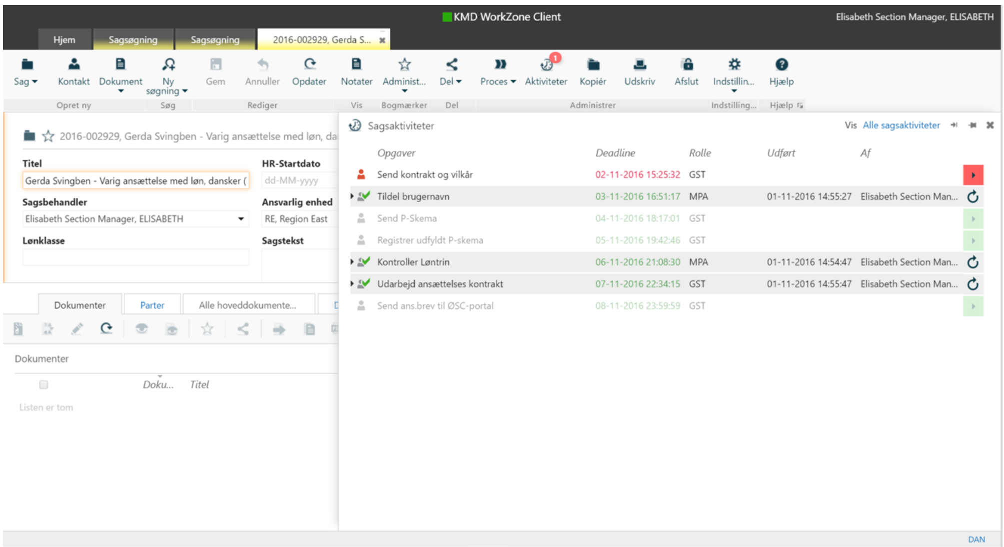


Work with case activities in WorkZone Client

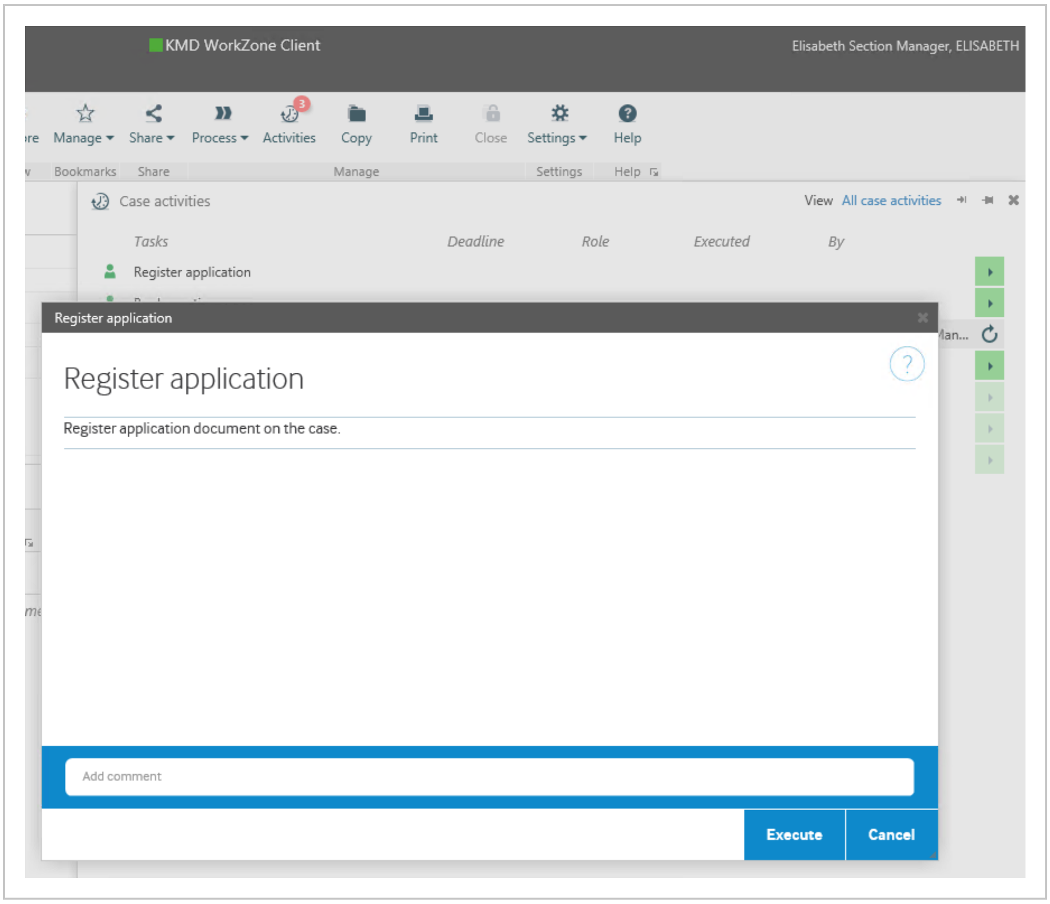
When the case activity process is deployed, users with the roles that are assigned to the activities in the process can see their activities in WorkZone Client.

To start case activities, click **Activities** on the **Activities** tab on the case detail tab in WorkZone Clientand select an activity list. You can start multiple activities on a case .

Below you can see a case activity in WorkZone Client.



When you double-click an activity, a form opens from where you can execute the activity.



For more information about executing case activities, see [Work with case activities](#) in the WorkZone Client User Guide.

About case activities

Maintain best practices and update dynamically

Case activities can help you maintain best practices for handling ad-hoc tasks and tasks based on legal requirements.

With case activities you can map the possible events in a workflow and associate each event with a rule that calls for a certain action. You can also continue to update your case activities to reflect changes in work routines. In this way you preserve knowledge about work processes and you ensure that new best practices are implemented immediately in the handling of daily tasks and work routines.

Rule-based activities

With case activities you can create workflows based on activities that are connected by a set of rules. The rules define the relationship between the activities. For example, the rules can ensure that activities in a workflow are completed in a specific sequence or that specific activities exclude other activities.

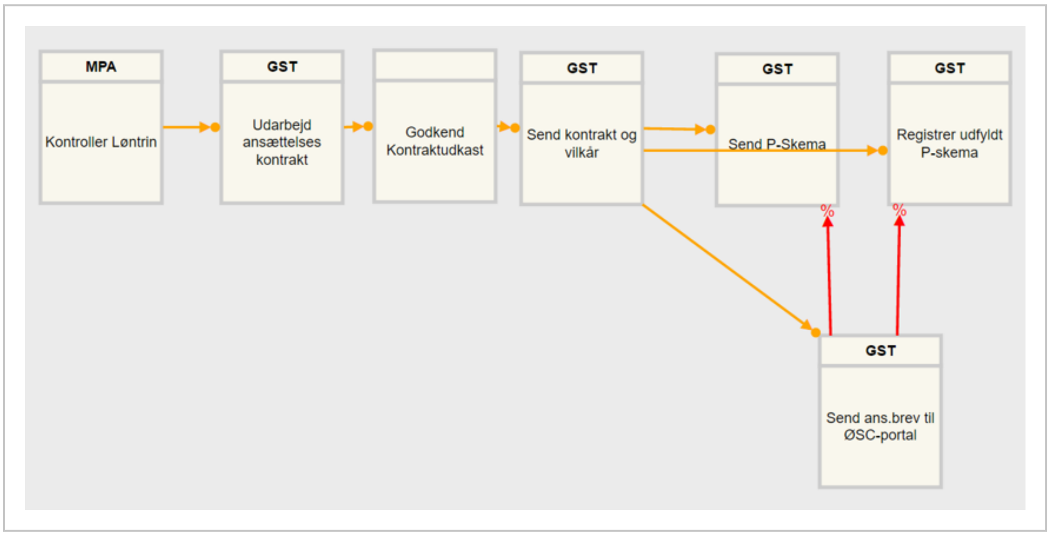
The case activity process

Case activities are modeled in a case activity process and once the process is deployed, the case activities can be executed in WorkZone Client.

In the following illustration, you see a case activity process with tasks, roles, and connections. The roles MPA and GST specify which employees are to execute the tasks, and the connections define the rules of the flow.

 - Condition: Indicates that a second activity can only be executed if the previous activity has been addressed.

 - Exclude: Excludes other activities upon execution

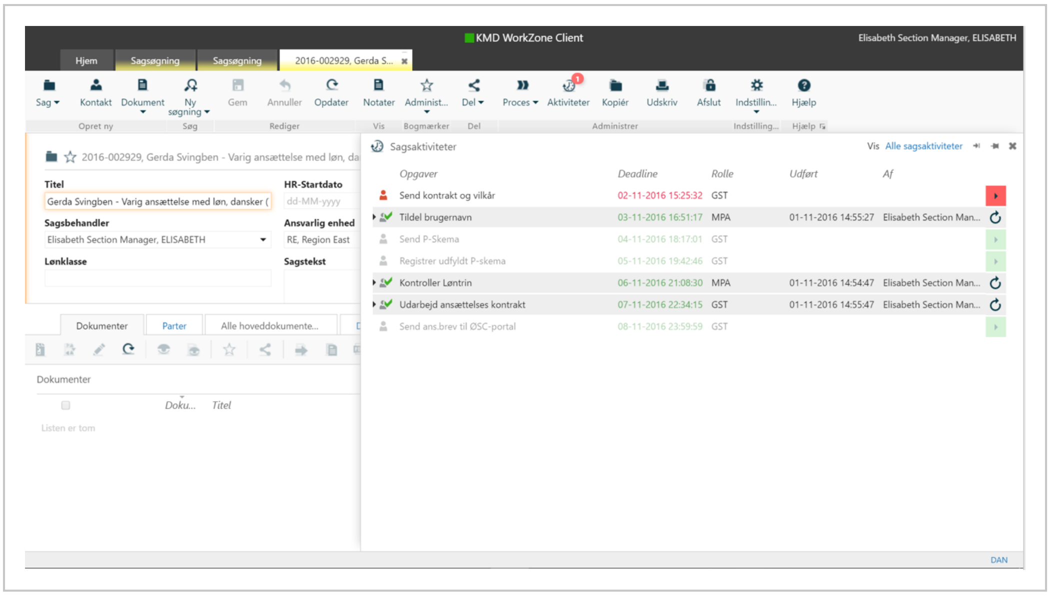


Work with case activities in WorkZone Client

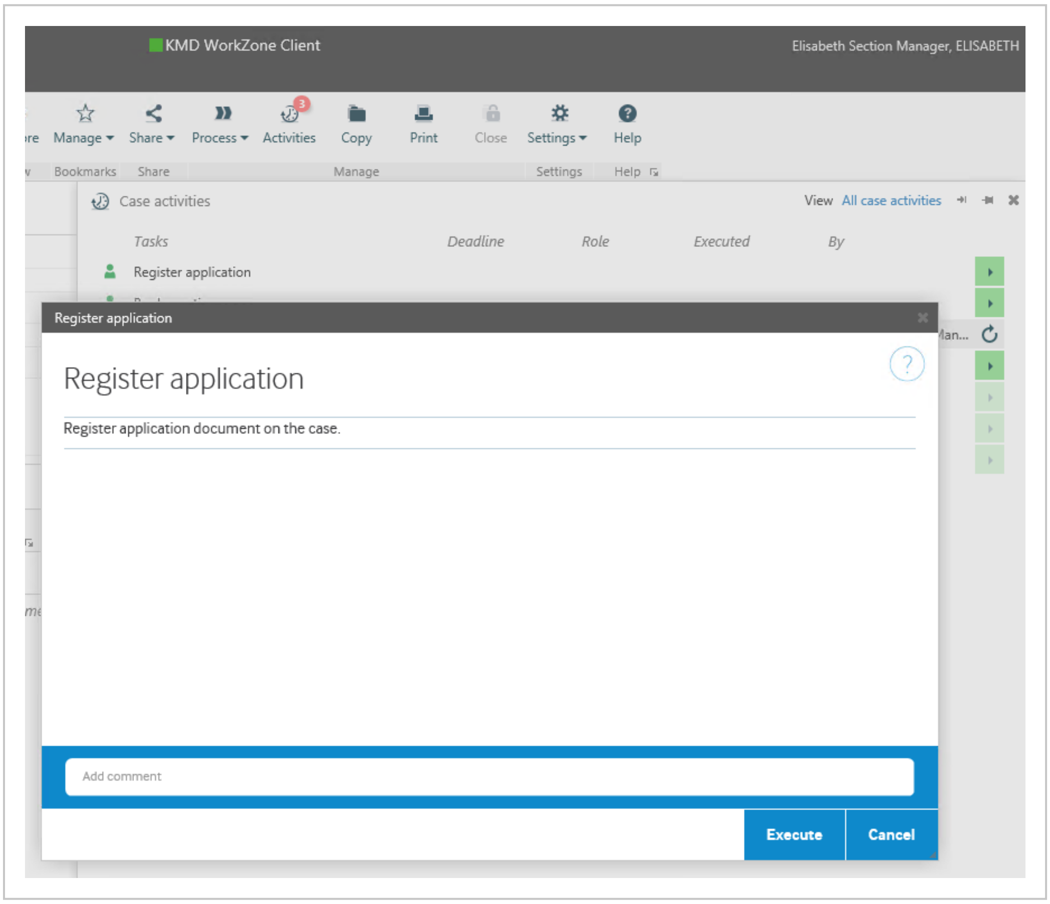
When the case activity process is deployed, users with the roles that are assigned to the activities in the process can see their activities in WorkZone Client.

To start case activities, click **Activities** on the **Activities** tab on the case detail tab in WorkZone Clientand select an activity list. You can start multiple activities on a case .

Below you can see a case activity in WorkZone Client.



When you double-click an activity, a form opens from where you can execute the activity.



For more information about executing case activities, see [Work with case activities](#) in the WorkZone Client User Guide.

Getting started with case activity processes

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.

1. Open DCR Portal in Google Chrome.
2. Create a profile.

You can work with your own personal processes or with processes that have been shared by others users.

Create a DCR process

The first step in modeling case activities is to create a DCR process and add the activities that you want for the case activity workflow.

1. Log in to the DCR Portal from DCRGraphs.net.
2. At the top of the dashboard, click **Create Process**.
3. Enter a name for the new process, and then click **Save**.

   - Or -

   Click the **Templates**, and then select **WorkZone Case Activities Template**. See Create a DCR process using the WorkZone template.
4. Add activities and create connections between the activities to model your case activity process.

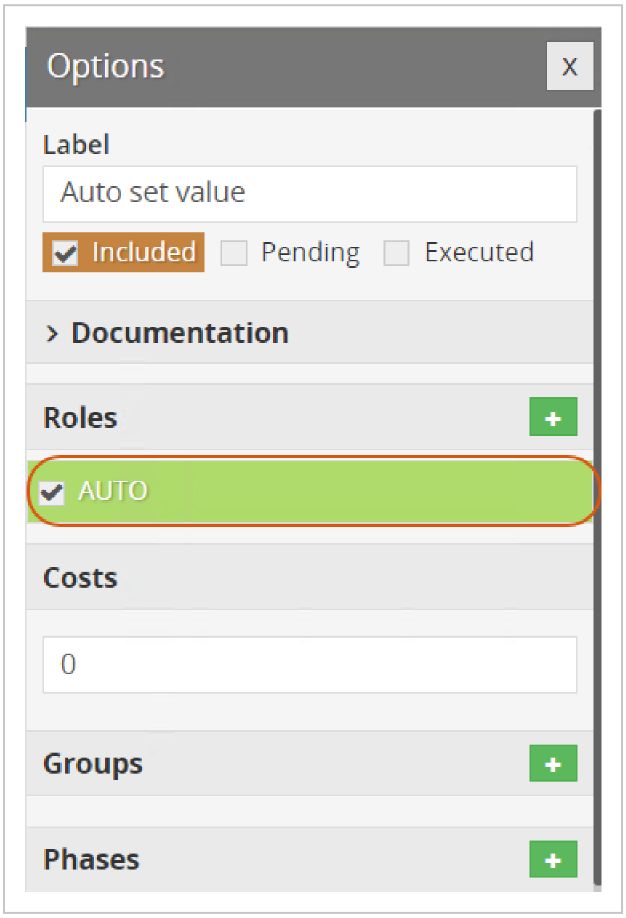
   For information about creating DCR processes, see the DCR documentation.

To export your DCR process and make it available in WorkZone, see Export and deploy case activity processes.

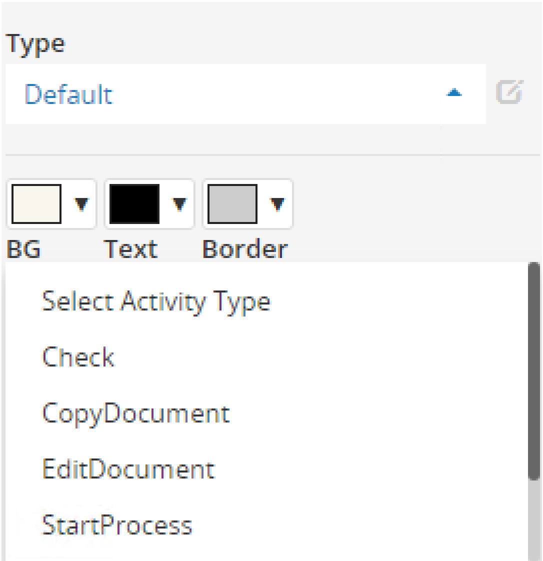
Create a DCR process using the WorkZone template

WorkZone provides a template that you can use to get started with a case activity process, which provides WorkZone specific activity types.

1. Log in to the DCR Design Portal from DCRGraphs.net.
2. At the top of the dashboard, click **Create process**.
3. In the **New Process** dialog box, click **Templates**.
4. Select the **WorkZone Case Activity Template**, and then click **Save**. The template is loaded, and you can start adding activities and connections.
5. Click  to insert an activity.
6. In the **Options** pane, add a label and a description, which will be displayed in the activity list in WorkZone Client.
7. If you want the activity to be executed automatically, select the role named **AUTO**.

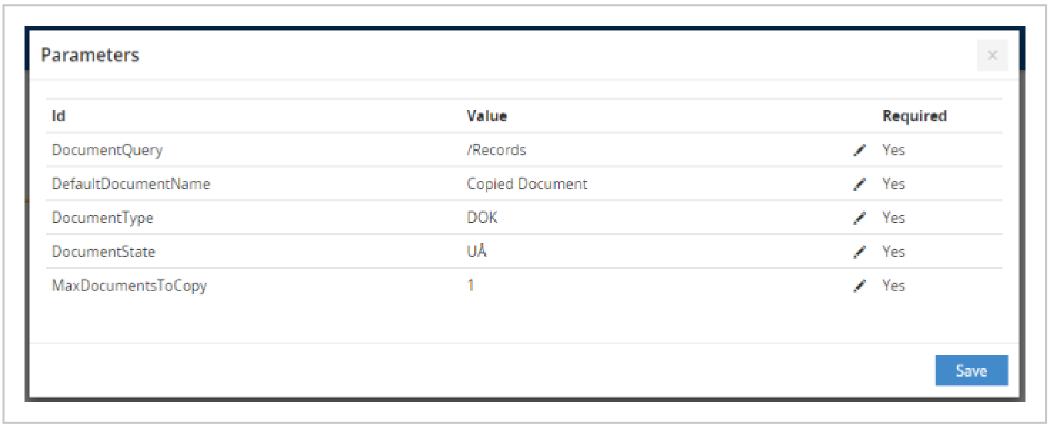


8. Click **Advanced** and scroll to the bottom of the **Options** pane, and then select an activity type in the **Activity Type** field.



See Activity types for a description of the activity types.

9. Select a WorkZone activity, for example **CopyDocument**, and a list of parameters for the selected type is shown.



10. Fill in the parameters. See Activity types for an overview of the parameters.
11. When you have completed the process, click **File** > **Save As** to save your DCR process.

To make your DCR process available in WorkZone, you need to export it first, see Export and deploy case activity processes.

Activity types

With the WorkZone template, you get a number of WorkZone-specific activity types.

Check

Check is the basic activity type, which you can use for creating items on a check list. You can, for example, use it for providing information that must be read before moving on to the next activity. You can add instructions and links to more information in this activity. This is the default activity type.

Check parameters

No parameters

CompleteGraph

CompleteGraph completes the process. You can use this activity to allow users to complete a case activity list even if some activities have not been executed, for example, if the activities were not needed in a work process.

CompleteGraph parameters

No parameters

CopyDocuments

CopyDocuments copies documents that are retrieved by a query to the current case. The documents are copied without the source meta data. The access code is verified on the basis of the case handler's or the case owner's access rights. For example, you can use this activity type to copy standard documents, such as templates to a case.

> **Note:** The **CopyDocuments** activity type can copy a maximum of 50 documents to a case at the same time.

CopyDocuments parameters

Parameter	Description	Required
DocumentSource	OData query that identifies the documents to copy. The example shows how to copy templates with the document type SKAB to the current case. **Example**: `/Records?$filter=RecordType_Value eq 'SKAB'&$select=ID,UserKey,Summary`	Yes
DefaultDocumentName	If you copy only one document, you can specify a default name that will be applied to the copied document. If you copy more than one document, the original name will be used.	Yes
DocumentType	The document type that will be applied to the copied documents.	Yes
DocumentState	The document state that will be applied to the copied documents.	Yes
MaxDocumentsToCopy	Defines the maximum number of documents to copy. The default value is 1. If the maximum number of documents to copy is exceeded, no documents will be copied.	Yes

EditDocuments

EditDocuments provides a list of documents for editing. The documents on the list are retrieved by a query, for example, documents on a specific case, documents with me as the case handler, and so on.

EditDocuments parameters

Parameter	Description	Required
DocumentQuery	OData query that searches for the documents to edit. By default all documents are listed. The example shows how to retrieve documents on the current case. **Example**: `/Records?$filter=FileKey_Value eq '{Case.ID}'` Where `Case.ID` refers to the current case.	Yes

StartProcess

StartProcess starts a process or another case activity list. When a user executes the activity, the **Start process** dialog box opens with the specified process.

Automatic execution

You can execute the **StartProcess** activity type automatically but it will only work if the process you start does not have any parameters. If you specify a process with parameters, an error message will be written to the activity history when the activity tries to start the process automatically. Note that all standard processes have parameters. Automatic execution works when starting a case activity list or a customized process without parameters. See Execute activities automatically for information about using the AUTO and L-AUTO roles.

StartProcess parameters

Parameter	Description	Required
ProcessGUID	The GUID of the process you want the activity to start. **Note:** You can look up the GUIDs in WorkZone Configurator, see FAQs about case activities.	Yes

Parameter	Description	Required
ProcessOwner	Specify the process owner using the NameCode of the process owner or using the case handler on the current case using the notation `Case.Officer_Value`. If you add the **AUTO** or **L-AUTO** roles, it is required to specify this parameter. Automatic start of the process will fail if the **ProcessOwner** parameter is not specified.	No

SendSmartPost

SendSmartPost starts a SmartPost process. In this release, you can send a letter to recipients. By default the **SendSmartPost** activity is executed automatically.

SendProcess parameters

Parameter	Description	Required
Letter	OData query that specifies which document to send as the letter in the SmartPost message. **Example**: `/Records?$filter=FileKey_Value eq '{Case.ID}' and (Title eq 'Standard letter')` The query retrieves a document with the title *Standard letter* from the current case.	Yes
Attachments	OData query that specifies which attachments to include in the message. **Example**: /Records?$filter=FileKey_Value eq '{Case.ID}' and (Title eq 'Attachment 1' or title eq 'Attachment 2')	No

<table>
<tr><th>Parameter</th><th>Description</th><th>Required</th></tr>
<tr><td></td><td>The query retrieves two documents with the titles Attachment 1 and Attachment 2 from the current case.</td><td></td></tr>
<tr><td>Recipients</td><td>Specify the recipients of the message.

You can use an OData query or you can enter the party roles separated by comma. If a party with a specific role is not found on the case or the role is invalid, you can specify which role to use instead after a slash /. You specify as many alternative roles as you need separated by slashes.

OData query

Example: <code>/Addresses?$filter=Name/Files/any(a: a/FileKey_Value eq '{Case.ID}' and a/CustomLabel_Value eq 'Reply-To')</code>

The query retrieves addresses of parties with the role Reply to on the current case.

Simple notation

Example: <code>Reply-To, Høringspart/Sagspart</code>

The query retrieves addresses of parties with the roles Reply to and Hearing party.

If no parties with the role Hearing part (Høringspart) are found parties with the role Sagspart will be retrieved instead.

You must specify the codes for the roles and not the localized labels. You can see the codes in WorkZone Configurator. Go to Case > Parties and references.</td><td>Yes</td></tr>
<tr><td>CopyRecipients</td><td>Specify the copy recipients of the message.</td><td>No</td></tr>
</table>

Parameter	Description	Required
	You can use an OData query or you can enter the party roles separated by comma and alternative roles separated by slashes in the same way as for Recipients. If the total number of recipients and copy recipients exceeds the maximum allowed number of 50 recipients, the message will not be sent.	
ProcessGuid	Specify the GUID of the SmartPost process you want the activity to start. Use this parameter if your organization has several SmartPost processes and you want to use to a specific SmartPost process. If you do not specify a GUID, the GUID of the default SmartPost process is used. **Note:** You can look up the GUIDs in WorkZone Configurator, see FAQs about case activities.	No
ProcessOwner	Specify the process owner of the SmartPost process. Possible values are: • NameCode–Enter the NameCode of the employee who will be the process owner using upper case letters. • `{Case.Officer_Value}`–The case handler on the case where the case activity is started becomes the process owner. • `{DocumentCaseHandler}`–The case handler on letter document that will be sent by SmartPost becomes the process owner. If the values are invalid, an error message will be written to the history.	Yes

UpdateEntities

UpdateEntities updates values of specific text fields on a case, for example if you want the case title and the case state of the current case to change after an action has been completed.

The activity type can be used to update both standard and custom fields.

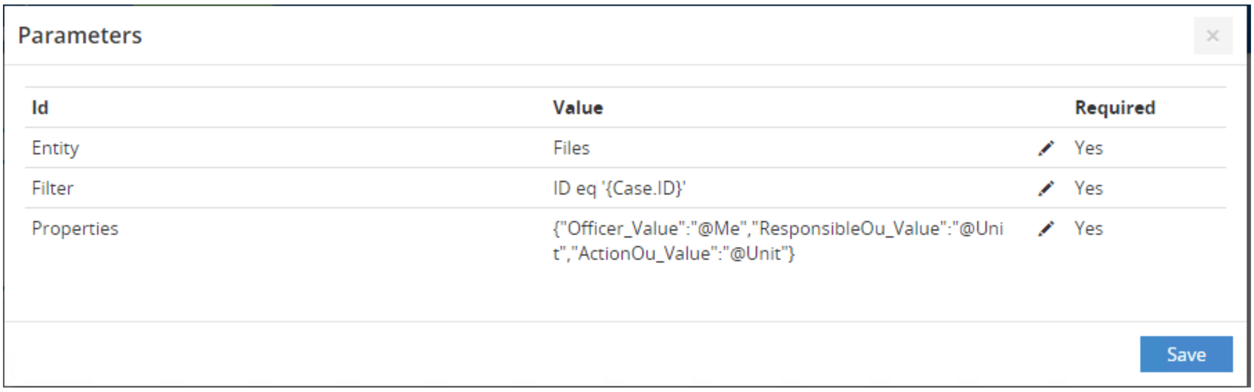
The following types of fields cannot be updated:

- Computed and read-only properties. See the WorkZone QueryBuilder documentation for information about which properties of the **Files** entity are computed.
- Other entities, for example **Case text** and **Information**, if they are empty.
- Custom droplists.

Current user and organizational unit

You can update fields on a case using @me and @unit to insert the current user as case handler on a case and the current user's organizational unit as the responsible unit.

To add the current user as case handler on the case and the current user's organizational unit as the responsible unit, define the parameters as follows:



Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"Officer_Value":"@Me","ResponsibleOu_Value":"@Unit","ActionOu_Value":"@Unit"}	Yes

Save

> **Note:** When using @Me or @Unit, do not set the **UpdateEntities** activity to execute automatically. It is a system user who executes activities with the **AUTO** role assigned, and therefore @Me and @Unit will fail. See Execute activities automatically.

UpdateEntities parameters

<table>
<tr><th>Parameter</th><th>Description</th><th>Required</th></tr>
<tr><td>Entity</td><td>Specify which entity you want to get values from, for example Files (Cases).</td><td>Yes</td></tr>
<tr><td>Filter</td><td>Enter the file key of the case whose values you want to update. If you always want to update the current case, meaning the case on which the case activity is started, you can enter:
<code>ID eq '{Case.ID}'</code>
Tip: You can use WorkZone QueryBuilder to build your query and copy the filter part to this parameter. See How do you copy a query from WorkZone QueryBuilder.</td><td>Yes</td></tr>
<tr><td>Property</td><td>Specify the properties and values you want to update in JSON format. For example, if you want to update the case state and the case title, enter:
<code>{"State_Value":"UB","Title":"Updated"}</code>
Which will update the State field with the state UB, Being processed and the Title to Updated.
If, for example, you want to update the Title field with the date and time that the current case was updated and the current state, enter:
<code>{"Title":"Title: {Case.Title}, updated: {Case.UpdateTime}, State: {Case.State_Value}"}</code>
Which will update the case title to, for example: Title: Case title, updated: 25-03-2020 11.50.00, State: UB, Being processed.
Tip: You can use WorkZone QueryBuilder to build your query, convert it to JSON format, and copy it to this parameter. See How do you copy a query from WorkZone QueryBuilder.</td><td>Yes</td></tr>
</table>

ValidateEntities

ValidateEntities allows you to validate values on a case based on a condition that you define, and if the condition is met, the subsequent activities will be included or excluded. The **ValidateEntities** activity type works in connection with guards that you define on the Include and Exclude relation types.

Guards

On the Include and Exclude relation types, you need to define guards that validate against the condition you have defined in an activity that holds the activity type **ValidateEntities**.

On the Include relation type, enter:

```
<Activity ID>=1
```

On the Exclude relation type, enter:

```
<Activity ID>!=1
```

This also works vice versa, depending on what you want the process to do.

`<Activity ID>` is the ID of the activity that holds the **ValidateEntities** activity type.

`=1` means that the condition you have defined in the activity is met (it is TRUE).

`!=1` means that the condition you have defined in the activity is not met (it is FALSE).

ValidateEntities parameters

Parameter	Description	Required
Entity	Specify which entity you want to get values from, for example **Files** (Cases).	Yes
Filter	Enter the file key of the case whose values you want to update. If you always want to update the current case, that is the case on which the case activity is started, you can enter: `ID eq '{Case.ID}'` **Tip:** You can use WorkZone QueryBuilder to build your	Yes

Parameter	Description	Required
	query and copy the filter part to this parameter. See How do you copy a query from WorkZone QueryBuilder.	

Property	Specify the properties and values you want to validate in JSON format. For example, if you want to validate the value of the case state and the responsible unit, enter:
	`{"State_Value":"FB","ResponsibleOu_Value":"AS"}`
	In connection with guards, it will validate if the state is *FB* and if the responsible unit is *AS* and then include or exclude the following activities depending on the outcome.
	Another example may be to validate the current case state in the title:
	`{"Title":"Case with state: {Case.State_Value}"}`
	In connection with guards, it will validate if the title is *Case with state: <currentState>* and then include or exclude the following activities depending on the outcome.
	Tip: You can use WorkZone QueryBuilder to build your query, convert it to JSON format, and copy it to this parameter. See How do you copy a query from WorkZone QueryBuilder.
		Yes

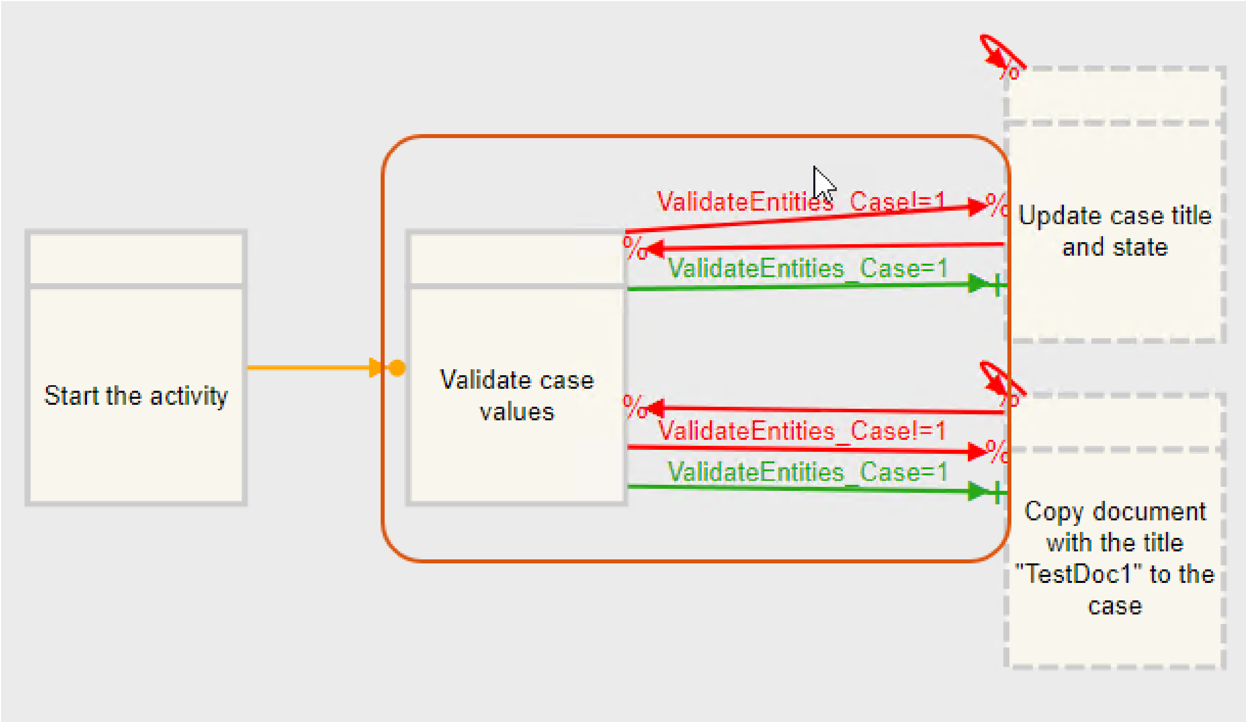
ValidationInterval	Specify at which interval you want the **ValidateEntity** activity to be executed automatically. Use this parameter if you await specific information to be available on a case before the next activity can be executed. For example, a receipt for payment must be saved on the case before the case handling can continue. Enter the interval in number of minutes. The minimum interval is 30 minutes.	No

Parameter	Description	Required
	The automatic execution will end when the **ValidateEntity** activity is no longer active, for example, if is not executable or not included in the process, or when the entire process is completed. If you have several **ValidateEntity** activities in a process, the activity with the lowest interval will determine when the entire process will be updated. The process will also be updated if only one of the **ValidateEntity** activities has this parameter filled in. If you do not specify this parameter, the user will need to click the **Update** button in WorkZone Client to update the activity list manually.	

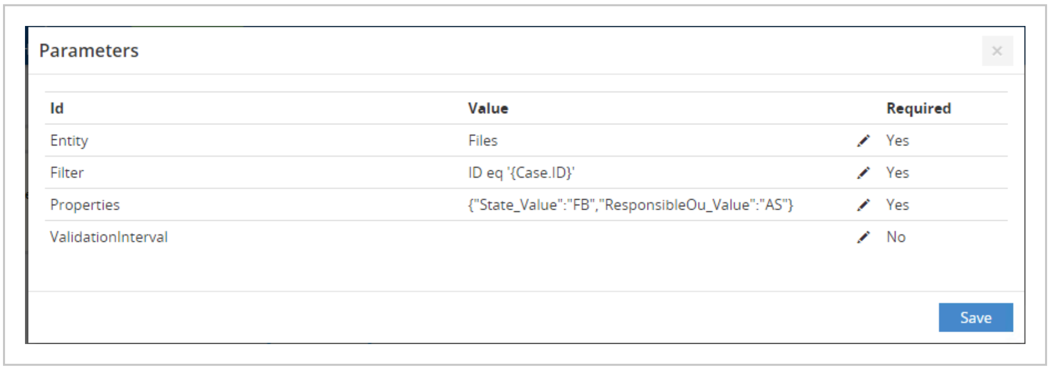
Example: ValidateEntities

> **Example**: The example below illustrates the use of the **ValidateEntities** activity type together with guards. The title and the state of the current case will be changed and a document will be copied to the case if the case has the state *FB* and the responsible unit is *AS*.

The DCR process looks like this:



The **Validate case values** activity is a **ValidateEntities** activity type that validates if the current case has the state *FB* and the responsible unit is *AS*. The parameters are defined as follows:



Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"State_Value":"FB","ResponsibleOu_Value":"AS"}	Yes
ValidationInterval		No

Save

The Include and Exclude relation types have guards that check if the condition above is met.

- Include relation type:

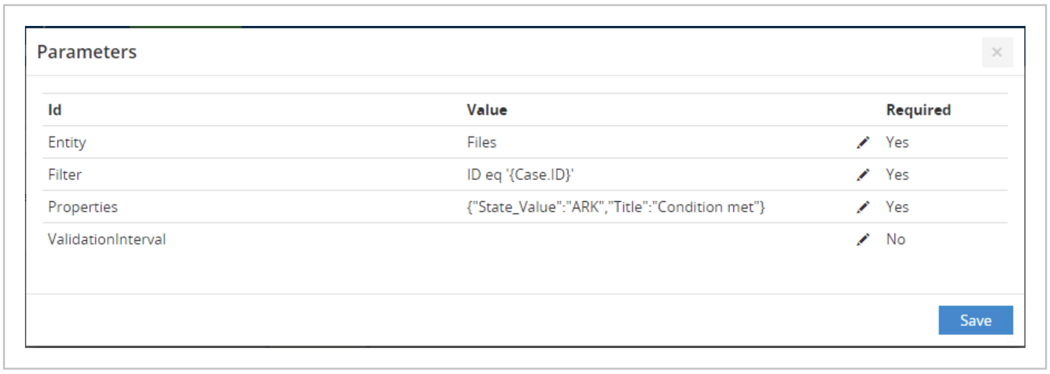
  `ValidateEntities_Case=1`

- Exclude relation type:

  `ValidateEntities_Case!=1`

If the condition is met, the **Validate case values** activity will hold the value `1`, and the **Update case title and state** activity and the **Copy document with title "TestDoc1"** activity will be included. If the condition is not met, it will result in `!=1` and nothing will happen.

The **Update case title and state** activity is an **UpdateEntities** activity type that changes the case title to *Condition met* and the state changed to *ARK*. The parameters are defined as follows:

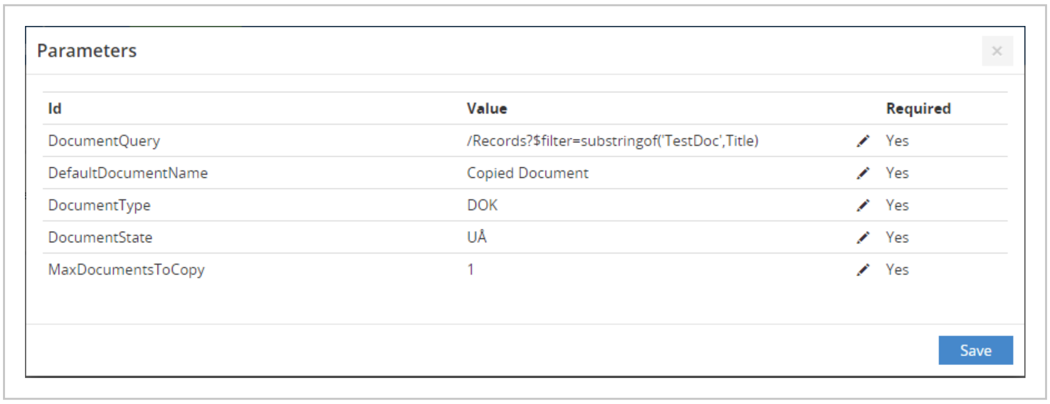


Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"State_Value":"ARK","Title":"Condition met"}	Yes
ValidationInterval		No

Save

The **Copy document with title "TestDoc1"** activity is a **CopyDocument** activity type that copies a document named *TestDoc1* to the case and name the document *Copied document*. The parameters are defined as follows:



Parameters

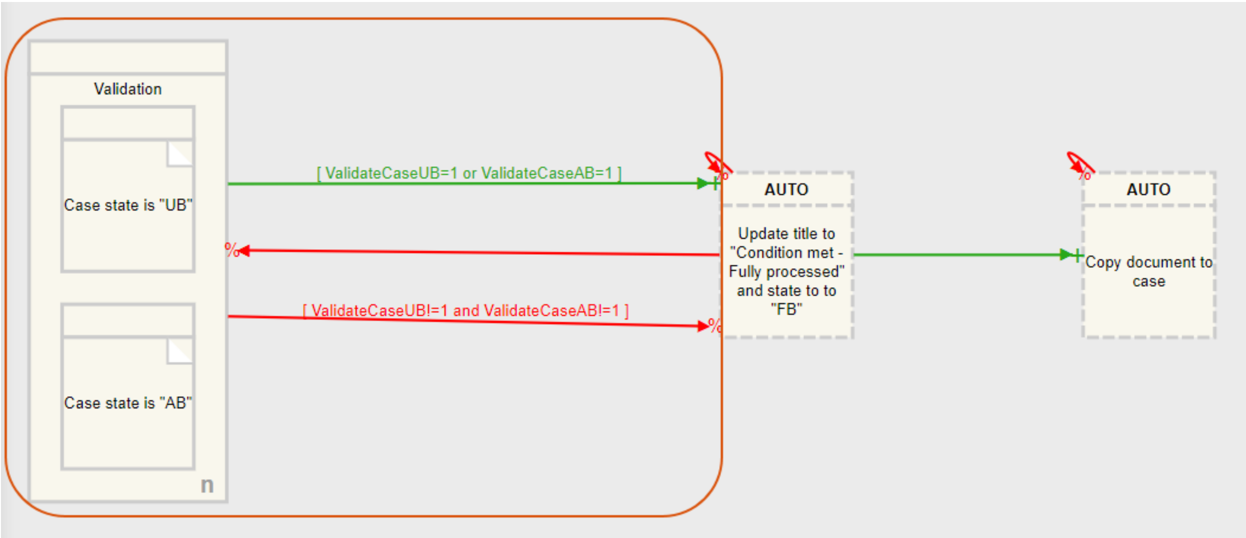
Id	Value	Required
DocumentQuery	/Records?$filter=substringof('TestDoc',Title)	Yes
DefaultDocumentName	Copied Document	Yes
DocumentType	DOK	Yes
DocumentState	UÅ	Yes
MaxDocumentsToCopy	1	Yes

Save

Example: ValidateEntities – Combine rules in a guard

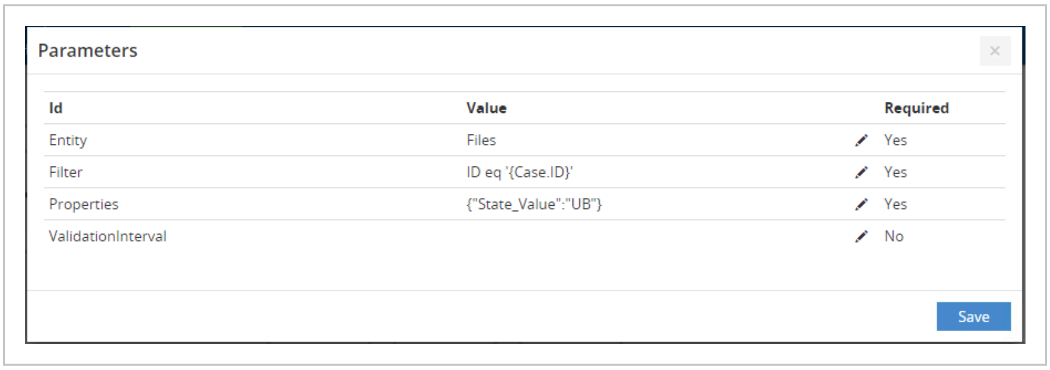
Example: The example below illustrates the use of the **ValidateEntities** activity type together with complex rules that are combined in a guard. The title will be changed to "Condition met - Fully processed" and the state of the current case will be changed to *FB, Fully processed* automatically if the case has the state *UB* or the case has the state *AB*.

The DCR process looks like this:



The **Validation** activity is a nested activity that holds two activities of the type **ValidateEntities**. Each nested activity contains a condition.

The first activity **Case state is "UB"** validates if the current case has the state *UB*. The parameters are defined as follows:

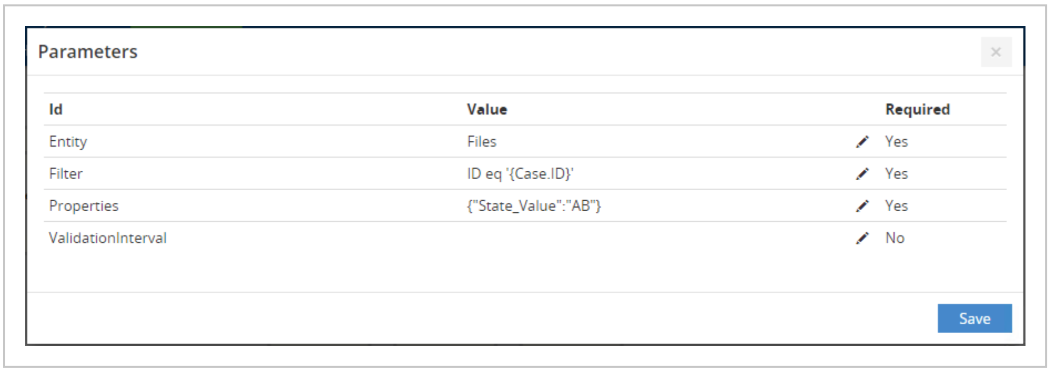


Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"State_Value":"UB"}	Yes
ValidationInterval		No

Save

The second activity **Case state is "AB"** validates if the current case has the state *AB*. The parameters are defined as follows:



Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"State_Value":"AB"}	Yes
ValidationInterval		No

Save

The Include and Exclude relation types have guards that validate if the above condition is met.

- Include relation type:

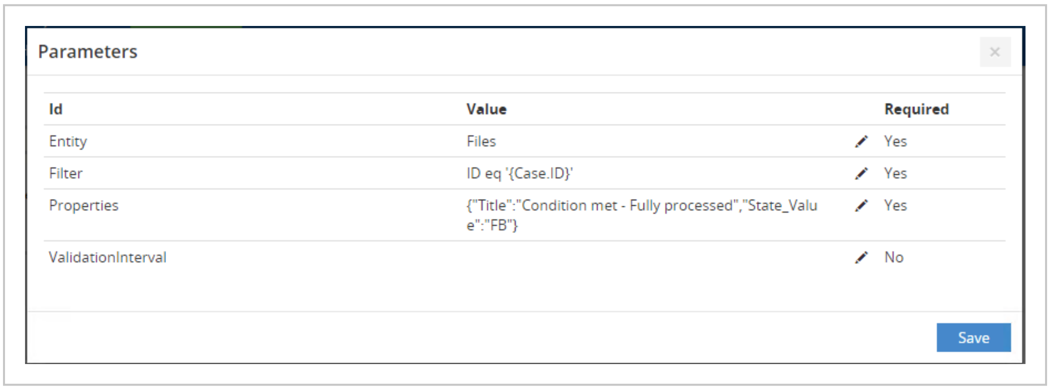
  `ValidateCaseUB=1 or ValidateCaseAB=1`

- Exclude relation type:

  `ValidateCaseUB!=1 and ValidateCaseAB!=1`

The condition is met if either the **ValidateCaseUB** activity or the **ValidateCaseAB** activity hold the value `1`, the **Update state and title** activity and the **Copy document to case** activity will be included. If none of the conditions are met, it will result in `!=1`, and nothing will happen.

The **Update state and title** activity is an **UpdateEntities** activity type that changes the case title to *Condition met - Fully processed* and the state of the current case to *FB, Fully processed*. The parameters are defined as follows:



Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Properties	{"Title":"Condition met - Fully processed","State_Value":"FB"}	Yes
ValidationInterval		No

Save

The **Copy document to case** activity is a **CopyDocument** activity type that copies a specific document to the case and names the document *Standard letter*. The parameters are defined as follows:

Parameters

Id	Value	Required
DocumentQuery	Records?$filter=RecordKey eq '47'&$select=ID,UserKey,Summary	No
DefaultDocumentName	Standard letter	No
DocumentType	DOK	No
DocumentState	UÅ	No
MaxDocumentsToCopy	1	No

Save

Note: Do not use @Me or @Unit in the **ValidateEntities** activity. The **ValidateEntities** activity is always executed automatically by a system user, and therefore @Me and @Unit will fail. See Execute activities automatically.

GetValue

GetValue allows you to fetch a value from an entity, for example a case. You can then use this value in guards to make conditions based on WorkZone data. If the condition is met, the subsequent activities will be included or excluded.

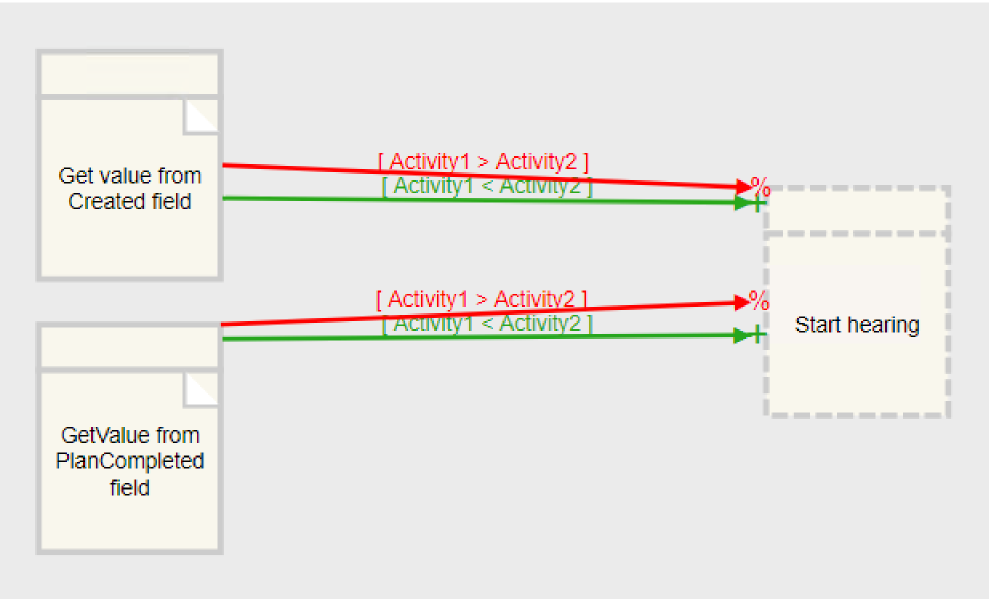
GetValue parameters

Parameter	Description	Required
Entity	Specify which entity you want to fetch a value from, for example **Files** (Cases).	Yes
Filter	Enter the key of the entity you want to get a value from. If you always want to fetch a value on the current case, which is the case on which the case activity is started, you can enter: `ID eq '{Case.ID}'` Tip: You can use WorkZone QueryBuilder to build your query and copy the filter part to this parameter. See How do you copy a query from WorkZone QueryBuilder.	Yes
Property	Specify the property field that you want to fetch a value from. For example, if you want to get the case state, enter: `State_Value` Tip: You can use WorkZone QueryBuilder to find the name of the available properties.	Yes

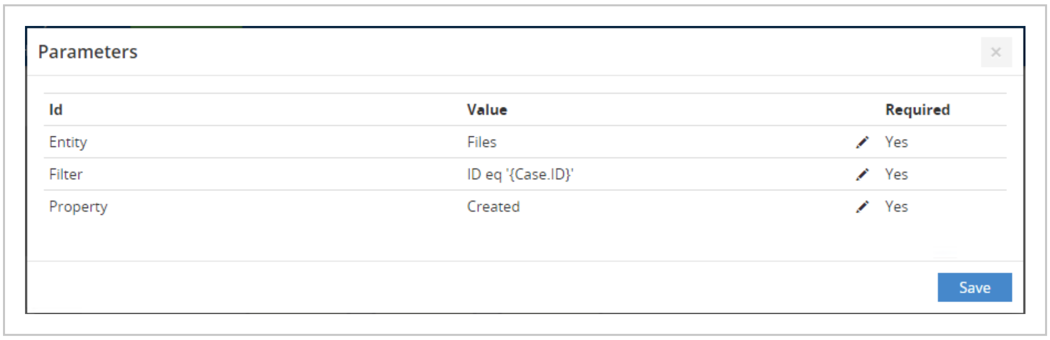
Example

> **Example**: The example below illustrates the use of the **GetValue** activity type together with guards. A date is fetched from the **Created** property on the current case and compared with a date fetched from the **PlannedCompleted** property. The dates are compared using the guards. If the condition in the guard is met, a hearing process is started.

The DCR process looks like this:



Activity1 (GetValue from Created field) fetches the date from the **Created** field on the current case. The parameters are defined as follows:

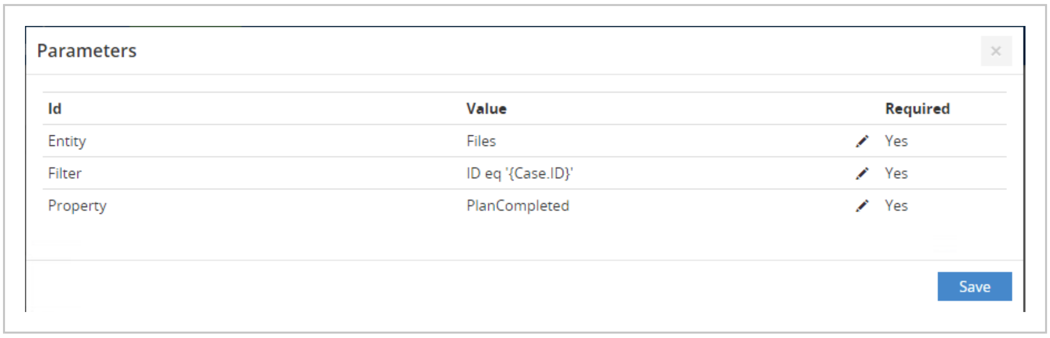


Parameters

Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Property	Created	Yes

Save

Activity2 (GetValue from PlanCompleted) fetches the date from the **PlanCompleted** field on the current case. The parameters are defined as follows:



The Include and Exclude relation types have guards that compare the dates.

- Include relation type:

  `Activity1<Activity2`

- Exclude relation type:

  `Activity1>Activity2`

If the date fetched by activity1 is less than the date fetched by activity2, the subsequent activity will be included, in this example a **StartProcess** activity is executed, which starts a hearing process. If the condition is not met, nothing will happen.

> Note: Do not use @Me or @Unit in the **GetValue** activity. The **GetValue** activity is always executed automatically by a system user, and therefore @Me and @Unit will fail. See Execute activities automatically.

SetValue

SetValue allows you to set a value based on a query in a WorkZone field. You can use the **Computations** field on the **SetValue** activity to provide an expression, for example combining a **GetValue** activity and actual values. The value that is calculated in the **Computations** field, will be the value that will be set in the specified WorkZone field.

Empty fields and computations

If a field being used as a basis for computations in DCR process is empty, some computations based on that field can result in an error with the error message similar to the following error message (triggered for some computations involving date and time): *Conversion is not supported from type DCR.Time.Duration to Odata type [Edm.DateTime Nullable=True]*

As the type of the result of the computations must match the type of the property it will be assigned to, for example integer fields with integer types and DateTime fields with DateTime types, using an empty field as a basis for calculation operations can result in an conflict of field types and thereby trigger the error.

SetValue parameters

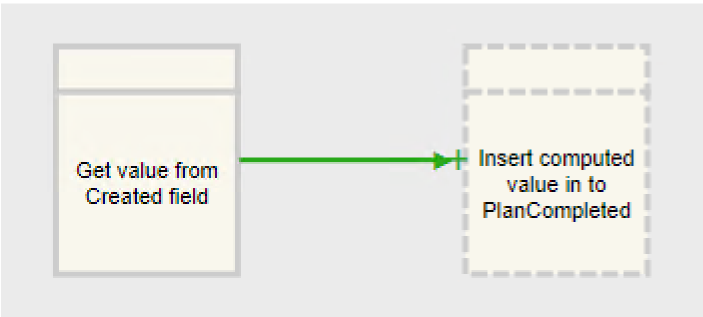
Parameter	Description	Required
Entity	Specify on which entity you want to set a value, for example **Files** (Cases).	Yes
Filter	Enter the key of the entity. If you always want to set a value on the current case, which is the case that the case activity is started on, you can enter: `ID eq '{Case.ID}'` **Tip:** You can use WorkZone QueryBuilder to build your query and copy the filter part to this parameter. See How do you copy a query from WorkZone QueryBuilder.	Yes
Property	Specify the property that you want to insert the value in to. For example, if you want to set a date in the **Planned completed** property, enter: `PlanComplete` **Tip:** You can use WorkZone QueryBuilder to find the name of the available properties.	Yes
MaxEntitiesToUpdate	The maximum number of entities that the activity can set. For example, if you set this parameter to 10, and your query results in 10 cases or less, all cases will be updated. If the result of the query exceeds the maximum, the activity will fail , and an error message	

Parameter	Description	Required
	will be shown in the history.	

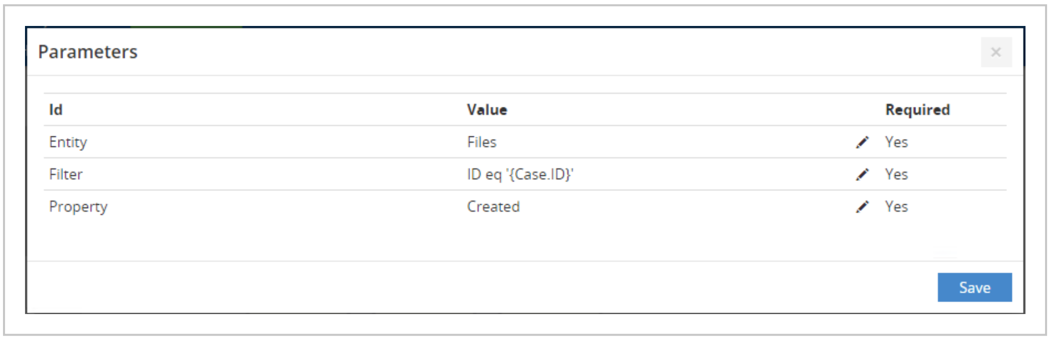
Example

> **Example**: In this example, the created date of the current case is retrieved using a **GetValue** activity. The **Created** value is used to calculate the planned complete date which will be 7 days later. The new date will be stored in the **PlannedComplete** property on the case.

The DCR process looks like this:



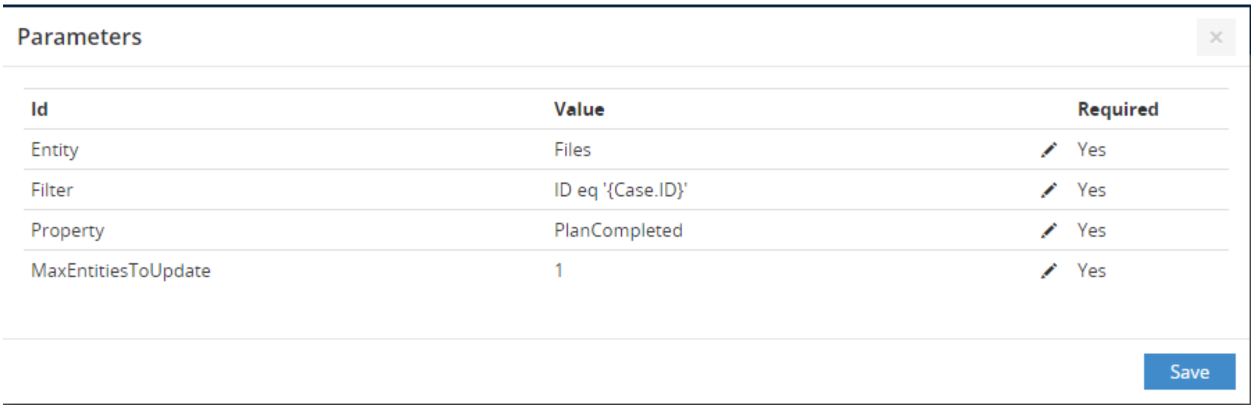
Activity0 (GetValue from Created field) fetches the date from the **Created** field on the current case. The parameters are defined as follows:


Parameters

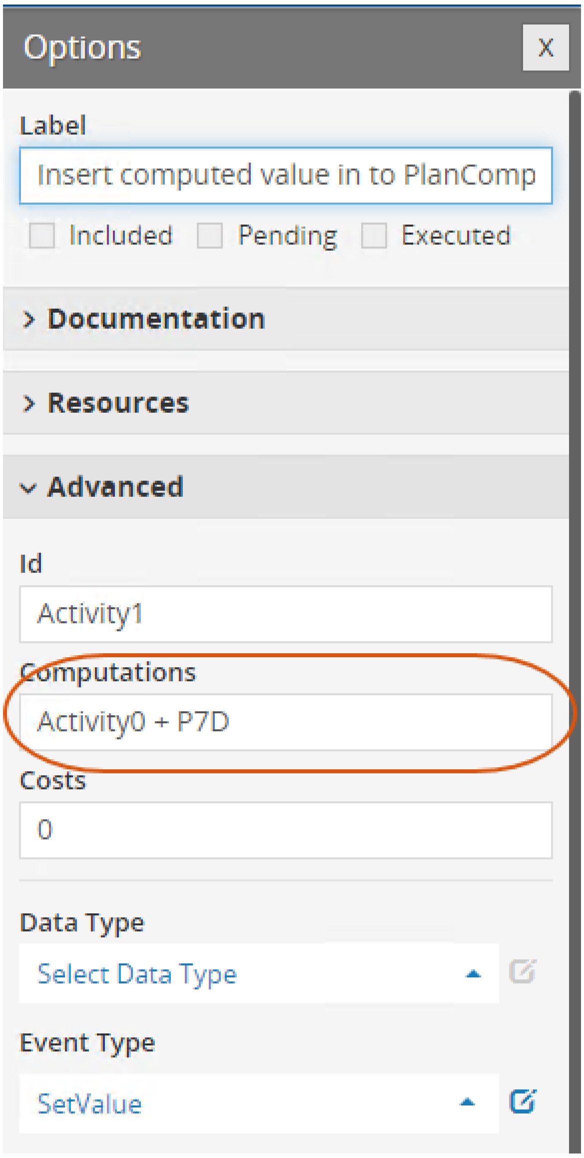
Id	Value	Required
Entity	Files	Yes
Filter	ID eq '{Case.ID}'	Yes
Property	Created	Yes

Save

Activity1 (Insert computed value to PlanCompleted) sets the new date in the **PlanCompleted** property on the current case based on the calculation of the date in the **Computations** field of the **SetValue** activity. The parameters are defined as follows:



In the **Computations** field of the Activity0, insert `Activtity0 + P7D`, which results in a value (Created date plus 2 days) that will be stored in the **PlanCompleted** property, when the **SetValue** activity is executed.



The Running status and idle processes

Whenever an activity is executed, the DCR process status will be changed to **Running**. If a DCR process remains in the **Running** status for more than 5 minutes without signs of active activities, the process will be considered to be idle, which enables users and the WorkZone system to perform operations on the process.

A DCR process is considered idle, even in the case of serious long-present network errors which could result in Case Activity process not being able to switch back to **Persisted** status.

Execute activities automatically

To reduce the manual work that a user has to do in a case activity list, you can configure activities to be executed automatically. You can apply automatic execution in two ways by assigning either the **AUTO** role or the **L-AUTO** role to the activity, depending on when you want the activity to be executed. The activity will be executed by a system user.

> **Note:** If there are more than 50 automatic activities executed in a loop or just sequentially in the DCR process, an error will be triggered at the 51st activity with the error message: *"Maximum number of loop iterations of graph execution reached. Loops or automatic execution flows with more than 50 executions are not allowed."*
>
> This restriction helps prevent endless loops which can result in Case Activity processes remaining locked in the **Running** status.

AUTO

Activities with the **AUTO** role assigned will be executed automatically once as soon as the activity is included. This means:

- If an **AUTO** activity is successfully executed automatically, it will be set to manual for any additional executions.
- If an **AUTO** activity fails to be executed automatically, it will be set to manual for any additional executions.

If an activity fails to execute automatically, it will stay active and the user can execute it manually. If the activity is executed manually, the default values as set in the DCR process are shown in the form. The user can then change the values and execute the activity.

L-AUTO

Activities with the **L-AUTO** role assigned are executed soon as they are included and pending. Pending in this context means that the activity is required before the process can be considered completed. If the activities become pending again later in the process, they will be executed automatically again.

You can also assign the **L-AUTO** role to activities if you want to align the behavior of your WorkZone case activities with the simulation in DCR Design Portal using the lazy user role. See the [DCR documentation](#).

The **L-AUTO** role itself does not execute an activity automatically. You need to design the process so that the activity becomes included and pending (the **Pending** check box is selected on the activity or the activity has a **Response** connection–a blue arrow in the process).

Note:

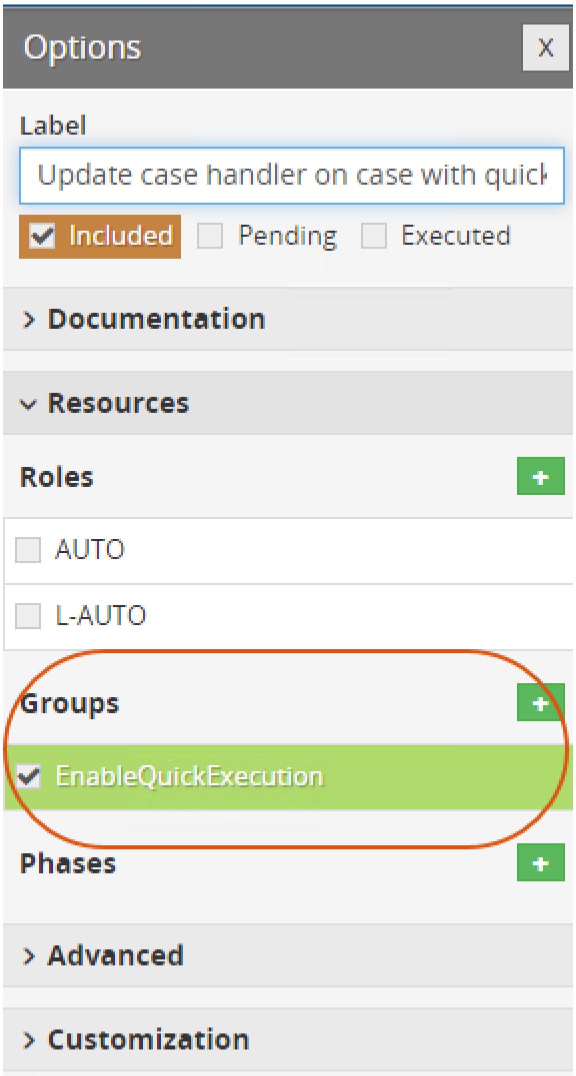
- If you assign the **AUTO** or the **L-AUTO** role to the **CopyDocument** activity, you cannot use the value UP (Personal draft) for the **DocumentState** parameter. As it is a system user who executes activities automatically, only the system user will be able to see the document. See CopyDocuments.
- If you assign the **AUTO** role or the **L-AUTO** to an **UpdateEntities** activity or a **ValidateEntities** activity, you cannot use the @Me or @Unit notations. @Me and @Unit will fail because it is a system user that executes activities automatically. See Current user and organizational unit.
- Assigning the **AUTO** role or the **L-AUTO** to a **StartProcess** activity only works for processes without parameters. See the StartProcess activity type.
- In DCR terminology, "Pending" means that the activity must be executed before the whole process (the case activity list) can be considered complete.

Enable quick execution of activities

You can configure activities to be executed without opening dialog boxes. On all activity types, you can select an **EnableQuickExecution** option, which will display a check box next to the activity in WorkZone Client. When a user selects the check box, the activity is executed immediately without opening a dialog box.

Enable quick execution

1. In your DCR process, select the activity you want to enable quick execution for.
2. In the **Options**, click **Resources**, and select the **EnableQuickExecution** check box under **Groups**.



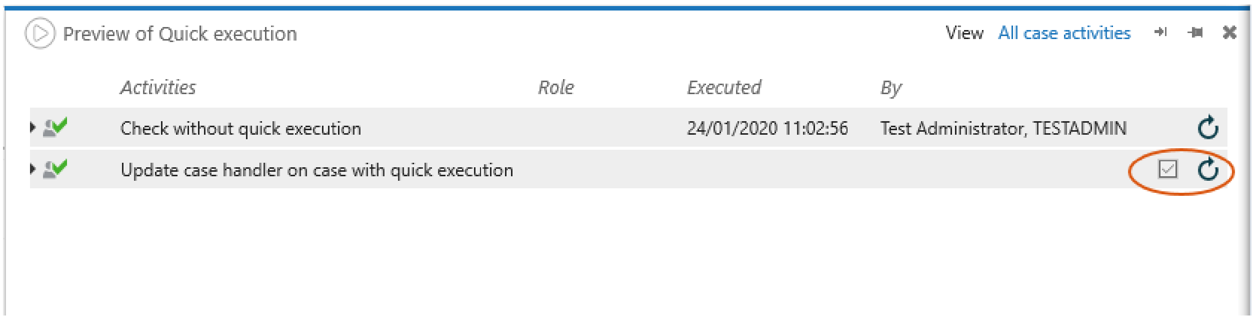
Quick execution in WorkZone Client

When users open an activity list in WorkZone Client, a check box appears next to activities that have the **EnableQuickExecution** option enabled. When a user selects the check box, the activity is executed immediately without opening a dialog box.

Example

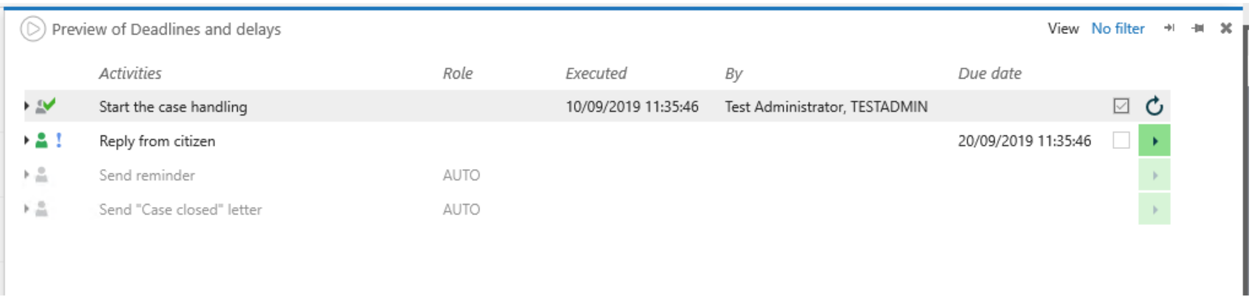
In this example, the activity list consists of a **Check** activity without quick execution enabled and an **UpdateEntities** activity with quick execution enabled.

The **UpdateEntities** activity named "Update case handler on case with quick execution" has the **EnableQuickExecution** option enabled and a check box is shown. When the user selects the check box, the activity is executed without opening a dialog box.



Apply deadlines and delays to activities

You can apply deadlines and delays to activities in a DCR process using relations, which means that you can execute an activity automatically after a certain amount of time has passed (a delay) or when a certain point in time is reached (a deadline). Users will see the date that is calculated on the basis of the deadline in the **Due date** column in the activities preview pane in WorkZone Client.



See Deadlines in the WorkZone Client User Guide.

Deadline

You can define a deadline for an activity to be executed. The deadline is relative and is calculated from the point in time that an activity is executed.

In the DCR process, you can add deadlines to the **Response** relation type.

For more information about the **Response** relation type, see the DCR documentation. .

Delay

In addition to deadlines you can define a delay which will enable an activity with a delay or execute it with a delay if the activity is of the type AUTO. The delay is calculated from the time that an activity is executed.

In the DCR process, you can add delays to the **Condition** relation type.

For more information about the **Condition** relation type, see the DCR documentation. .

Set a deadline or a delay on an activity

1. In your DCR process, insert a relation of the type **Response** if you want to apply a deadline or **Condition** if you want to apply a delay.
2. In **Options**, enter a deadline in the **Deadline** field or a delay in the **Delay** field depending on the relation type and what you want the process to do.

The notation for deadlines and delays is: days.hours:minutes:seconds

> **Example**: 1.1:30:00 which indicates a deadline or a delay within one day, one hour, and 30 minutes from the activity was executed.

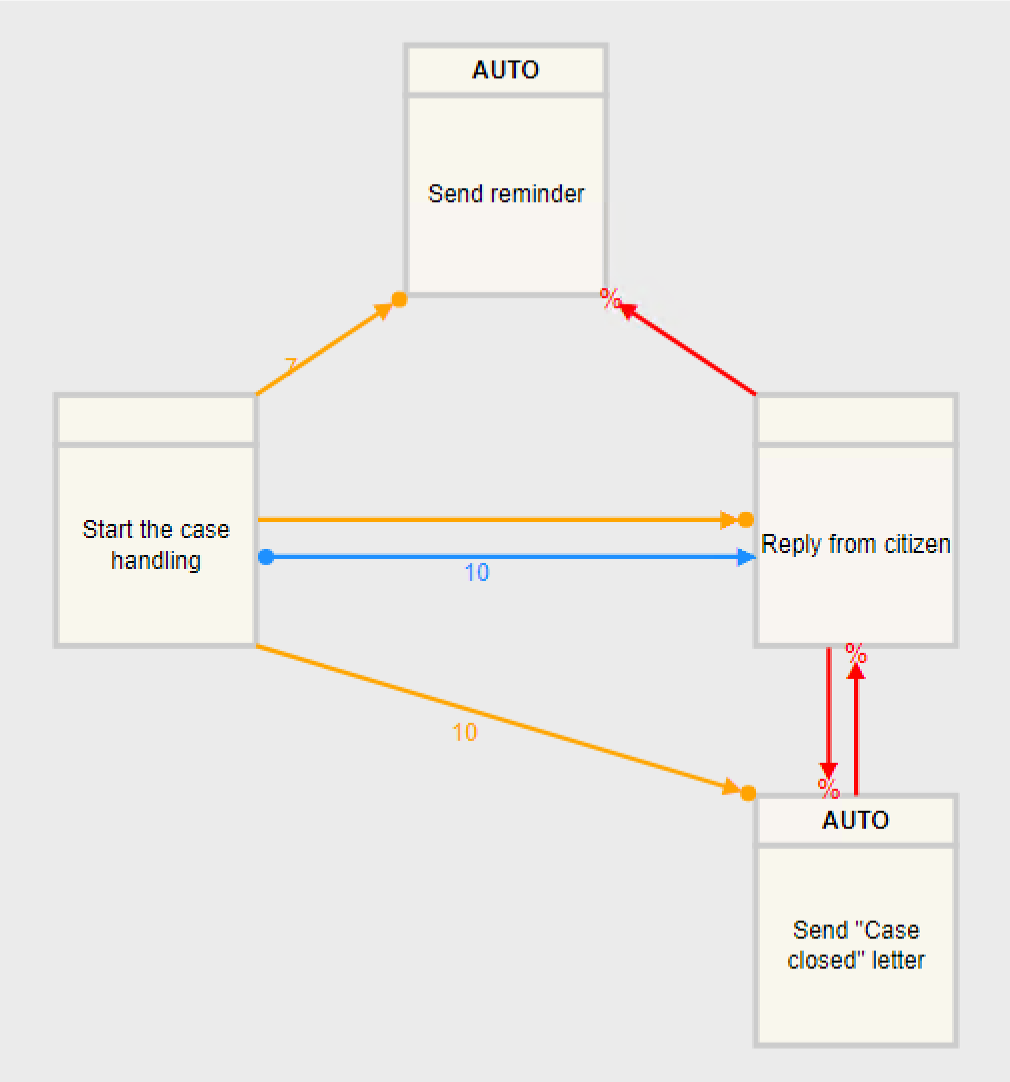
If you only specify, for example, 2 it means two whole days.

For more information about use of deadlines and delays in DCR processes, see the DCR documentation.

Example: DCR process with deadlines and delays

A case handler sends a letter to a citizen with a reply deadline 10 days after the letter has been sent. If the citizen has not replied after 7 days, a reminder letter will be sent to the citizen's e-Boks automatically using SmartPost. When the reply from the citizen is received, a letter with information about the case being closed it is sent automatically to the citizen with a one minute delay using SmartPost.

The DCR process may look like this:



- A deadline of 10 days is specified on the **Response** relation type for the Reply from citizen activity.
- A delay of 7 days is specified on the **Condition** relation type, which ensures that the Send reminder activity is executed if a reply has not been received.
- A delay of 10 days is specified on the **Condition** relation type that sends the Send "Case closed" letter when the deadline has passed and no reply has been received.

Export and deploy case activity processes

To prepare your DCR process for packaging and for import into WorkZone, you need to export the process to an XML file, and then deploy it using WorkZone Configurator.

Export case activity processes as XML

1. In DCR, select the process that you want to export.
2. Click **File** > **Export As XML**. The process is now exported to an XML-document wit the same name as the process.

To make the case activity workflow available to WorkZone Client users, you must deploy the DCR process using WorkZone Configurator.

Deploy the case activity process

In WorkZone Configurator, you must import the DCR process XML-document that you just exported from DCR and deploy it.

> **Prerequisite:** To configure and deploy case activities, you must have the PROCESSADM access code.

1. Open WorkZone Configurator.
2. Click **Process** and follow the instructions in the Case activities topic in the WorkZone Configurator Administrator Guide.

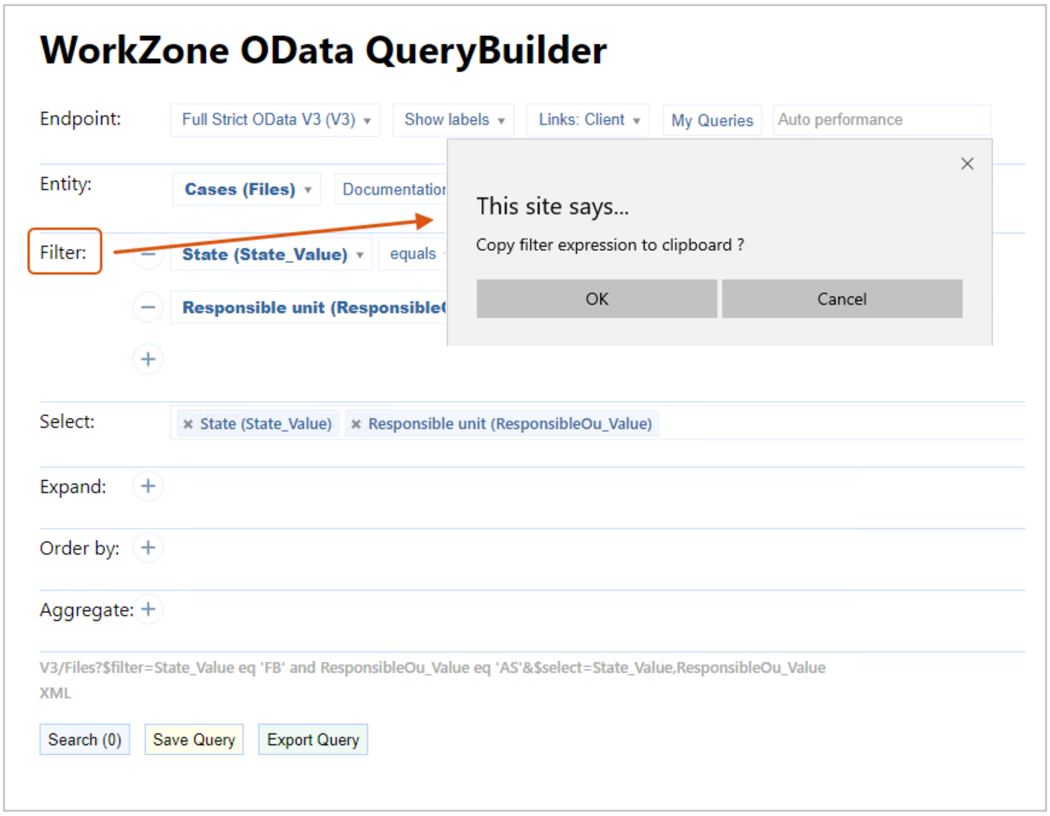
FAQs about case activities

This section contains a list of frequently asked questions on WorkZone Process functionality. Click any question below to see the answer.

How do you copy a query from WorkZone QueryBuilder

Some activity types have parameters that require you to specify properties and values or filters in JSON format. You can use WorkZone QueryBuilder to create queries, and then copy them to the activity type parameters.

1. Create a query in WorkZone QueryBuilder.
2. Click the **Filter** element to copy the filter expression, and then click **OK** to copy the filter to the clipboard.



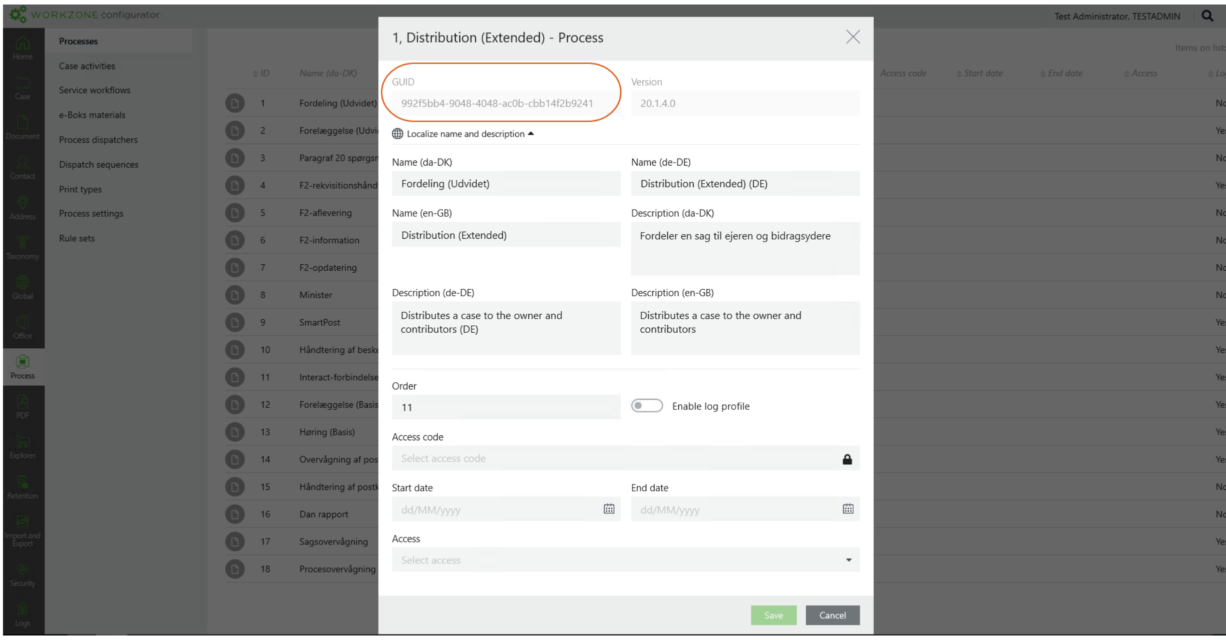
3. Paste the filter in to the **Properties** parameter of an activity. In this example, the filter expression `State_Value eq 'FB' and ResponsibleOu_Value eq 'AS'` is copied and pasted.

How do you look up process GUIDs

Some activity types require that you specify the GUID of a process in a **ProcessGuid** parameter. You can look up process GUIDs in WorkZone Configurator.

1. In WorkZone Configurator, go to **Process** > **Processes**.
2. Point to the process you want to get the GUID for.
3. Click  **Edit process parameters**.

4. Copy the GUID from the **GUID** field and paste it into the GUID parameter of the activity.



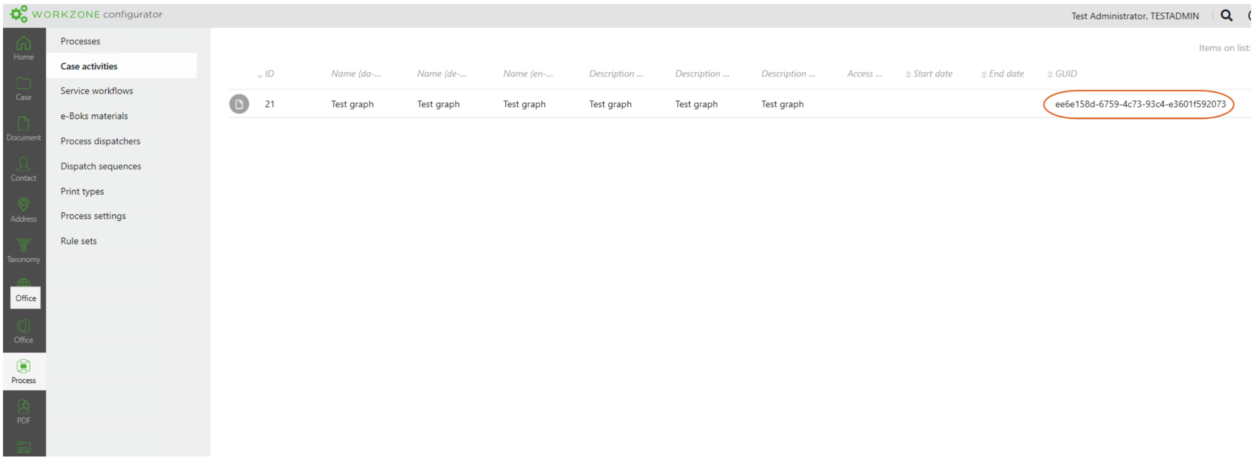
> **Tip:** You can also look up GUIDs in the WZP_PROCESS table using ScanSQL.

How do you look up case activities GUIDs

Some activity types require that you specify the GUID of a process in a **ProcessGuid** parameter. You can look up process GUIDs in WorkZone Configurator.

1. In WorkZone Configurator, go to **Process** > **Case activities**
2. Point to the case activity you want to get the GUID for.
3. Scroll to the **GUID** column.
4. Copy the GUID from the **GUID** field and paste it into the GUID parameter of

the activity.



> **Tip:** You can also look up GUIDs in the WZP_PROCESS table using ScanSQL.

Why can't users access their cases during Case activity execution?

Users will temporarily be unable to modify a case when the case is locked during process execution (for example during SmartPost execution). The users will encounter an error message indicating lack of appropriate access rights because the case is running with the system user's access rights and not the user's assigned access rights. Automatically triggered Case Activities on the case are executed normally, but manually triggered activities cannot be executed by the user.

This behavior is implemented to temporarily protect the case from updates during the execution of actions (for example generation of pdf reports). After these actions are completed, the user will be able to access the case and execute case activities again.

Troubleshooting case activities

Click an issue below to see the solution or workaround.

Send SmartPost error messages

When users execute an activity list in WorkZone Client and an activity fails, an error message is shown under **History** in the **Case activities** pane. The activity may fail due to wrong configuration of the Send SmartPost activity in the DCR process. Below you will find a list of error messages with extended descriptions.

"The activity cannot find the specific letter document to send."

Message in Danish: "Aktiviteten kan ikke finde det specifikke brevdokument, der skal sendes."

The message is shown if the letter document specified in the **Letter** parameter does not return a specific document that can be used as the letter document. The query must only return one specific document. For example, if more than one Word document is saved on the case, the query must define exactly which document must be used as the letter. The activity may also fail if the specific document does not exist on the case.

"The activity cannot find valid recipient addresses."

Message in Danish: "Aktiviteten kan ikke finde gyldige modtageradresser."

The message is shown if the **Recipient** parameter in the query or the role notation do not return any recipients, for example if the activity contains a wrong query or it lists wrong or non-existing roles.

"The total number of messages to send exceeds the allowed maximum number. The maximum number is 50 messages."

Message in Danish: "Det samlede antal beskeder, der skal sendes, overstiger det tilladte maksimale antal. Du kan højst sende 50 beskeder."

The message is shown if the number of messages to send exceeds the allowed maximum number, which is currently set to 50 messages. The number of messages is calculated based on both messages to recipients and copy recipients. You can as the process designer modify the **Recipient** parameter to retrieve less recipients, or the user can reduce the number of case parties with the specified roles on the case.

"The activity cannot start the SmartPost process. The SmartPost process is not valid."

Message in Danish: "Aktiviteten kan ikke starte SmartPost-processen. SmartPost-processen er ikke gyldig."

The message is shown if the activity contains an invalid SmartPost process GUID in the **ProcessGuid** parameter.

"The activity cannot start the SmartPost process. The value {ProcessOwner} is not valid for the 'ProcessOwner' parameter."

Message in Danish: "Aktiviteten kan ikke starte SmartPost-processen. Værdien {ProcessOwner} er ikke gyldig for parametret 'ProcessOwner'."

The message is shown if the process owner cannot be found because the contact does not exist or has reached the end date or there is no case handler on the case or the document.

Troubleshooting

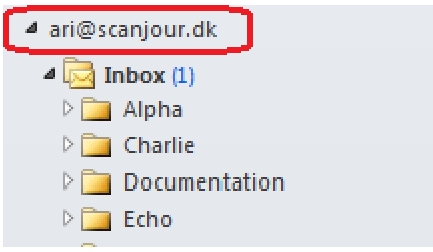
Click an issue below to see the solution or workaround.

Problems related to Proxy users in Microsoft Outlook

When a proxy user performs an action in a smarttask, the state of the user task is not updated according to the action.

The issue is caused by incorrect write permissions for the user account in Microsoft Outlook. To work around this issue:

1. Right-click the top-level node in the navigation pane (normal view):



2. Select **Folder Permissions**. The **Outlook Today - [user account] Properties** dialog box is displayed.
3. Click the **Permissions** tab.
4. For each listed user, select **Edit all** if not already selected.
5. Click **OK**.

> Important: You need to perform the same steps for all shared folders under the user account. To enter settings for shared folders, right-click a shared folder and select **Properties**.

Service is stopped when a process is started

To work around this issue:

Ensure that WorkZone Process Services (`Scanjour Service COM WZP` and `ScanJour workZone Process Asset Update Service`) are running when WorkZone Process is being used.

404 error when running in a load balanced environment

A 404 error may occur when you run the `Scanjour.Workflow4.UpdateAssets` service.

To work around this issue:

1. Select **Run as a different user** in Internet Explorer and, for the user who uses the service, add the website as a trusted site on the local intranet.
2. Select **Automatic logon with current user name and password** under **User Authentication**.
3. Locally on the server, select the following security settings for the local intranet zone:
    - MIME Sniffing: **Enable**
    - Include local directory path when uploading files to a server: **Enable**
    - Launching applications and unsafe files: **Enable**
4. In **Local Area Network (LAN) Settings**, leave **Automatically detect settings** unselected.

An error icon is displayed in the Processes overview

Sometimes an error icon can be displayed in the Processes overview.

To work around this issue:

1. See the tooltip of the error icon ⚠.
2. Take the necessary action - for example, give the actor read access to the document or ensure that the actor's e-mail address exists in WorkZone Client.

Smarttask appear as not loaded

The content of smarttask may appear as not loaded or loaded with no other content than a grey background.

This may be happen if the Exchange Server is using an SSL certificate that does not work (for example, it has become inactive).

In order to debug this issue:

1. In Outlook, click **File** > **Options**.
2. On the left pane, select **Advanced**.
3. In the **Developers** section in the contents on the right, select the **Show add-in user interface errors** check box.
4. Click **OK**.
5. Restart Outlook.
6. Open a smarttask.

If you get an error message saying that an exception has occurred and it contains the word “Autodiscover”, then it is a known issue with an SSL certificate that does not work.

To work around this issue:

1. Open the **IIS Manager** on the Exchange server.
2. Navigate to Default Web Site.
3. On the action pane to the right (under **Edit Site**), click **Bindings**.
4. Edit all the bindings of the type `https`.
5. From the **SSL certificate** list, select a valid SSL certificate.
6. Recycle all the `MSExchange(x)` application pools.
7. Click **OK**.

Task locked by other user

When a user has opened a task, it is locked, and other users cannot work on it.

Workaround:

To unlock a task, you need `PROCESSADM` access rights.

Searching by document ID does not produce a search result

To search for documents from WorkZone Process, you must know part of the title of the document. If you want to search for a document based on the document ID, you should process the search from WorkZone. In WorkZone 2016, the search option is already available.

To enable the search feature in WorkZone 2014, run the script i_ctx_record_title.sql which is located in **Program Files** (x86) under \KMD\Workzone\Process\Config\scripts in sqlplus:

```
sql> @i_ctx_record_title.sql
sql> execute create_i_ctx_record_title;
sql>
```

A mail agent user does not receive smart tasks in Outlook as expected

Setting up a mail agent user who is not the user running the WorkZone Process Mail Agent, when you configure WorkZone Process in environments, where you cannot make changes to the Active Directory, requires a workaround. Failing to complete this workaround will have the effect that users will not receive smart tasks in Outlook as expected. The server event log will report that users running the WorkZone Process Mail Agent do not have permission to send mails on behalf of the mail agent user.

To work around this issue, complete this step:

- Open Outlook as the mail agent user and to add the WorkZone Process user as a delegate or representative, click **File** -> **Account Settings** -> **Delegate Settings** -> **Add** > [user running WorkZone Process Mail Agent]

Changes to mail notification settings don't seem to be applied

When you enable email notifications for one or more users you must update the email notification settings to make the changes apply. We recommend that you update the settings by recycling the WzpSvc application pool from the Internet Information Services (ISS).

Mail notifications are also updated if you restart the ISS. However, restarting the IIS will affect applications and services apart from the email notifications so recycling the WzpSvc application pool is the preferred method.

For more information about the mail notification configuration, see Configure notifications.

Smart task and Start process do not load correctly

When trying to open a smart task or start a process from the Process view, the task or process might fail to load correctly. You will get the message that a value is missing to complete the action.

To work around this issue, complete these steps:

- Close Outlook

- Clear the cache in Internet Explorer

- Reopen Outlook

Configurator fails to load data into database

When working with the configurator, you might experience that it fails with the following message:

Error 6 initializing SQL*Plus

SP2-0667: Message file sp1<lang>.msb not found

SP2-0750: You may need to set ORACLE_HOME to your Oracle software directory.

To work around this issue, either restart the server machine or log off and then log on to the machine again.

"Concurrent connections exceeded" when using the Mailbox Monitor and F2 integration service workflows

You may experience errors if you use the Mailbox Monitor and F2 integration service workflows. Error text in the event log:

```
Unable to initialize ExchangeConnection on "host address": Microsoft.Exchange.WebServices.Data.ServiceResponseException: You have exceeded the available concurrent connections for your account. Try again once your other requests have completed.
```

```
Error is caused by a high number of concurrent exchange connection on single email account.
```

To solve this issue, you can configure multiple Mailbox Monitor/F2 integration services to run on different user accounts. You can also modify the Exchange throttling policy based on Microsoft guidelines. See Modify the EWS throttling policy to handle concurrent connections.

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.